

Administering Security for Solaris 2.x Operating Environments

SC-300



Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303, U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun Logo Solaris, and NFS are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

The OPEN LOOK and Sun Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government approval required when exporting the product.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g) (2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015 (b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.



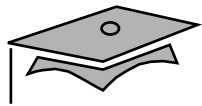
About This Course



Course Goal

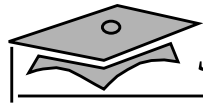
This course provides you with knowledge and skills to

- Function as a Solaris™ Operating Environment security administrator



Course Overview

- Solaris Operating Environment utilities from a security point of view
- Security tools available on the Internet



Course Map

Security Basics

Terminology
and Overview

Basic System
Security

UNIX
Vulnerabilities

Common
Security Cracks

Access Control

Protecting
Files and
Data

Controlling
Root Access
With sudo

Secure Shell

Remote Access
and
Authentication
Services

Using
Secure NFS

Logging and Auditing

Solaris
Operating
Environment
syslog

Basic Security
Module
(BSM)

Automated
Security
Enhancement
Tool (ASET)

SATAN and
Courtney

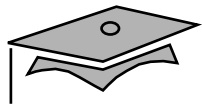
TripWire

TCP_Wrappers

Crack

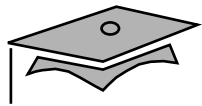
Summary

Security
Strategies



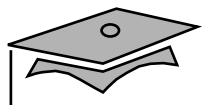
Module by Module Overview

- Module 1 – "Terminology and Overview"
- Module 2 – "Basic System Security"
- Module 3 – "UNIX Vulnerabilities"
- Module 4 – "Common Security Cracks"
- Module 5 – "Protecting Files and Data"



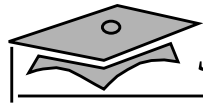
Module by Module Overview

- Module 6 - "Controlling Root Access With sudo"
- Module 7 – "Secure Shell"
- Module 8 – "Remote Access and Authentication Services"
- Module 9 – "Using Secure NFS"
- Module 10 – "Solaris Operating Environment syslog "
- Module 11 – "Basic Security Module (BSM)"



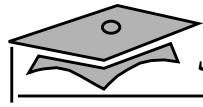
Module by Module Overview

- Module 12 – "Automated Security Enhancement Tool (ASET)"
- Module 13 – "SATAN and Courtney"
- Module 14 – "TripWire"
- Module 15 – "TCP_Wrappers"
- Module 16 – "Crack"
- Module 17 – "Security Strategies"



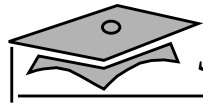
Course Objectives

- Describe the difference between system and physical security
- List three common causes of data damage
- Describe the terms *accountability*, *availability*, *authentication*, *confidentiality*, and *integrity*
- Create and maintain secure user accounts and passwords
- Administer a guest user account with a restricted shell
- Use operating system tools on processes, swap spaces, and devices to determine which users or processes are affecting the system
- Manage and terminate unwanted processes
- Change the permissions of devices and files to better secure the system
- Describe seven common cracks in security and describe two implications of each
- Describe how tools such as SATAN and Crack can be used against your system
- Troubleshoot and recover from a simulated system attack.
- Securely create directories, share file systems, and mount network file systems
- Securely set basic permissions and extended permissions using Access Control Lists (ACLs)
- Use SKIP to encrypt network data between systems
- Install and configure `sudo`, configure administrative groups using `sudo`, and grant and monitor root access



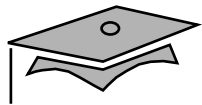
Course Objectives

- Describe how `sudo` can be used to better secure your system by limiting root login usage and providing detailed logging
- Install, configure, and use the secure shell
- Secure specific utilities, such as `rlogin`, `telnet`, `rsh`, and `ftp`, in order to provide limited access to specific users
- Change an authentication module by modifying the PAM configuration file
- List the differences between Diffie-Hellman and Kerberos authentication
- Describe Secure RPC (Remote Procedure Call) as it relates to Secure NFS
- List the security advantages of Secure NFS over NFS
- Configure an NIS+ name server and client to support Secure NFS
- Configure Secure NFS to securely share specific file systems with certain users
- Configure an Network Information Service Plus (NIS+) name server and client to support the use of Secure NFS
- Use `inetd` to log Transmission Control Protocol (TCP) connection utilizing `syslog` messages for the `telnet` and `ftp` services
- Configure `syslog` to capture log messages for incoming network services in a separate log file
- Configure a loghost machine to act as a centralized syslog message collection site
- Use the Basic Security Module (BSM) to log user login information



Course Objectives

- Using administrative files, implement device allocation functionality
- Describe the three different ASET security levels
- Properly configure ASET at each security level
- Given an ASET report, better secure the system
- Compile and install SATAN and Courtney
- Use SATAN and Courtney to find weaknesses in a system and monitor attacks
- Describe how SATAN and Courtney can be used together for better security
- Procure, compile, and install TripWire
- Use TripWire to monitor system files for unauthorized modification
- Describe how TripWire can be used to better secure a system
- Describe how TCP_Wrappers are used
- Procure, compile, and install TCP_Wrappers
- Use TCP_Wrappers to log use of telnet, ftp, and rsh utilities; control access; display messages; and send email
- Describe the specific use of Crack
- Procure, compile, and install Crack
- Using Crack and supplied password libraries, check for weak passwords
- Create a security policy and strategy



Skills Gained by Module

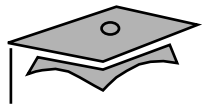
Meaning of:

- Black boxes
- Gray boxes

Skills Gained	Module			
	1	2	3	4
Skill or Objective 1	Black			
Skill or Objective 2	Black		Gray	
Skill or Objective 3		Gray	Black	
Skill or Objective 4				

Guidelines for Module Pacing

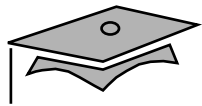
Module	Day 1	Day 2	Day 3	Day 4	Day 5
"About This Course"	AM				
Module 1 – "Terminology and Overview"	AM				
Module 2 – "Basic System Security"	AM				
Module 3 – "UNIX Vulnerabilities"	PM				
Module 4 – "Common Security Cracks"	PM				
Module 5 – "Protecting Files and Data"		AM			
Module 6 – "Controlling Root Access With sudo"		AM			
Module 7 – "Secure Shell"		PM			
Module 8 – "Remote Access and Authentication Services"		PM			
Module 9 – "Using Secure NFS"			AM		
Module 10 – "Solaris Operating Environment syslog"			AM		
Module 11 – "Basic Security Module"			PM		
Module 12 – "Automated Security Enhancement Tool (ASET)"				AM	
Module 13 – "SATAN and Courtney"				PM	
Module 14 – "TripWire"				PM	
Module 15 – "TCP_Wrappers"					AM
Module 16 – "Crack"					PM
Module 17 – "Security Strategies"					PM



Topics Introduced

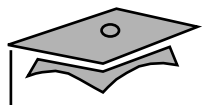
Topics that are introduced but not covered *in depth* are:

- Pluggable Authentication Module (PAM)
- C2
- Basic Security Module (BSM)
- SATAN, CRACK, TripWire, TCP_Wrappers, and Courtney from an administrative point of view
- Network Information Service (NIS and NIS+)



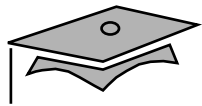
How Prepared Are You?

- Use Solaris 2.x Operating Environment user utilities, system utilities, and networking and device utilities
- Administer and monitor Solaris 2.x Operating Environment network configurations
- Administer user accounts, and configure Solaris Operating Environment routing and network interfaces



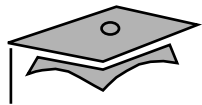
Introductions

- Name
- Company affiliation
- Title, function, and job responsibility
- UNIX[®] administration experience
- UNIX security experience
- Reasons for enrolling in this course
- Expectations for this course



How to Use Course Materials

- Course map
- Relevance
- Overhead image
- Lecture
- Exercise
- Check your progress
- Think beyond



Typographical Conventions and Symbols

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your .login file. Use <code>ls -a</code> to list all files. system% You have mail.
AaBbCc123	What you type, contrasted with on-screen computer output	system% su Password:
<i>AaBbCc123</i>	Command-line placeholder—replace with a real name or value	To delete a file, type <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class options</i> . You <i>must</i> be root to do this.



Module 1

Terminology and Overview



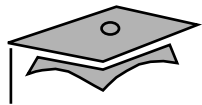
Overview

- Objectives
- Relevance



What Is Security?

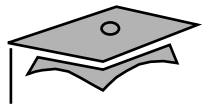
- Philosophy
 - Everything is allowed
 - Nothing is allowed
- Policy



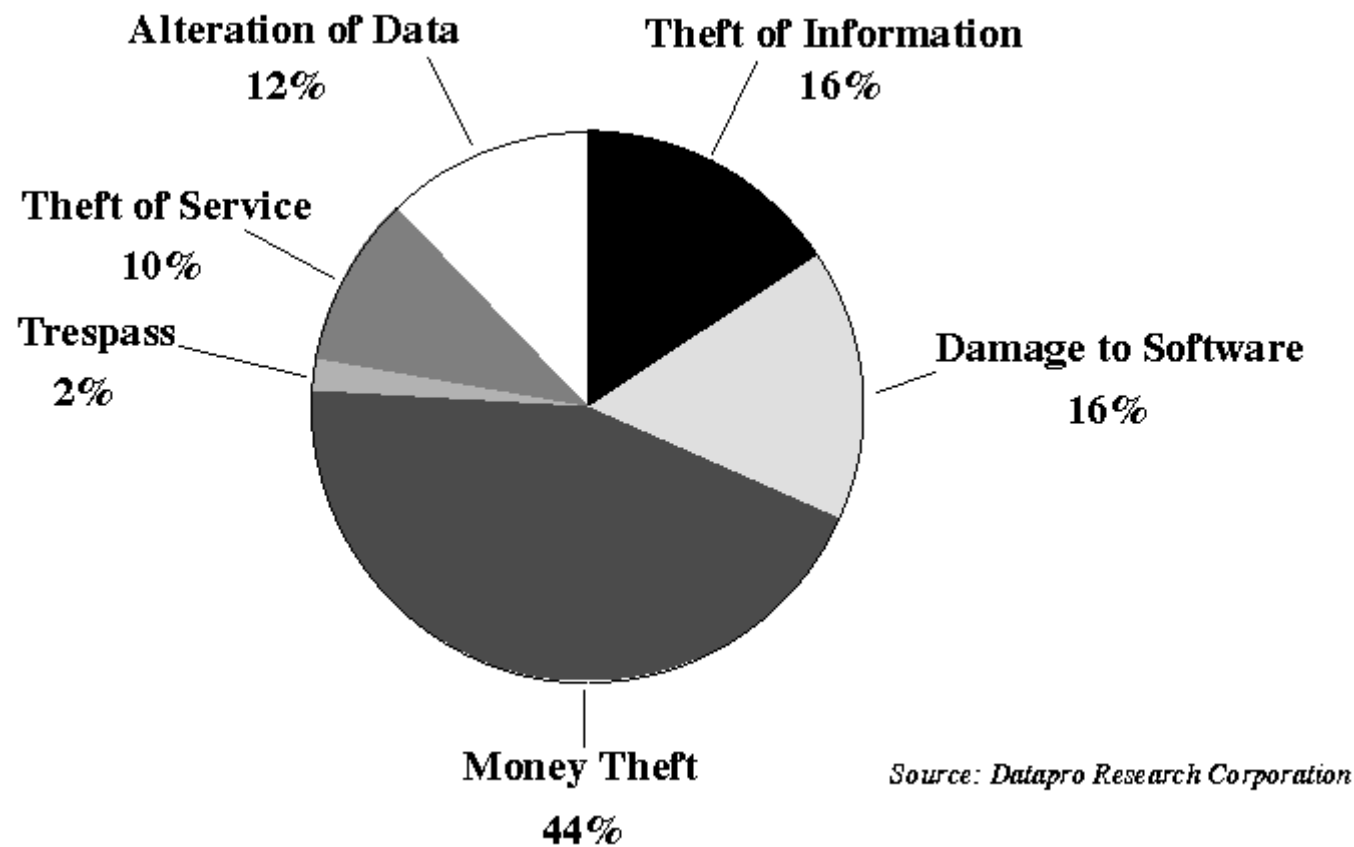
Common Causes of Damage to Data

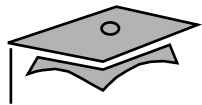


Source: Datapro Research Corporation

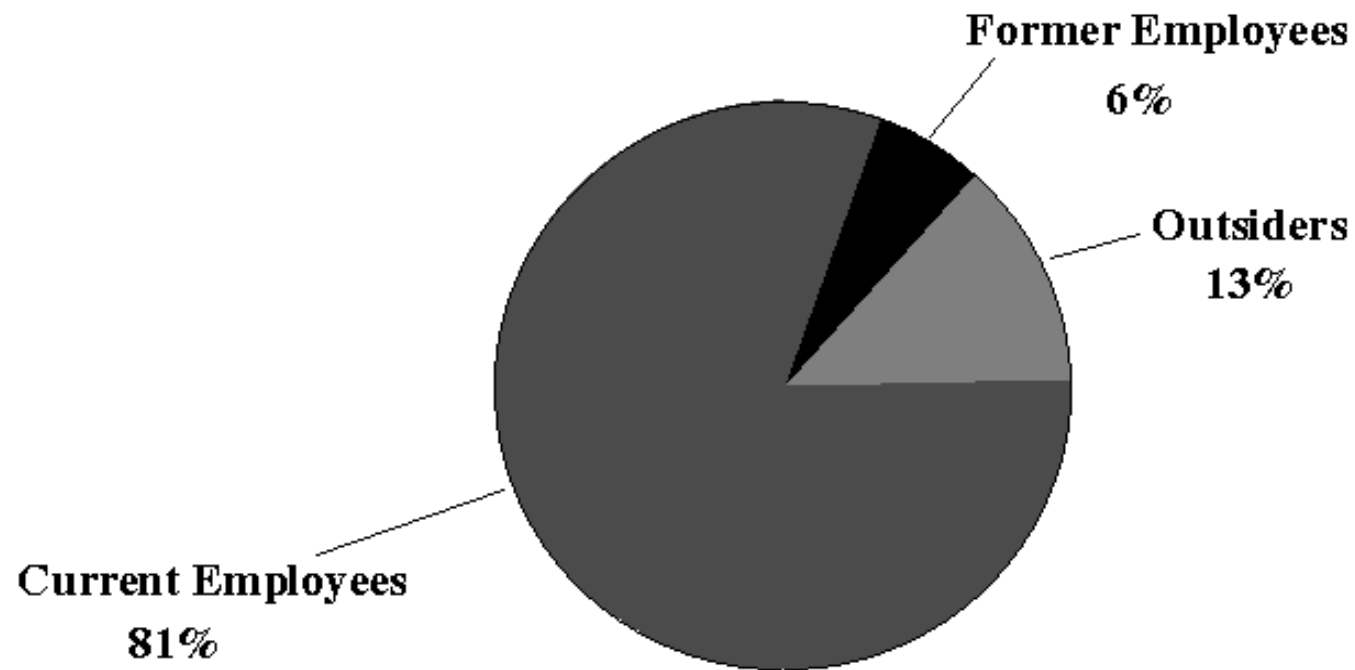


Types and Perpetrators of Computer Crimes

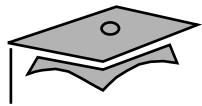




Types and Perpetrators of Computer Crimes

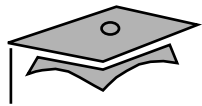


Source: Data Processing Management Assoc.



Advisories

- Computer Emergency Response Team (CERT) Coordination Center
- Computer Incident Advisory Capability (CIAC)
 - Studies Internet security vulnerabilities
 - Provides incident response services
 - Publishes security alerts



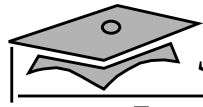
Security Standards

- National Security Agency (NSA)
- National Institute for Standards and Technology (NIST)
- Information Technology Security Evaluation Criteria (ITSEC) in Europe
- Institute of Electrical and Electronic Engineers (IEEE)
- Internet Engineering Task Force and Generic Security Service Application Program Interface (IETF GSS-API)
- The Open Group



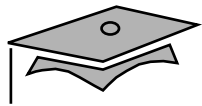
Secure Operating Systems Standards

- The Department of Defense (DoD)
 - Rainbow Series of security books



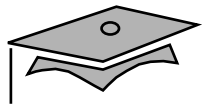
The DoD Seven Layers of Trust

D	Minimal protection is provided, and no security features are provided.
C1	Discretionary access control (DAC) and access permissions are provided. Logins with passwords required.
C2	Auditing and authentication events are provided. Authentication data is kept in a secure place.
B1	Mandatory access control and labeled output are provided. Access is based on labels which designate security clearance.
B2	Configuration control, facility management and system configuration must be documented and controlled. All administrative security and operator functions are separated.
B3	Access control lists and full system documentation are provided, Access is based on lists of users plus labels.
A	Formal proof of the security of the system is required.



System Security

- Authentication
 - Password control
 - Network authentication
 - Key
 - Biometric



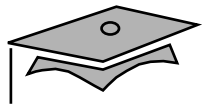
System Security

- Accountability
 - UNIX accounting
 - BSM
 - syslog daemon
 - Quotas



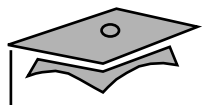
System Security

- Availability
 - Security policy
 - Confidentiality
 - Integrity



Physical Security

- Cables
- Physical devices
- Device environments



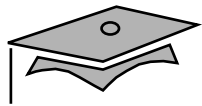
Module 2

Basic System Security



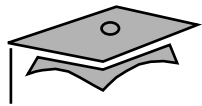
Overview

- Objectives
- Relevance



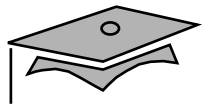
Security Policy

- Appointing a security administrator
- Communicating the security policy and its purpose
- Making the security policy practical
 - Prioritize systems that need security
 - Educate, trust, and suspect users
 - Publish backup and restore strategy
 - Involve senior management



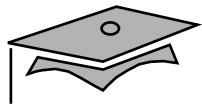
Passwords

- Password secrecy
- Selection of secure passwords
 - Do not use common words, familiar names, or numbers, either backwards or forwards
 - Make it six characters or longer
 - Mix upper- and lowercase letters and use special characters
 - Make it fast to type to reduce *shoulder surfing*
 - Use a mnemonic method to remember a phrase



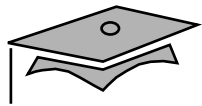
Passwords

- Password aging
 - Change user passwords only when necessary
 - Change superuser passwords periodically
 - Expire guest or temporary passwords immediately
- Automated generation of a password
- Password checking programs



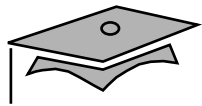
Password and Shadow Files

- The `/etc/passwd` file
 - Is readable by everyone
 - Contains user account information which is a security risk
- The `/etc/shadow` file
 - Is readable only by superuser
 - Contains encrypted password and aging parameters



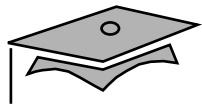
Password Aging and Expiration

- The `passwd` command
 - Restrictions and old password are needed for user operation only.
 - Options control aging parameters.
 - Restrictions are defined in the `/etc/default/passwd` file.



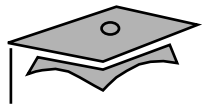
Secure Account Management

- Remember dormant accounts are a favorite target of attackers
- Use `usermod` command to automatically expire accounts
 - `-f` – Option for long periods of inactivity
 - `-e` – Option for a specific date
- Temporarily disable accounts for people on extended leave
- Check for duplicate user ID numbers with `logins -d`



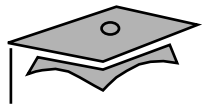
Guest Accounts

- Try to avoid creating guest accounts
- Isolate the computer or partition if possible
- If on the network, use *restricted shell* with minimal access to necessary programs
- Expire account immediately after use
- Use only for untrusted users



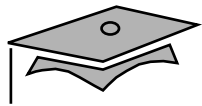
Restricted Shells

- Access limited to only necessary tools for untrusted users
- Configuration
 - Create normal account, but use `/usr/lib/rsh` for shell in `/etc/passwd`
 - Control user's startup files and directories by limiting `PATH` variable settings
 - Create and maintain restricted working directory
 - Refuse to load untested custom software (SUID)



Search Paths and Startup Files

- PATH variable order dependency
- Possible key for Trojan horse



Superuser

Log in as normal user first, then use the su command.

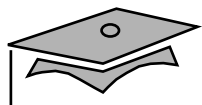
- The su command
 - Changes *effective user ID*, even root
 - Should be used with the full path of `/bin/su`
 - Is logged by default in `/var/adm/sulog`
 - Has its behavior specified in `/etc/default/su`

Consider restricting access to su by limiting execute permission.



EEPROM Security

- Extreme security for physical access to systems
- Attacker needs to be highly skilled
- The `eeeprom` command
- Lost password = no system access; hardware fix



Module 3

UNIX Vulnerabilities



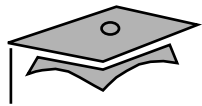
Overview

- Objectives
- Relevance



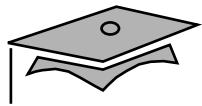
Security of Disk Files

- Backdoors
 - Repeated access
 - Superuser privileges
- Device files
- The `mknod` command
- Character files with creative names
- The `find` command



Denial of Service

- User using more than fair share of resources
- Worms and fork bombs
- Process monitoring and control commands
 - Common – `who`, `ps`, `whodo`, and `kill`
 - Virtual memory – `swap` and `vmstat`
 - System activity – `ps`, `vmstat`, and `sar`
 - Detailed reports – `acctcom` and `lastcomm`

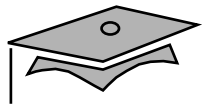


The who Command

- Lists users on the system
- Uses the -a option for expanded listing

Example:

```
# who -a
```

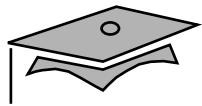


The ps Command

- Displays process status
- Returns the process ID (PID)

Example:

```
# ps -ef
```

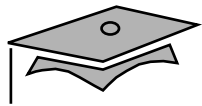


The `whodo` and `w` Commands

- Is similar to `ps` but briefer
- Uses the `-l` option for long format

Example:

```
# whodo -l
```

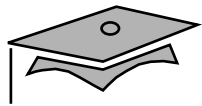


The `kill` Command

- Requires process ID as input
- Uses the `-HUP` or `-KILL` options

Example:

```
# kill -KILL 234
```

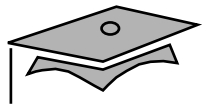


The swap Command

- Uses the `-a` option to display resources
- Uses the `-l` option to list current available swap space

Example:

```
# swap -l
```

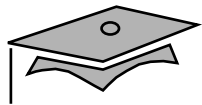


The vmstat Command

- Provides real-time reporting with period parameter

Example:

```
# vmstat 10
```

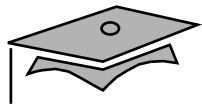


The sar Command

- Reports the utilization of various system resources such as memory, central processing unit, swap space, paging, disk, and others
- Provides real-time reporting with period parameter

Example:

```
# sar -k -o temp 10 5
```



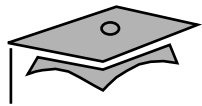
Process Accounting Tools

- `acctcom`
 - Displays detailed reports of users, times, and ports
 - Is used as secondary tool for preliminary monitoring
- `lastcomm`
 - Displays command execution information
 - Displays output in reverse chronological order



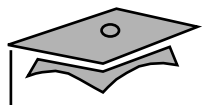
Temporary File Systems (tmpfs)

- Increases performance when creating and destroying multiple temporary files
- Uses virtual memory



Important System Log Files

- `/var/adm/messages`
- `/var/adm/lastlog`
- `/var/adm/loginlog`
- `/var/adm/utmpx` and `/var/adm/wtmpx`
- `/var/adm/acct`
- `/var/adm/sulog`



Module 4

Common Security Cracks



Overview

- Objectives
- Relevance



Common Security Cracks

- Password cracks
- Trojan horses



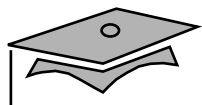
Common Security Cracks

- Worms
- Access control failures
- Data integrity failures
- Denial of service



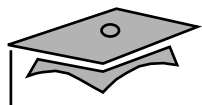
Common Security Cracks

- Logic bombs
- Tools
 - SATAN
 - Crack



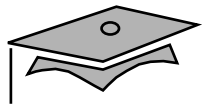
Module 5

Protecting Files and Data



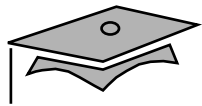
Overview

- Objectives
- Relevance



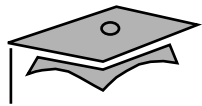
File Permissions

- Review basics with *security* as the focus
 - Owner, group, others
 - Read, write, execute
 - File or directory
- Remember access request rules have no hierarchy
- Monitor SUID / SGID (switch user and group identification) permissions
- Remember sticky bit is obsolete except for directories



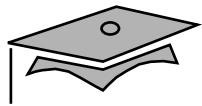
The chmod Command

- Basic permissions
 - Symbolic mode – `#chmod o+w my_file`
 - Absolute mode – `#chmod 761 my_file`
- Extended permissions
 - SUID – `# chmod 4xxx my_file`
 - SGID – `# chmod 2xxx my_file`
 - Sticky – `# chmod 1xxx my_file`



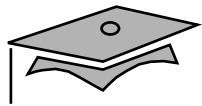
umask – Creation Mask

- Sets permissions on newly created files
- Is controlled in setup file
(`.profile`, `.cshrc`, `.login`)
- Has a default setting in `/etc/skel` which is `022`, giving open access
- Uses `umask 077` for more secure system



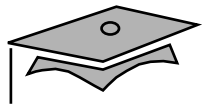
Sticky Bit on Directories

- Protect users' files in otherwise public directory
- Use `chmod 1777` to keep users from deleting each other's files



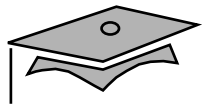
SUID and SGID Programs

- Beware of compiled SUID / SGID programs
 - Do not install a program if it is unknown
- Never install SUID / SGID scripts, they might be altered
- Scan the system for SUID / SGID programs with the `find` command
- Use `mount -o nosuid` to restrict SUID / SGID programs across the network



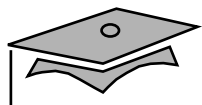
Access Control Lists (ACLs)

- Extended permissions enable more specific control
- The `setfacl` command uses
 - `-m` option for incremental changes
 - `-r` option, which must be used with `-m` option, for results
 - `-s` option for absolute changes; it resets everything
- The `getfacl` command lists extended permissions



Backup / Restore

- Consider full versus incremental backups
- Test backups and restores randomly, periodically, and perform a full restore at year end
- Protect, transport, and retire backup media
- Use *day-zero* backups for comparison
- Maintain an off-site set of backups; beware of the courier transporting them
- Encrypt very sensitive data; use the key strategy
- Perform backups in single-user mode if possible

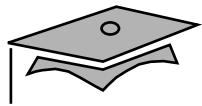


Encrypting Files

- Last line of defense
- The `crypt` command
 - Makes use of symmetric key

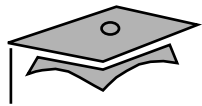
```
% crypt my_passwd < file.orig > file.crypt
```

- Deletes original file
- Uses longer passwords which are more difficult to crack



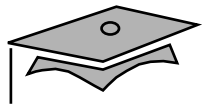
Encrypting Transmissions (SKIP)

- Use SKIP utility, Solaris Server Intranet Extension 1.0
- Build encrypted channel between computers
- Authenticate network packets
- Generate independent keys for each host
- Use SKIP outside of firewalls



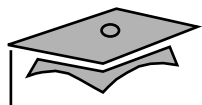
SKIP Commands

- `skiplocal` – Creates, lists, and removes keys
- `skipif` – Enables SKIP daemon
- `skiphost -a` – Causes key pair exchange and tunnel creation
- `skiphost -o` – Enables / disables SKIP for secure transmission



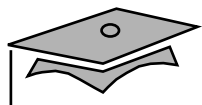
SKIP Advantages

- Provides networked application encryption
- Does not require prior messaging connections
- Is well suited to IP networks because of a stateless protocol
- Provides high availability due to quick recovery without having to renegotiate connections
- Is well suited to uni-directional IP networking such as satellite or cable
- Can be configured in parallel



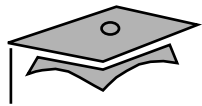
Module 6

Controlling Root Access With sudo



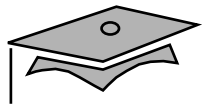
Overview

- Objectives
- Relevance



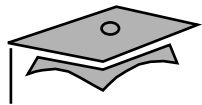
What Is sudo?

- Allows trusted users to perform certain functions as though they were root
 - Root password not required
 - Limited command set to specific users
 - All sudo activity is logged
- Requires additional utilities for installation
 - `gunzip` for precompiled package
 - `pkgadd` (Solaris Operating Environment resident)



sudo Configuration File

- `/usr/local/etc/sudoers`
 - Specifies which commands users may execute
- `/usr/local/sbin/visudo` is used to edit configuration file
 - Provides error checking and file locking

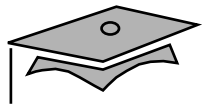


sudo Configuration File

- Basic structure of a rule
 - *user host=commandlist[:host=commands]*
- sudoers file structure example

```
fred          grommit=ALL:wallace=ALL,morepower=ALL
```

```
user1         grommit=/usr/sbin/ufsdump, \
               /usr/sbin/ ufsrestore \
               :wallace=/usr/sbin/ufsdump, \
               /usr/sbin/ufsrestore \
```



Using sudo Commands

- Precede the command to be executed with sudo

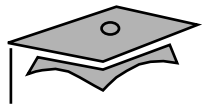
```
/usr/local/bin/sudo /usr/sbin/halt
```

- Print out the current version of sudo

```
/usr/local/bin/sudo -V
```

- Print out the commands a user may execute

```
/usr/local/bin/sudo -l
```



sudo Aliases

- User aliases

User_Alias SENIOR=shughes, tbussart, hagerty

- Command aliases

Cmnd_Alias PRINT=/usr/etc/lpc, /usr/ucb/lprm

- Host aliases

Host_Alias SERVERS=everest, denali, annapurna

- User specification

SENIOR ALL=ALL

JUNIOR ALL=ALL, !NET



Enabling syslogd Logging for sudo

- Edit the `/etc/syslog.conf` file and add an entry to save `sudo` messages
- Create the log file for `syslogd` to log to
- Restart the `inetd` daemon



Module 7

Secure Shell



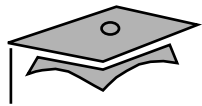
Overview

- Objectives
- Relevance



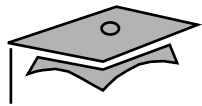
Describing the Secure Shell (ssh)

- Secure replacements for Berkeley "r" commands (rcp, rlogin, rsh)
- Rivest-Shamir-Adelman (RSA) public key cryptography
- Source available from `ftp://ftp.cs.hut.fi/pub/ssh`



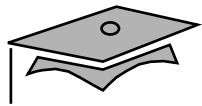
Working With the sshd Daemon

- Has the server daemon listen for ssh requests
- Generates the RSA key before the daemon starts
- Is started by `/etc/rc.local` or equivalent
- Supports use of `.rhosts` and `hosts.equiv`, but is *not* recommended



Installing the Secure Shell

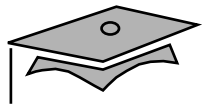
- Build program with C compiler and make
- Locate in `/usr/local/bin`, the default directory
- Use primary executables
 - `sshd` – Server daemon
 - `ssh` – Client program (same as `slogin`)
 - `scp` – Secure copy
 - `ssh-keygen` – RSA key generator



Configuring the Secure Shell

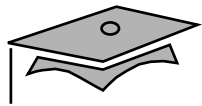
- `sshd_config` – Server configuration file
 - Default settings suitable for most situations
- `ssh_config` – Client configuration file
 - Default file contains only comments and is suitable for most situations

These files must exist in `/etc` before the daemon can start.



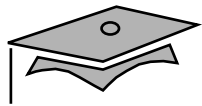
Creating the Server Keys

- Is created automatically if it is installed using `make install`
- Is created manually using `ssh-keygen` command
- Is stored in the `/etc` directory under the following names:
 - `ssh_host_key` – Private portion
 - `ssh_host_key.pub` – Public portion
- Must exist prior to starting `sshd` server daemon
- Must start server daemon by using `sshd` command



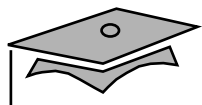
Starting the Secure Shell From the Client

- Log in as user
- Run `ssh` command followed by the remote host name
- Remember, the first time `ssh` runs it creates:
 - `.ssh` directory in user's home directory
 - `known_hosts` file for future use
 - `random_seed` file for session use



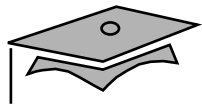
Creating Alternative Configurations

- Disable `rcp`, `rlogin`, `rsh`, and replace with `ssh` commands for consistent security
- Use package's flexible configuration options (see man page)



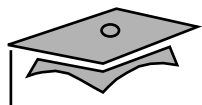
Module 8

Remote Access and Authentication Services



Overview

- Objectives
- Relevance



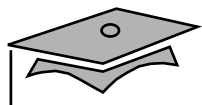
Remote Access System Files

- `/etc/nodename`
- `/etc/hostname.XX0`
- `/etc/inet/hosts`
- `/etc/net/ticlts/hosts`
- `/etc/net/ticots/hosts`
- `/etc/net/ticotsord/hosts`
- `/etc/defaultdomain`
- `/etc/resolv.conf`



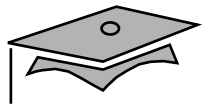
Restricting Connectivity Commands and Services

- Restricting connectivity commands
- Restricting networking services



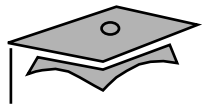
Berkeley “r” Commands

- The `rlogin` command
- The `rsh` command
- The `rcp` command



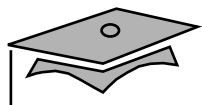
Network Authentication – rlogin, rcp, and rsh

- The ~user/.rhosts file



Netgroups

- NIS or NIS+
- The `/etc/netgroup` file
- Member definition



Netgroups

- Match all
- Match none



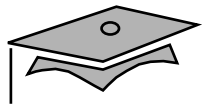
Authentication Services Used With Secure RPC

- Diffie-Hellman (DH)
- Diffie-Hellman Key Agreement Protocol
- Diffie-Hellman authentication



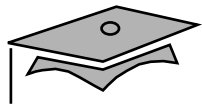
Authentication Services Used With Secure RPC

- Kerberos V4



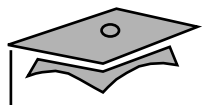
What Is PAM?

- Allows authentication technologies to be “plugged in” without having to change system entry services such as login, ftp, telnet, and so on
- Integrates with UNIX, Kerberos, RSA, smart cards, and GSS-API DCE
- Uses four module types:
 - Authentication
 - Account management
 - Session management
 - Password management

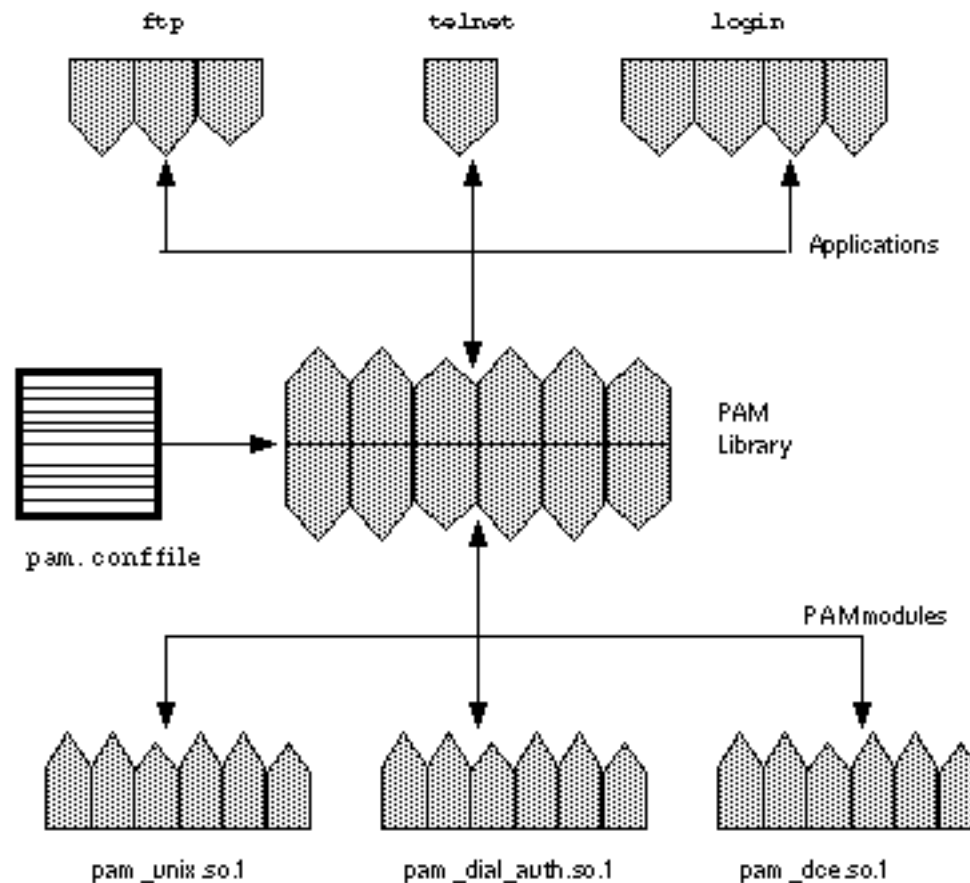


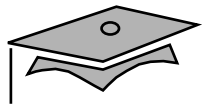
PAM Runtime Module Types

- Module types
 - Authentication modules
 - Account modules
 - Session modules
 - Password modules
 - The `dial_auth` module
 - The `rhosts_auth` module



PAM Runtime Module Types





PAM Configuration File

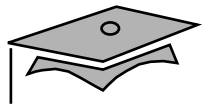
- Configuration file syntax is:

```
login    auth required    /usr/lib/security/ \
pam_unix.so.1
```

```
su       auth requisite   /usr/lib/security/ \
pam_inhouse.so.1
```

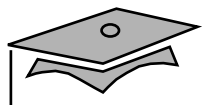
```
su       auth required    /usr/lib/security/ \
pam_unix.so.1             debug
```

- Syntax error causes the file to not be loaded



PAM Configuration File

- Configuration file syntax
- Control flags
 - requisite
 - required
 - optional
 - sufficient



The /etc/pam.conf File

```
login auth required /usr/lib/security/  
pam_unix.so.1
```

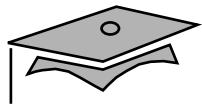
```
login auth required /usr/lib/security/  
pam_dial_auth.so.1
```

```
rlogin auth sufficient /usr/lib/security/  
pam_rhost_auth.so.1
```

```
rlogin auth required /usr/lib/security/  
pam_unix.so.1
```

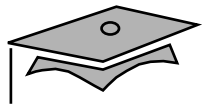
```
. . .
```

```
. . .
```



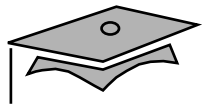
The /etc/pam.conf File

- *required* – Authentication must succeed for each module.
- *sufficient* – The second entry is ignored if the first entry succeeds.
- *OTHER* – It serves as a catchall.



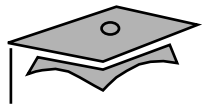
The `/etc/pam.conf` File

- *OTHER* is used to simplify `/etc/pam.conf`.
- `/usr/lib/security/` is prepended if a relative path is used.
- Absolute path is required when modules are not in default directory.
- You can use `optional` with `required` to permit login passwords to be different.



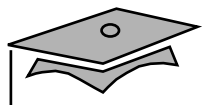
Configuring PAM

- Module usage
- OTHER module
- Module order
- Necessary control flags
- PAM module addition



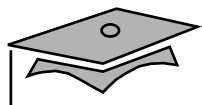
Preventing Unauthorized Remote Access With PAM

- Stop `~/ .rhosts` from being read
- Disable `rsh`
- Initiate PAM error reporting



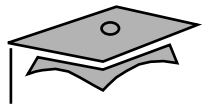
Module 9

Using Secure NFS



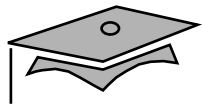
Overview

- Objectives
- Relevance



Secure NFS

- Time share secure because of terminal authentication
- NFS authenticates file request, but not user
- Impersonation possible with `SU` command
- Data eavesdropping problems
- Data integrity compromised; more serious problem
- Secure NFS uses *Secure RPC* (remote procedure call) authentication as foundation



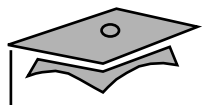
Secure RPC

- *Secure Remote Procedure Call*
- Data encryption standard (DES) authentication
- Credential and verifier sent by client to server
- Server returns verifier

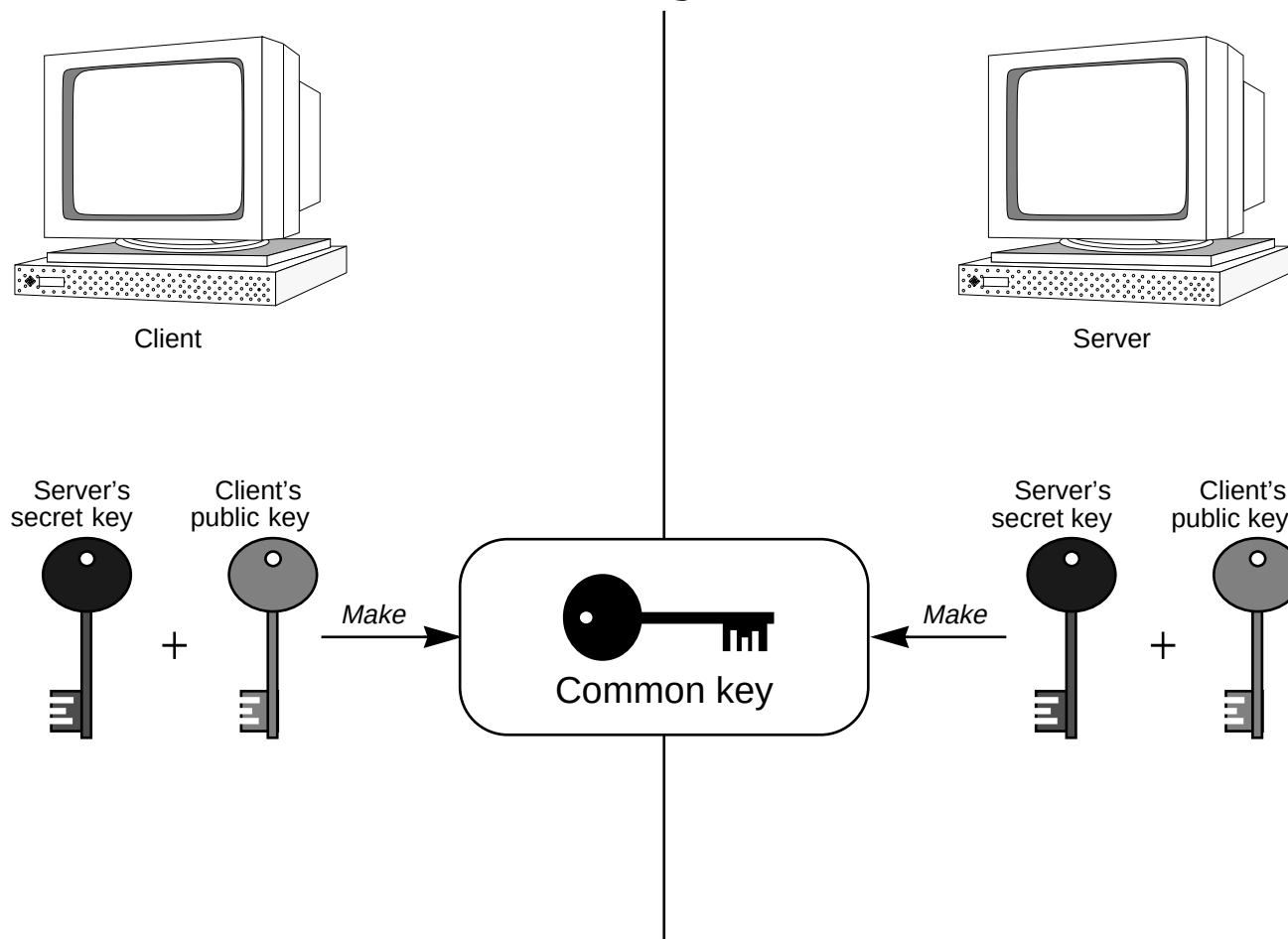


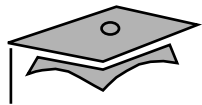
DES Authentication Protocol

- Diffie-Hellman public-key cryptography
- Authentication timestamped to prohibit later reruns
- Conversation key generated is host and time dependent
- NIS+ tables used to hold public and secret keys

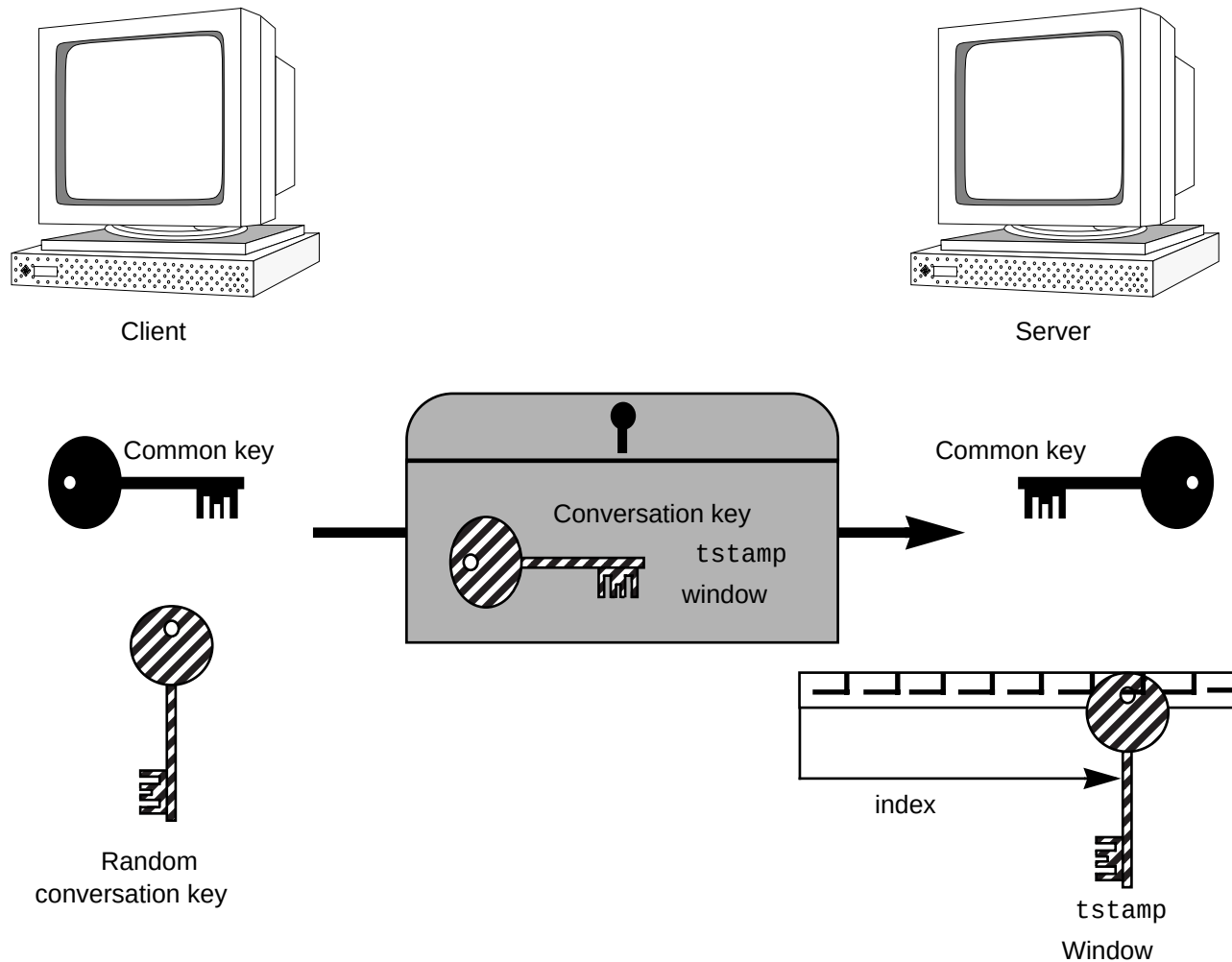


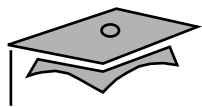
Common Key Creation



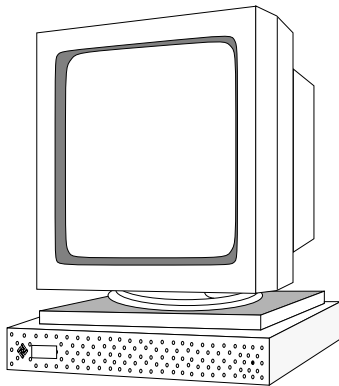


Conversation Key Generation

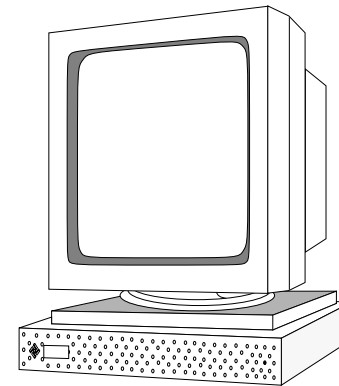




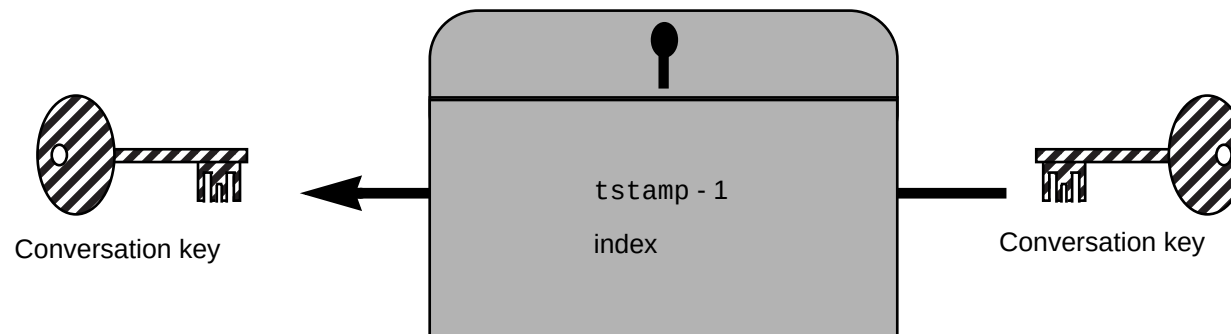
Conversation Key Decryption

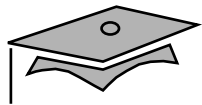


Client

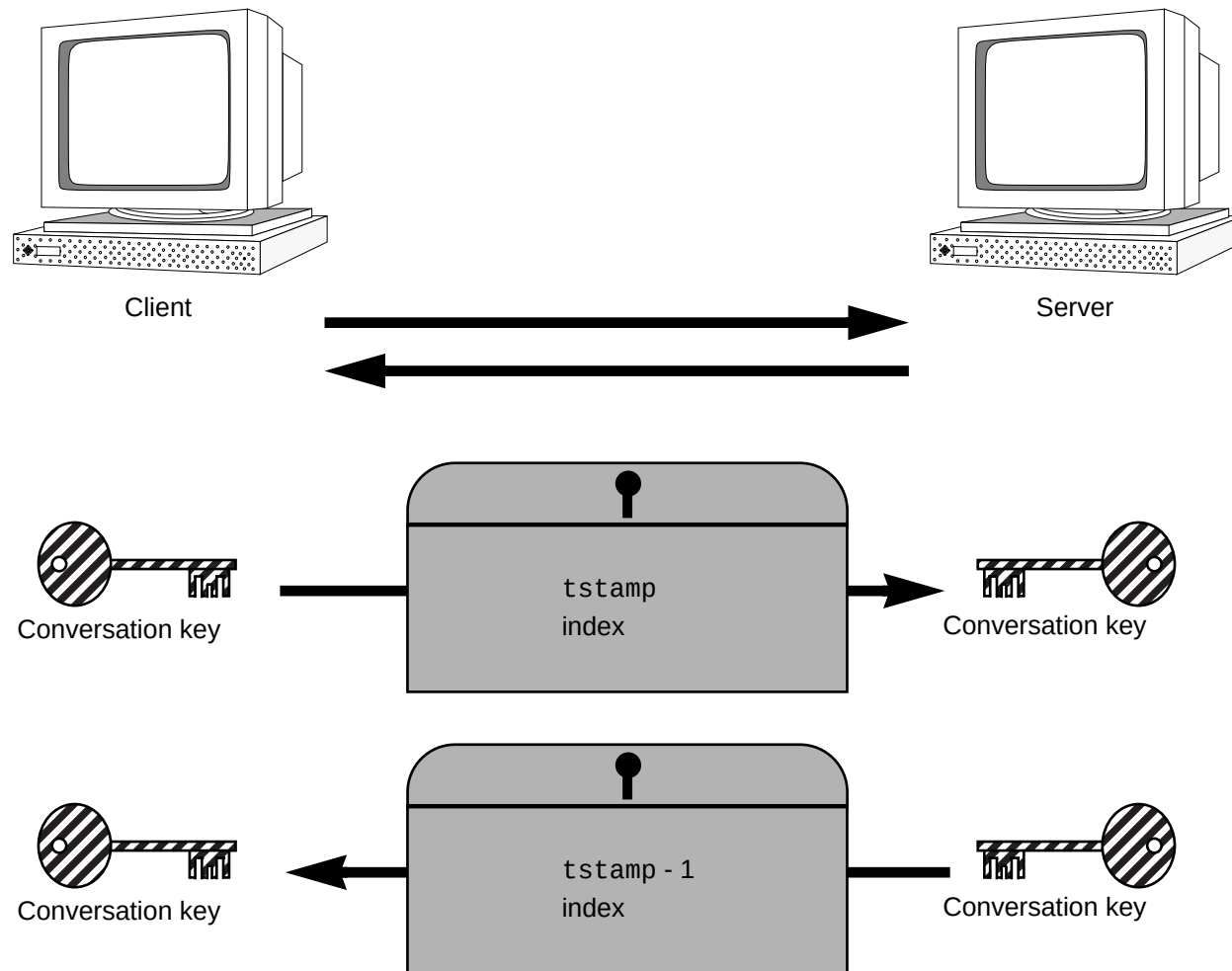


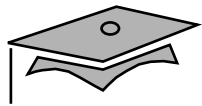
Server





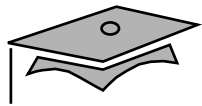
Secure RPC / NFS Enabled





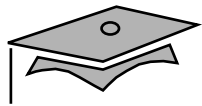
Secure NFS Setup

1. Assign domain name to all hosts.
2. Establish public and secret keys on clients.
3. Verify name service and key server is running.
4. Log in with password.
5. Add secure option to share entry in `/etc/dfs/dfstab`.
6. Add secure option to mount entry in `/etc/auto_master`.



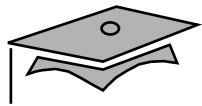
Problems With Secure NFS

- Server crashes will destroy keys; this opens access.
- Diskless clients are not secure.
- Accounts with no password are blocked.
- The su command for system administrators is not always available due to key access.



The `fsirand` Command

- Remember, new devices have predictable inode generation numbers.
- Use `fsirand` command to generate random numbers for inodes when adding new devices.



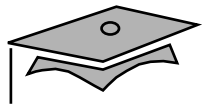
Module 10

Solaris Operating Environment syslog



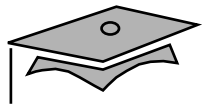
Overview

- Objectives
- Relevance



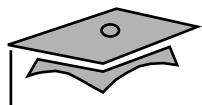
Why Use syslog?

- Provides easier messaging for application writers
- Enables applications to rely on it
- Creates a typical log file entry contains
 - Date
 - Hostname
 - Daemon
 - Protocol
 - Internet protocol address



Configuring `/etc/syslog.conf`

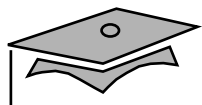
- Tab-separated entries – the selector and action fields
 - `facility.level; facility.level<TAB>action`
- Selector field – `facility.level; facility level`
 - Facility – `auth`, `daemon`, `*`, and so on
 - Level – `none`, `debug`, `emerg`, and so on
- Action field – Target for message
- Sample entry – `*.emerg <TAB> *`



Using Different syslog Severity Levels

- Different severity levels for events
- Not all available severity levels are used by every program

For example, `inetd` supports `syslog` messaging when the `trace` option is used. Only the `notice` severity level is supported.



Using syslog With telnet

- Have the daemon facility report for telnet
- Edit S72inetsvc and add trace (t) option for inetd

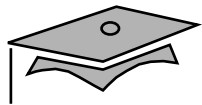
```
# grep 'inetd -s' /etc/rc2.d/S72inetsvc
```

```
/usr/sbin/inetd -s -t
```

```
# grep '^daemon' /etc/syslog.conf
```

```
daemon.notice      /var/adm/messages
```

```
#
```

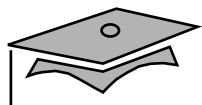


Using syslog With ftp

- Have the daemon facility report for ftp
- Edit `/etc/inet/inetd.conf` to resemble

```
ftp stream tcp nowait root \  
/usr/sbin/in.ftpd in.ftpd -dl
```

- Restart `inetd`
- Have `syslog` log incoming ftp entries

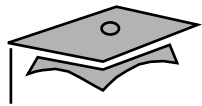


The logger Utility

- Enables a system administrator to add one-line entries to the system log file

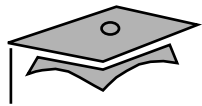
```
logger [ -i ] [ -f file ] [ -p priority ] [ -t tag ] [ message ]
```

- Uses command options
 - *-f file*
 - *-i*
 - *-p priority*
 - *-t tag*
 - *message*



Using syslog to Log Messages to a Remote Host

- Advantages of centralized logging include:
 - Logs are on one server providing all information while troubleshooting complex problems
 - Backups of log information are run from one server instead of several
 - Real-time log monitoring for multiple hosts is enabled

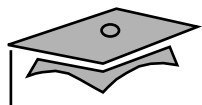


Configuring and Debugging Logging to Remote Hosts

- Edit `/etc/syslog.conf` and place an entry in the following form:

auth.notice *@loghost*

- Restart `inetd`
- Troubleshoot `syslog` problems
 - Stop the `syslogd` daemon
 - Run `syslogd` in debug mode
 - Use the command `/usr/sbin/syslogd -d`



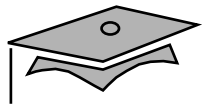
Module 11

Basic Security Module (BSM)



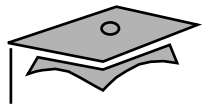
Overview

- Objectives
- Relevance



Basic Security Module (BSM) Auditing

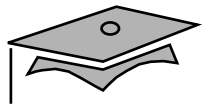
- Is *C2 level security* auditing compliant
- Logs high-detail, low-level event activities
- Requires maintenance
- Uses audit classes which group events that are logged
- Uses audit records
- Is configured with `/etc/security/audit_control`
- Uses `/etc/security/audit_user` to qualify audit data for specific users



Audit Data

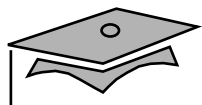
- Binary data is contained in `/var/audit` directory in time-stamped file
- `auditreduce` command selects record types for examination
- `praudit` command displays data in readable form
- `auditreduce` and `praudit` combine to create reports

```
# auditreduce -u <user> -c <audit flag> | praudit
```



Major Components of Auditing

- `/etc/security/audit_control`
 - Contains audit flags that control the type of audit records that will be logged
- `/etc/security/audit_user`
 - Determines what gets audited at user level beyond system defaults
- `auditd` daemon
 - Responsible for creating and maintaining the audit trail



Auditing Startup

The audit feature is enable once `auditd` is started.

- To enable auditing

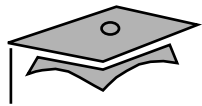
```
# /etc/security/bsmconv
```

```
# init 6
```

- To disable auditing

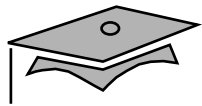
```
# /etc/security/bsmunconv
```

```
# init 6
```



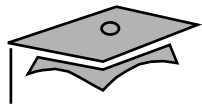
Device Allocation

- Minimizes the security risks that are associated with the use of various I/O devices (tape drives, diskette drives, and so forth).
- Prevents simultaneous access to an allocatable device
- Prevents unauthorized extrapolation of information from an allocatable device or driver's internal storage
- Prevents a user from reading a tape just written by another user before the first user has removed the tape from the drive



Device Allocation Files

- `/etc/security/device_allocate`
 - Contains the mandatory access control information about each physical device managed by the device-allocation mechanism
- `/etc/security/device_maps`
 - Defines the device-special file mappings for each device



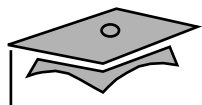
User Commands

- `allocate`
 - Manages the ownership of devices
- `deallocate`
 - Disables user's access to that device
- `list_devices`
 - Lists all of the allocatable devices defined
- `dminfo`
 - Provides information from the `/etc/security/device_maps` file



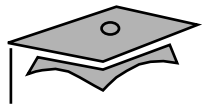
Module 12

Automated Security Enhancement Tool (ASET)



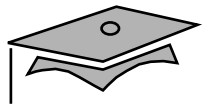
Overview

- Objectives
- Relevance



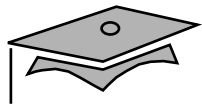
What Is ASET?

- Is an automated program that checks common security problems
- Provides different levels of control depending on needs
 - *Low* – Reports general problems; minor file changes made
 - *Medium* – Reports problems, restricts system access
 - *High* – Changes system files for minimal access
- Is part of a security policy



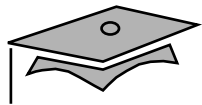
The aset Command

- The `/usr/aset/aset` file is used to start the utility.
- The `-l` option controls the security level of the list of *tasks*.
 - `low` – Default, low level
 - `med` – Medium level
 - `high` – High level
- Tasks are customize in `/usr/aset/tasks` files.
- Progress of `aset` process is checked with `taskstat`.



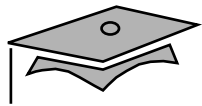
Interactive and Periodic Modes

- Interactive
 - Run from command line
 - Use for initial setup
- Periodic
 - Use -p option
 - Add entry to crontab for periodic jobs
 - Control schedule in `/usr/aset/asetenv`



ASET Reports

- A file for each task is in
`/usr/aset/reports/latest-/* .rpt .`
- The directory named `latest` contains the most recent reports.
- Dated directories contain old reports.
- Reports need review and action.



Security Level Changes

- Use `-l` option again with a different level selection
- Disable ASET with `/usr/aset/aset.restore`
 - Restore archive files from initial setup
 - Remove `/etc/crontab` entry if it was configured
- Fine-tune file settings using `task tune.*` files
 - Use them to better understand what `aset` does
 - Edit them to customize file permissions and settings



Module 13

SATAN and Courtney



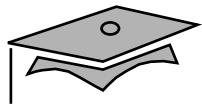
Overview

- Objectives
- Relevance



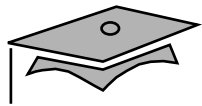
What Is SATAN?

- It examines network services
- It is to network services what ASET is to system file configurations



Utilities for SATAN

- Many additional applications are required by SATAN:
 - gzip and gunzip
 - Web browser
 - Perl Version 5.000
 - C compiler
 - make



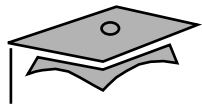
Procuring a Web Browser

- Use Netscape Navigator™
- Uncompress
- Unarchive
- Run the install script
- Add netscape to the search path



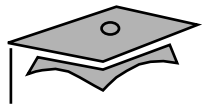
Testing the Web Browser Installation

- Start the browser
- Remove Perl helpers



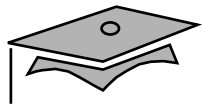
Utilities for SATAN

- Configure the Web browser
 - Change the default fonts
 - Procure, install, and test Perl Version 5.000 or later



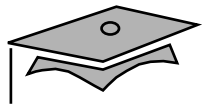
Procuring a C Compiler

- Procure
- Uncompress
- Install package
- Create link to cc
- Test the compiler



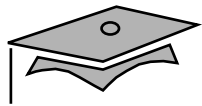
Procuring make

- Part of the Solaris Developers installation
- Included in the SUNWsprt package
- Needs `/usr/ccs/bin` in the path statement



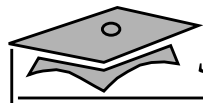
Procuring and Installing SATAN

- Obtain from <http://www.fish.com/satan/>
- Uncompress
- Unarchive
- Run the `reconfig` script



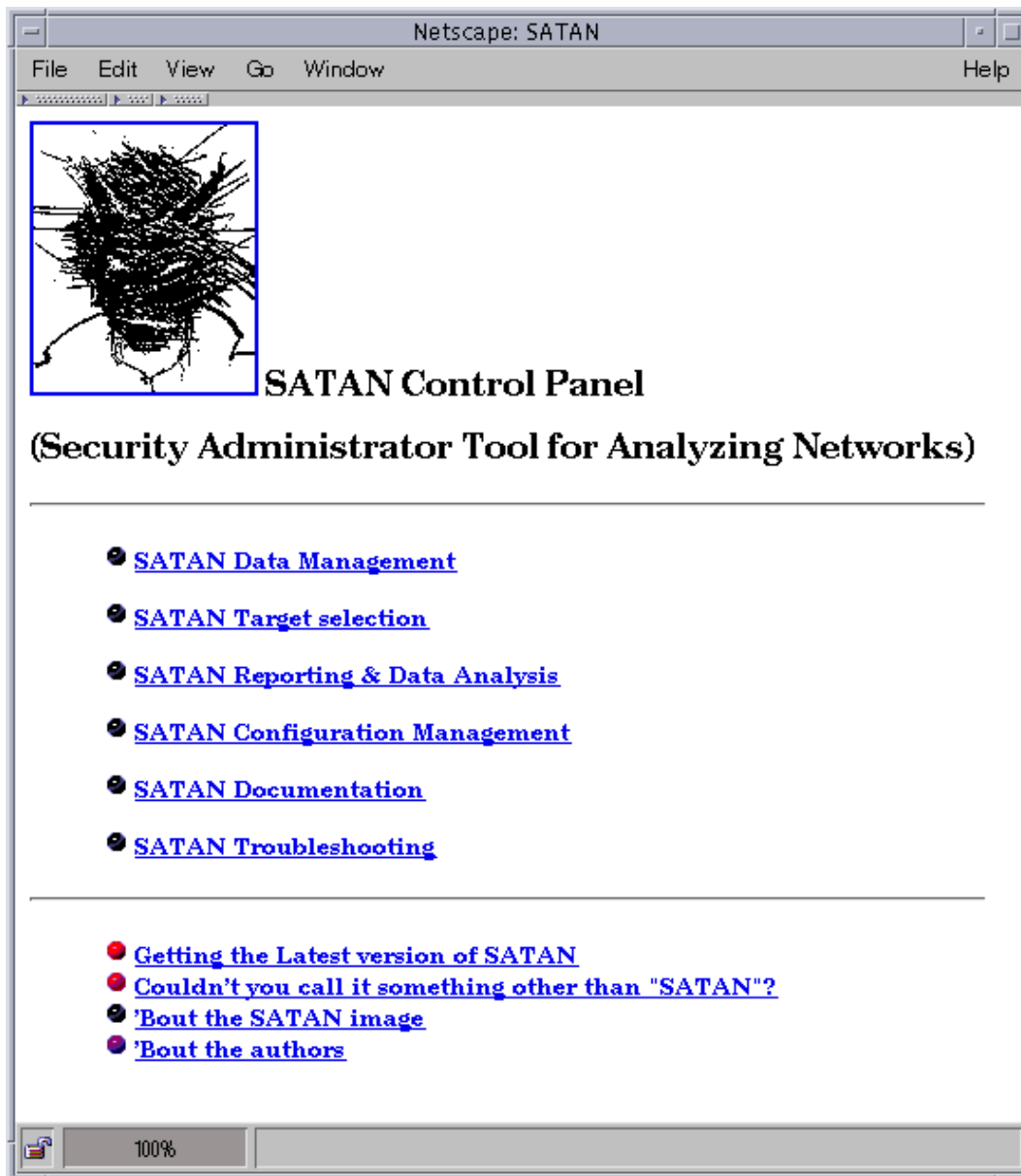
Installing and Configuring SATAN

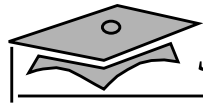
- Use # **make sunos5**
- Edit the `satan.cf` file
- Adjust the X server access control



Using SATAN

- # `./satan`





Using SATAN

- Change Primary Target selection
- Change Scanning Level selection

Netscape: SATAN target selection

File Edit View Go Window Help

 **SATAN target selection**

Primary target selection

Primary target host or network, e.g. verdun:

☐ Scan the target host only.

☒ Scan all hosts in the primary (i.e. the target's) subnet.

Scanning level selection

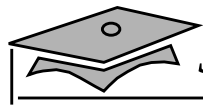
Should SATAN do a light scan, a normal scan, or should it hit the (primary) target(s) at full blast?

☐ Light

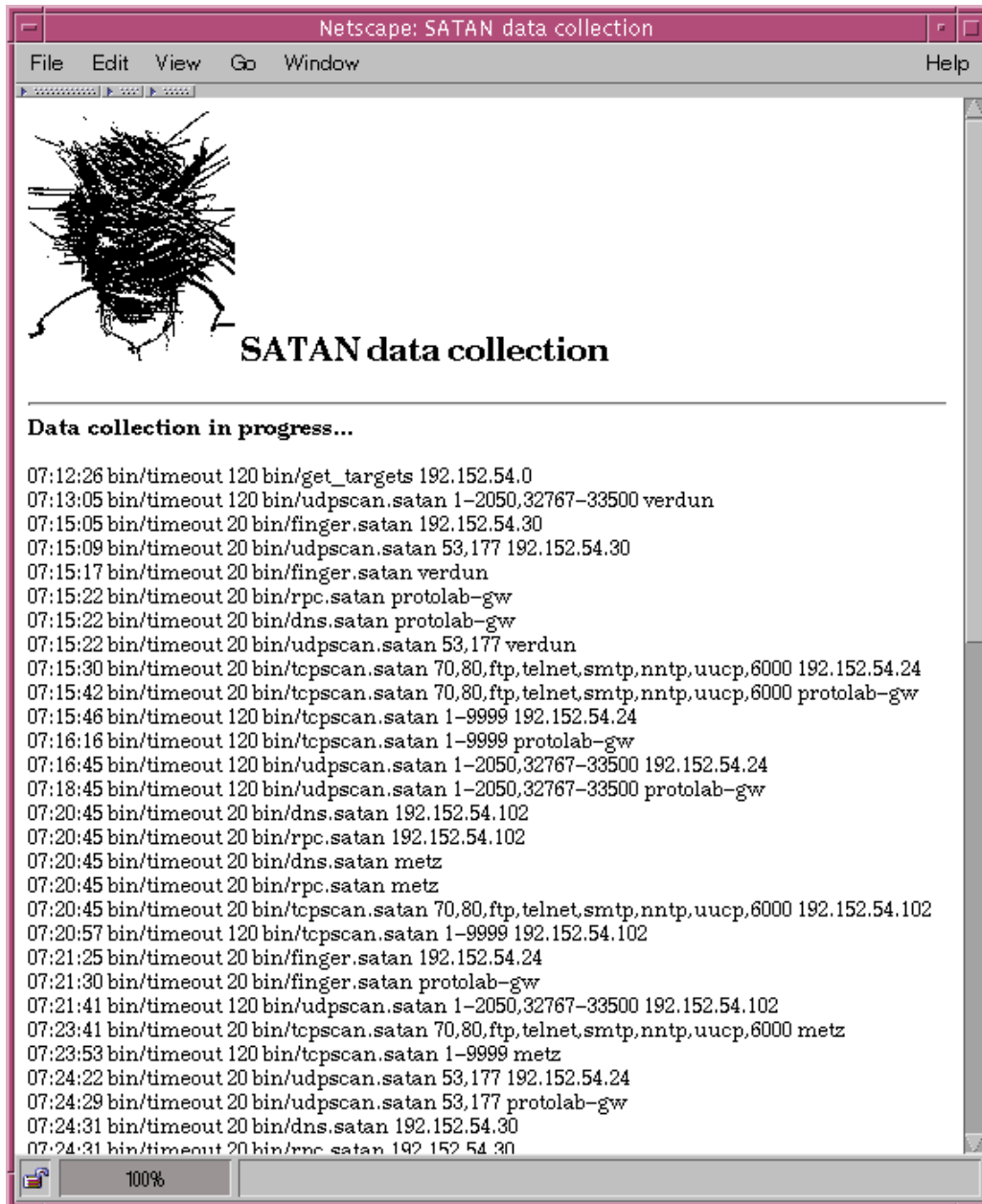
☐ Normal (may be detected even with minimal logging)

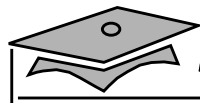
☒ Heavy (error messages may appear on systems consoles)

- Start the scan



Using SATAN





Using SATAN

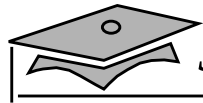
- Completed data collection

```
07:24:29 bin/timeout 20 bin/udpscan.satan 53,177 protolab-gw
07:24:31 bin/timeout 20 bin/dns.satan 192.152.54.30
07:24:31 bin/timeout 20 bin/rpc.satan 192.152.54.30
07:24:32 bin/timeout 120 bin/udpscan.satan 1-2050,32767-33500 metz
07:26:32 bin/timeout 20 bin/dns.satan 192.152.54.24
07:26:32 bin/timeout 20 bin/rpc.satan 192.152.54.24
07:26:32 bin/timeout 20 bin/finger.satan 192.152.54.102
07:26:38 bin/timeout 20 bin/tcpscan.satan 70,80,ftp,telnet,smtp,nntp,uucp,6000 192.152.54.30
07:26:50 bin/timeout 120 bin/tcpscan.satan 1-9999 192.152.54.30
07:27:20 bin/timeout 20 bin/rpc.satan verdun
07:27:20 bin/timeout 20 bin/dns.satan verdun
07:27:20 bin/timeout 120 bin/udpscan.satan 1-2050,32767-33500 192.152.54.30
07:29:21 bin/timeout 20 bin/finger.satan metz
07:29:24 bin/timeout 20 bin/udpscan.satan 53,177 192.152.54.102
07:29:31 bin/timeout 20 bin/tcpscan.satan 70,80,ftp,telnet,smtp,nntp,uucp,6000 verdun
07:29:42 bin/timeout 20 bin/udpscan.satan 53,177 metz
07:29:49 bin/timeout 120 bin/tcpscan.satan 1-9999 verdun
07:30:06 bin/timeout 20 bin/ftp.satan 192.152.54.102
07:30:07 bin/timeout 20 bin/rusers.satan metz
07:30:07 bin/timeout 20 bin/xhost.satan -d 192.152.54.102:0 192.152.54.102
07:30:07 bin/timeout 20 bin/xhost.satan -d 192.152.54.30:0 192.152.54.30
07:30:07 bin/timeout 20 bin/ftp.satan metz
07:30:09 bin/timeout 20 bin/xhost.satan -d 192.152.54.24:0 192.152.54.24
07:30:09 bin/timeout 20 bin/rusers.satan 192.152.54.30
07:30:09 bin/timeout 20 bin/rusers.satan 192.152.54.24
07:30:10 bin/timeout 20 bin/xhost.satan -d metz:0 metz
07:30:10 bin/timeout 20 bin/rusers.satan protolab-gw
07:30:11 bin/timeout 20 bin/ftp.satan 192.152.54.30
07:30:12 bin/timeout 120 bin/nfs-chk.satan -t 10 192.152.54.30
07:30:12 bin/timeout 20 bin/ftp.satan 192.152.54.24
07:30:12 bin/timeout 20 bin/ftp.satan protolab-gw
07:30:13 bin/timeout 20 bin/rusers.satan verdun
07:30:13 bin/timeout 20 bin/xhost.satan -d verdun:0 verdun
07:30:13 bin/timeout 120 bin/nfs-chk.satan -t 10 protolab-gw
07:30:14 bin/timeout 20 bin/rusers.satan 192.152.54.102
07:30:14 bin/timeout 20 bin/showmount.satan 192.152.54.30
07:30:14 bin/timeout 20 bin/ftp.satan verdun
07:30:14 bin/timeout 20 bin/showmount.satan protolab-gw
07:30:15 SATAN run completed
```

Data collection completed (6 host(s) visited).

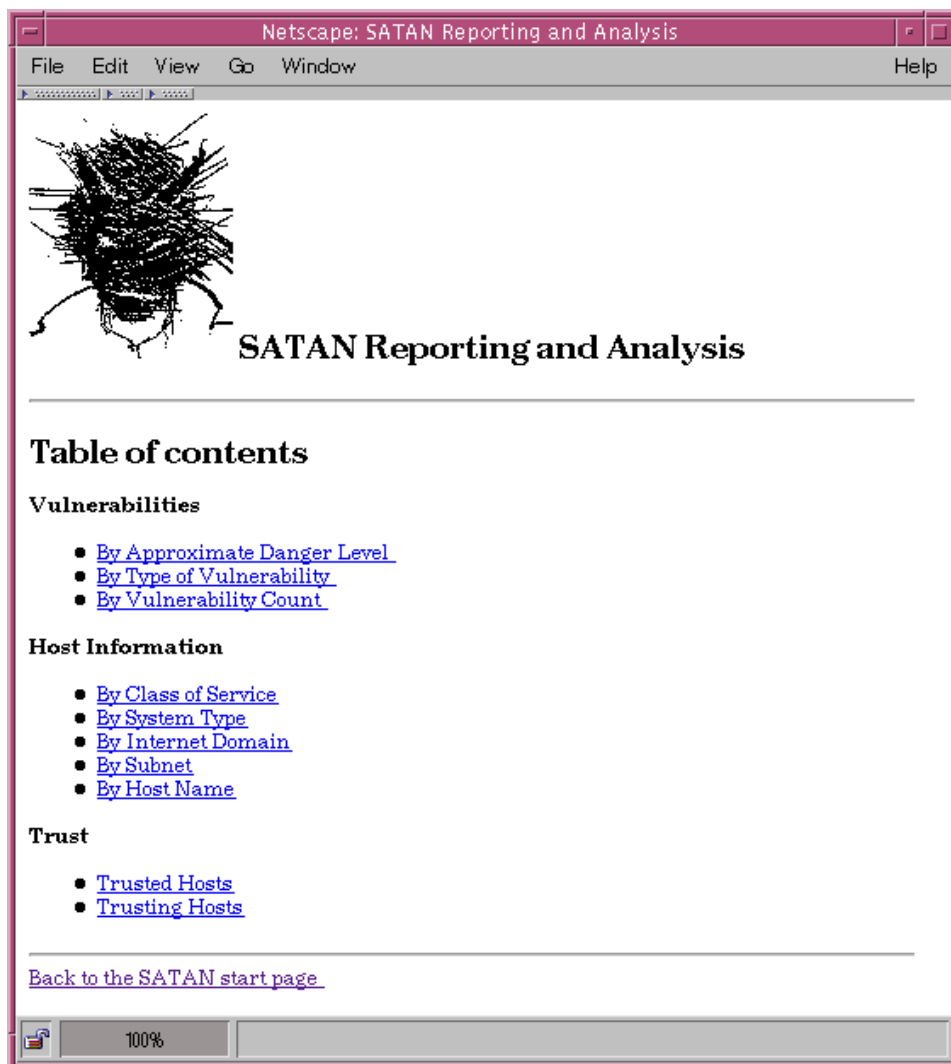
[Back to the SATAN start page](#) | [Continue with report and analysis](#)

- Continue with report and analysis

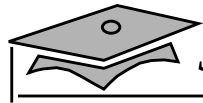


Using SATAN

- Vulnerabilities
- Host information
- Trust

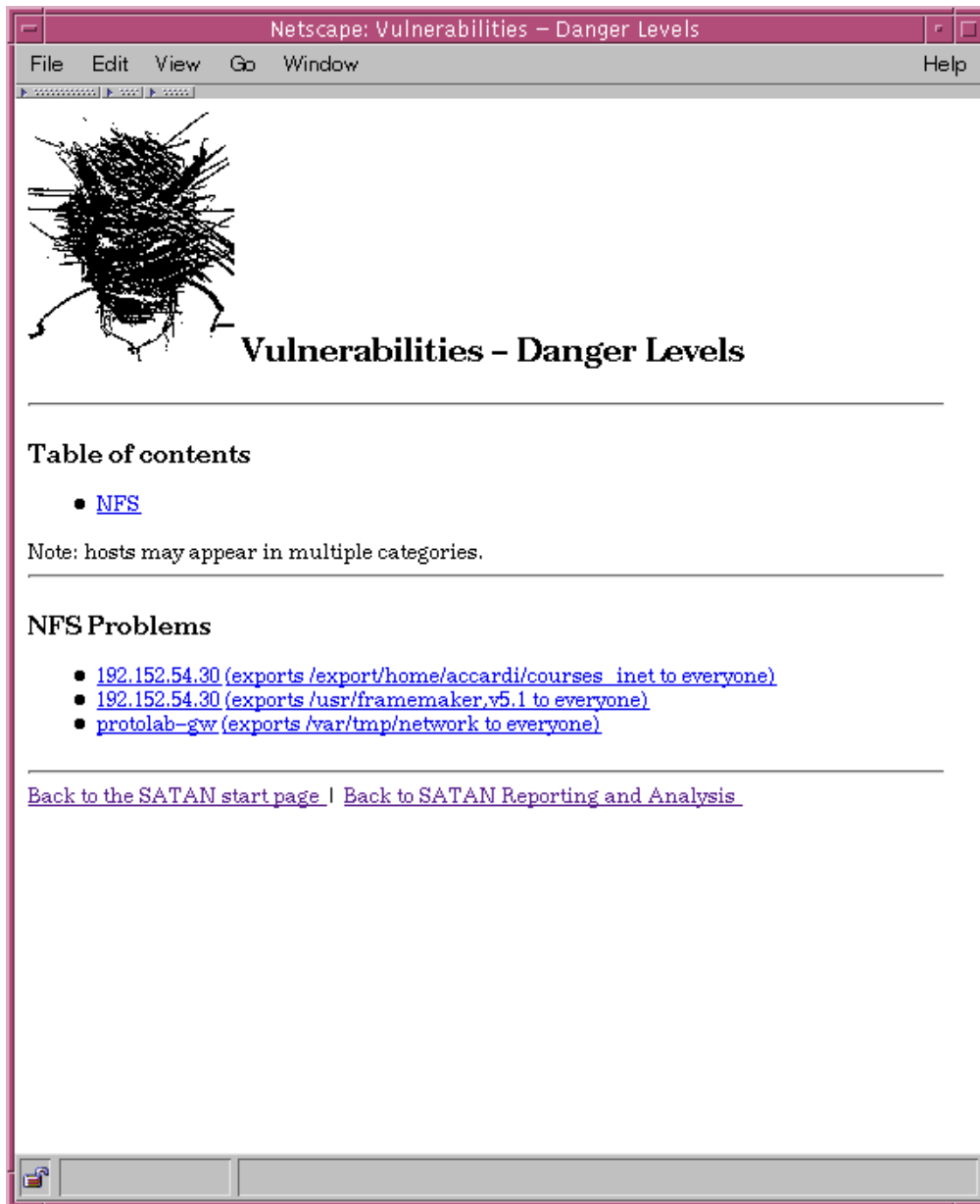


- Click By Approximate Danger Level

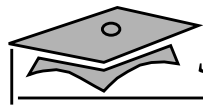


Using SATAN

- Found NFS™ problems

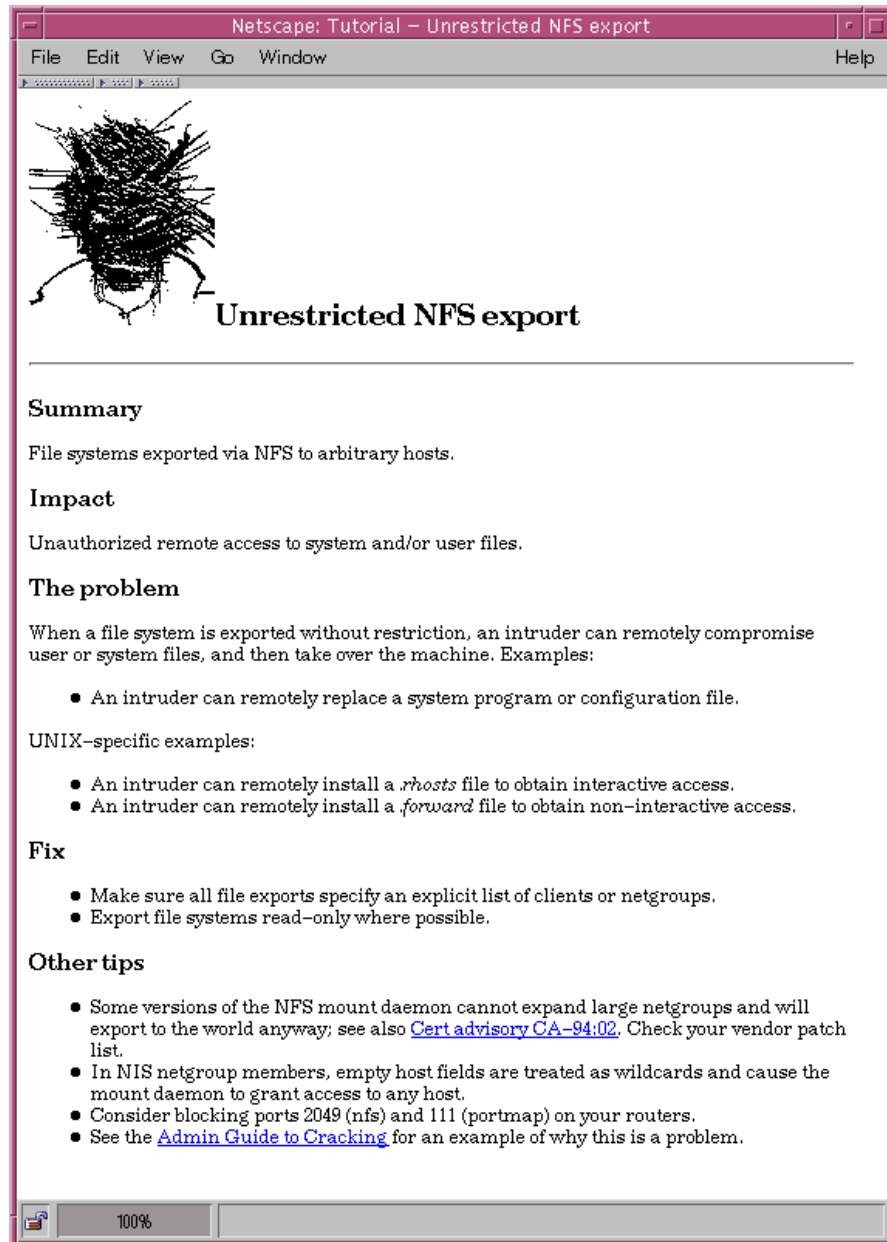


- Click NFS Problems

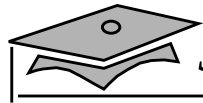


Using SATAN

- Problem is unrestricted NFS export

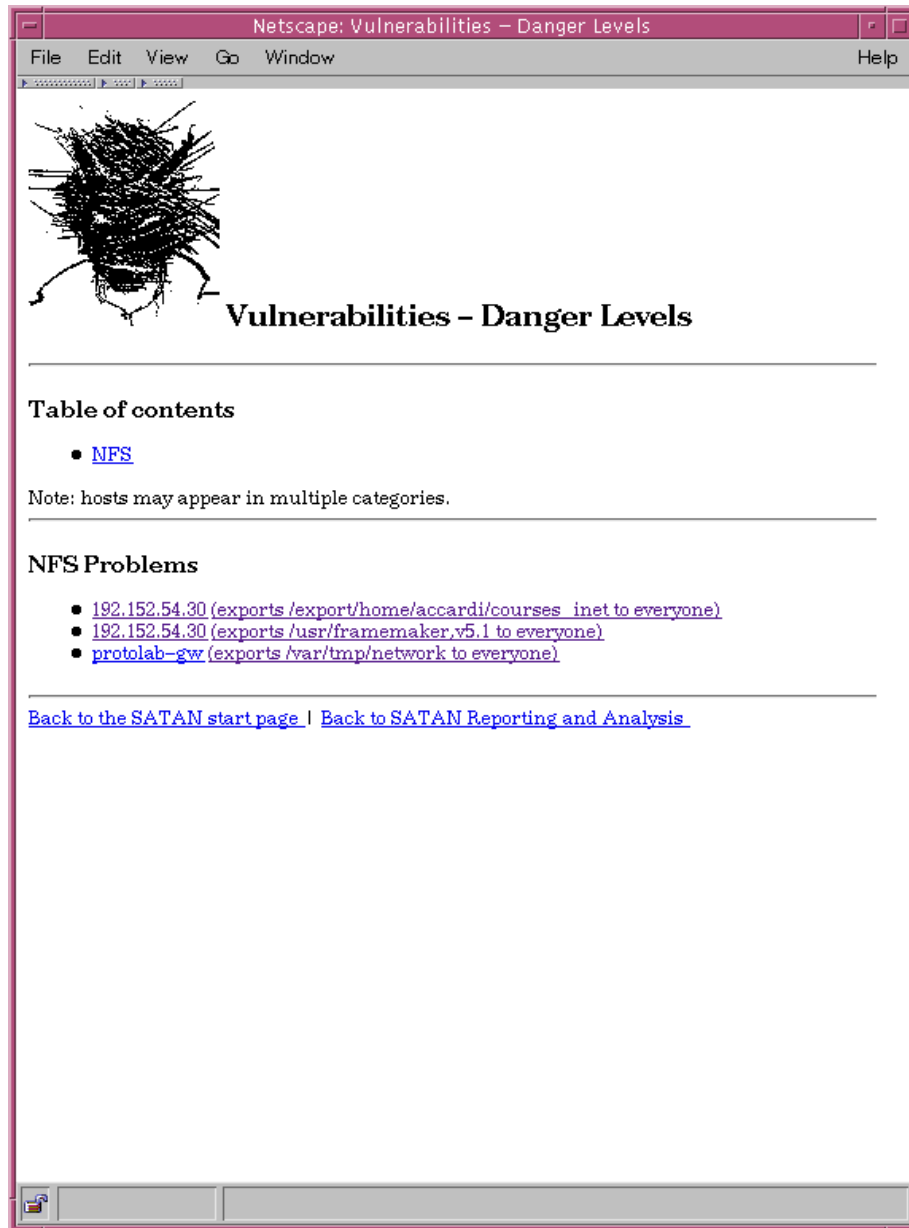


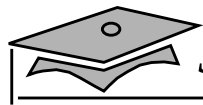
- Right click to go back



Using SATAN

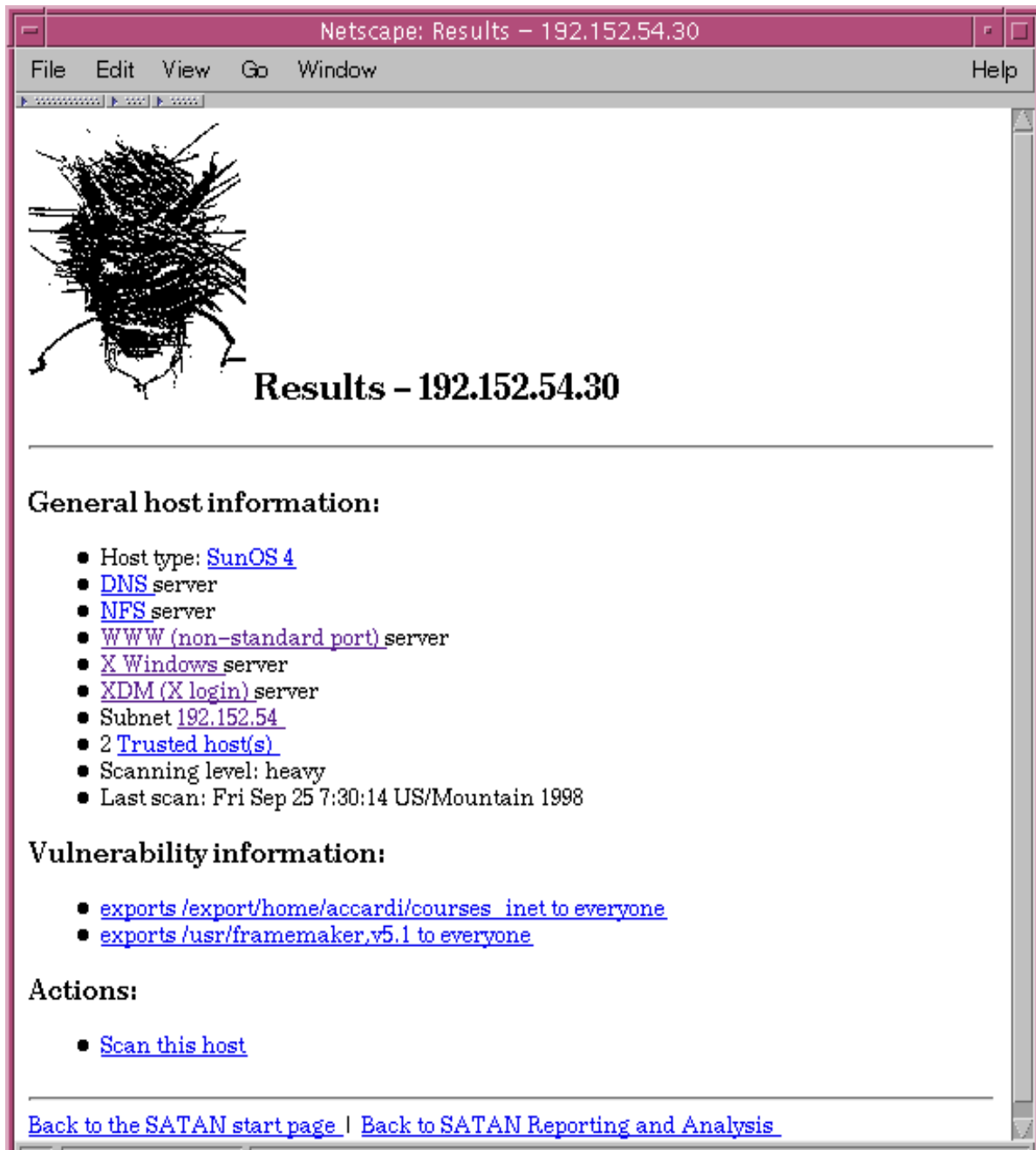
- Click on 192.152.54.30

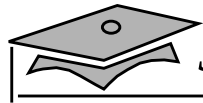




Using SATAN

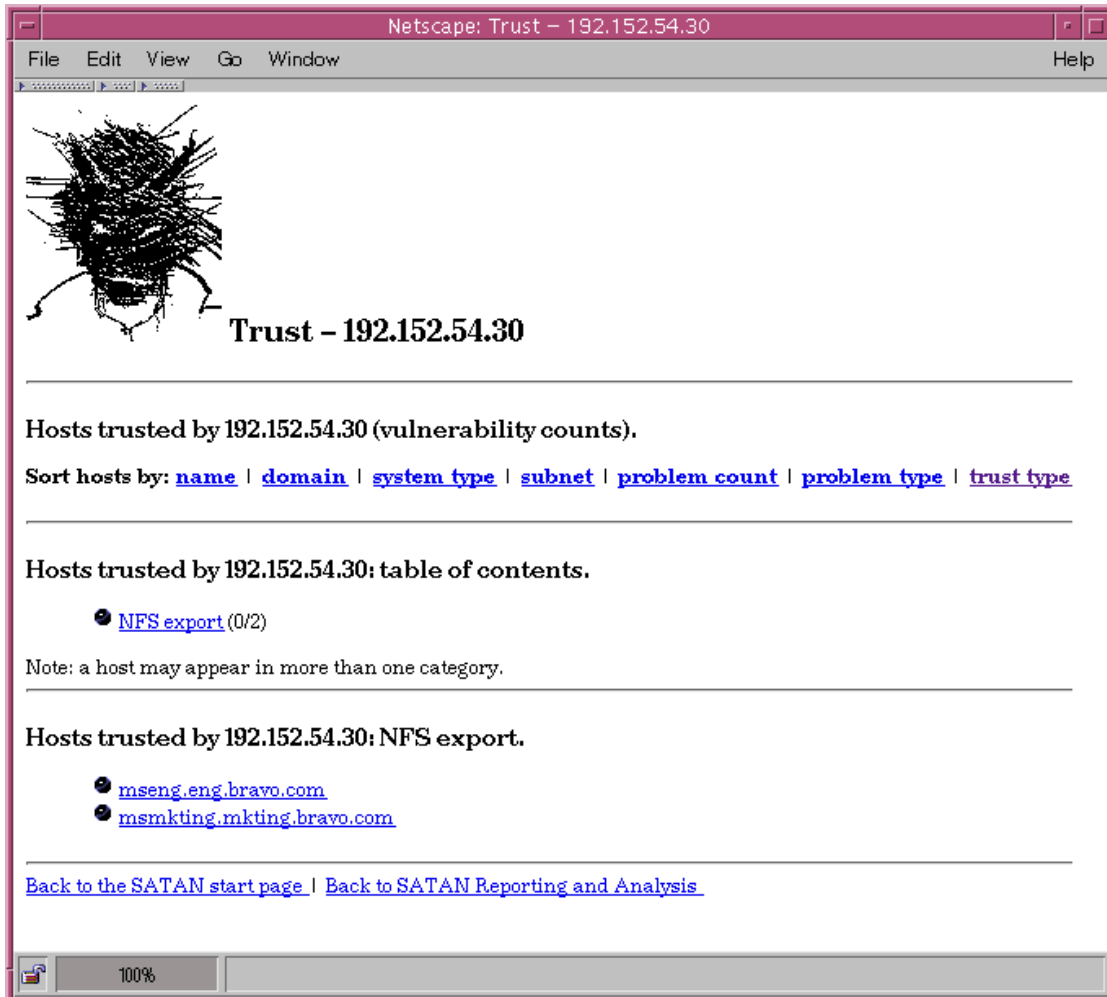
- Click on Subnet 192.152.54



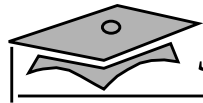


Using SATAN

- Black dots represent secure system
- Red dots represent vulnerabilities

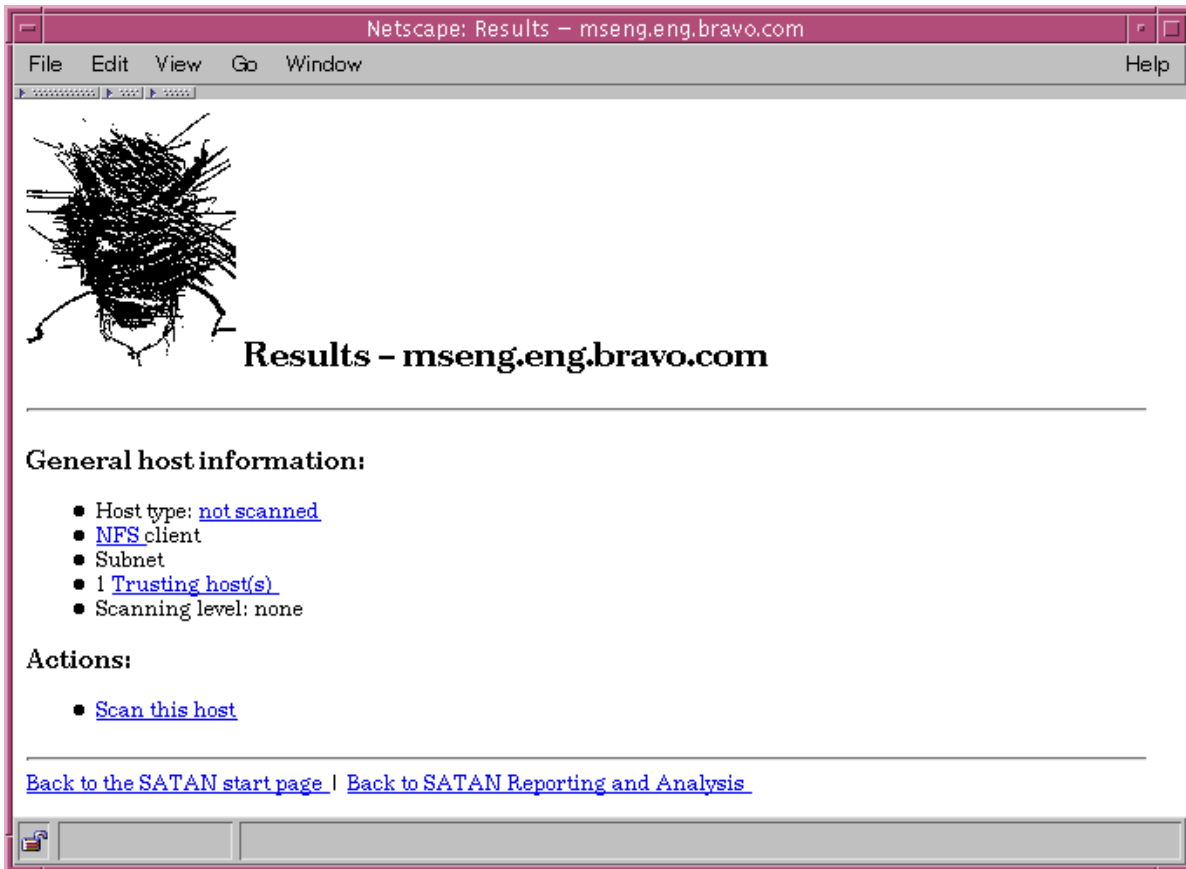


- Click 192.152.54.18

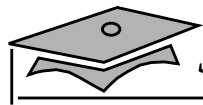


Using SATAN

- Host-specific information is displayed

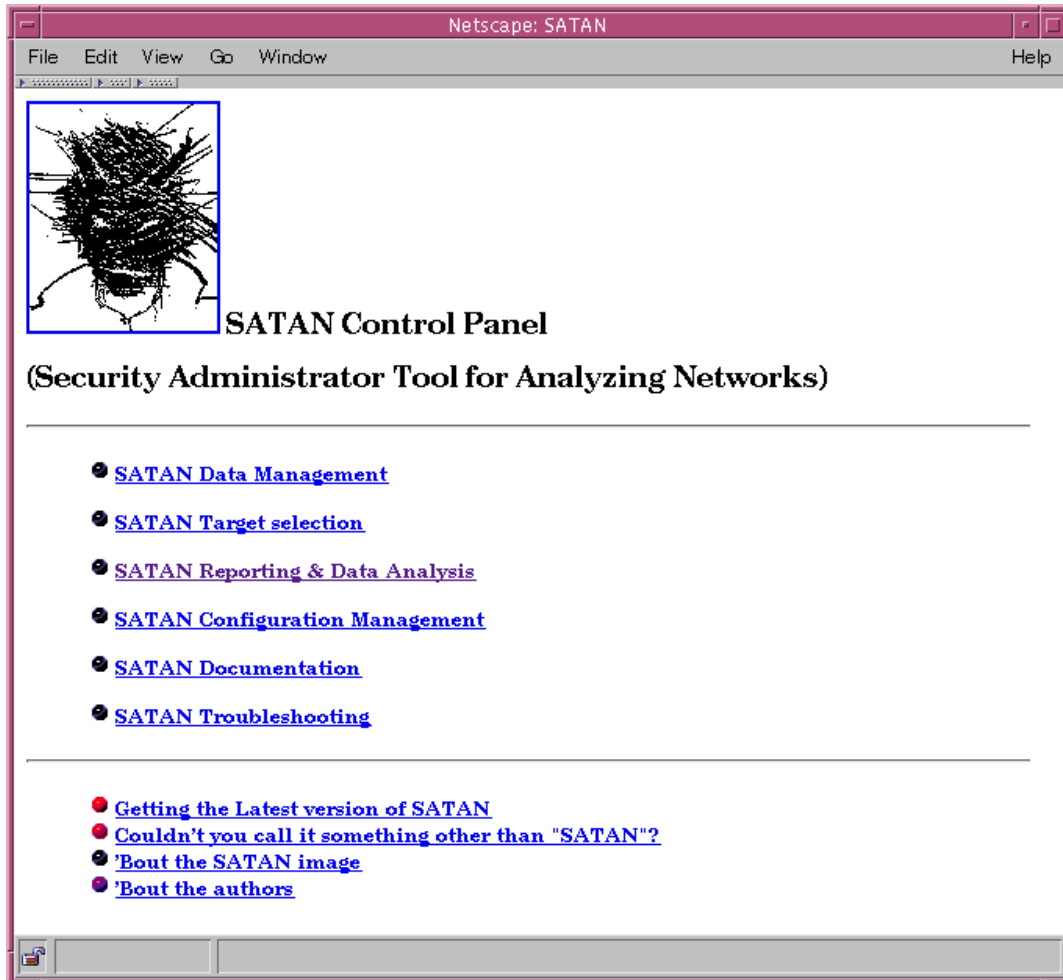


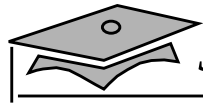
- Right click to go back



Using SATAN

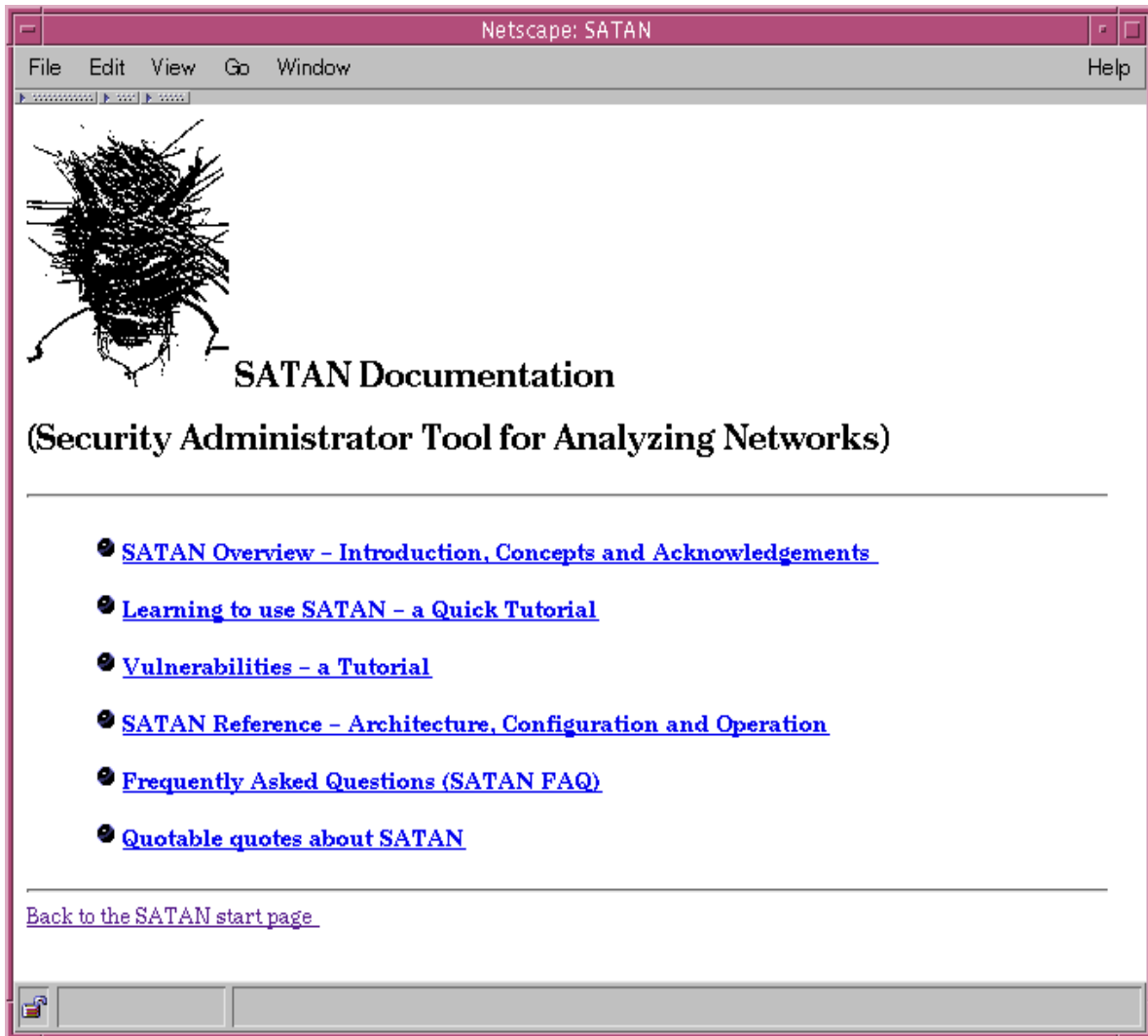
- Click on SATAN Documentation





Using SATAN

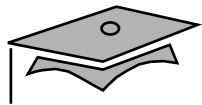
- Online documentation is available





SATAN Summary

- One host at risk due to unrestricted NFS export (share)
- All other hosts are secure from known network attacks



What Is Courtney?

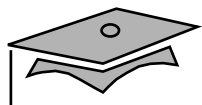
- Uses tcpdump to warn of SATAN probe
- Requires
 - Perl Version 5 or later, libpcap, and tcpdump
- Is started by:

```
# perl ./courtney.pl -s
```

```
tcpdump: listening on le0
```

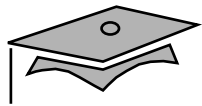
```
00:18:10: NORMAL_ATTACK from gaul - target alesia
```

```
00:18:11: HEAVY_ATTACK from gaul - target
```



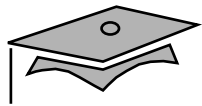
Module 14

Trip Wire



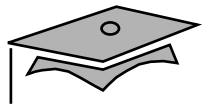
Overview

- Objectives
- Relevance



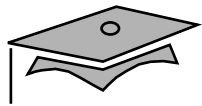
An Indicator of Intrusions – File Integrity

- Easiest way to notice completed intrusions
- File integrity verifiers do basic security examinations
- TripWire
 - Automatically monitors file changes
 - Looks for changes in file size, name, access date, and inode
 - Watches actual file contents



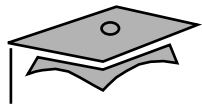
What Is TripWire?

- Checks archived image of files with current state of files
- Requires
 - gcc
 - make



Installing TripWire

- Edit `config.h` file and change
 - Configuration file path
 - Database path
 - Name of configuration file
- Create configuration file directory
- Copy default configuration file
- Create directory for binary
- Create directory for man pages



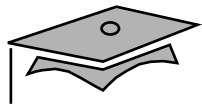
Installing TripWire

- Edit the Makefile
 - Change directory for binaries
 - Change C compiler
 - Change path for `install` utility
- Use **# make install**



Installing TripWire

- Verify binary existence
- Verify man pages
- Edit the configuration file



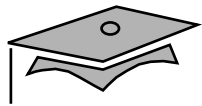
Generating a TripWire Database

- Use # **tripwire -v -initialize**
- Copy database to expected directory
- Perform integrity check
 - Use # **tripwire -v**
 - Change data



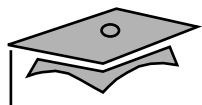
Checking the Integrity of the System

- Perform another integrity check
 - Use # **tripwire -v**



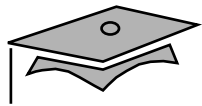
Updating the Database

- Use # **tripwire -v -update /fred**
- Copy database to expected directory
 - # **cp databases/tw.db_jeeves /tmp**
 - # **tripwire -v**
- Consult the man pages
 - **tripwire(8)**
 - **tw.config(5)**



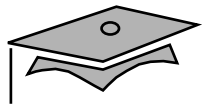
Module 15

TCP_Wrappers



Overview

- Objectives
- Relevance



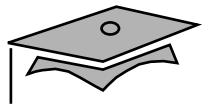
What Are TCP_Wrappers?

- Transparently log TCP and some UDP services
- Control access
- Have a simple installation
- Do not allow information to be exchanged with client
- Have no communication overhead



Installing TCP_Wrappers

- Two methods of installation
 - Hidden – Move many files
 - Visible – Edit `/etc/inetd.conf`



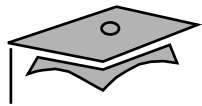
Installing Visible TCP_Wrappers

- Use required utilities
 - `gunzip`
 - `make`
 - `gcc`
- Edit `Makefile`
 - Define directory for network services
 - Enable `DPROCESS_OPTIONS` for banners



Installing Hidden TCP_Wrappers

- Use **make sunos5**
- Move binaries to another directory
- Replace binaries with renamed tcpd



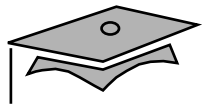
Installing TCP_Wrappers

- Installing visible TCP_Wrappers
 - Place `tcpd` in `/usr/sbin`
 - Edit `/etc/inetd.conf` to reference `tcpd`

```
# egrep -e 'in.ftpd' /etc/inetd.conf
```

```
ftp      stream  tcp      nowait  root    /usr/\n/sbin/tcpd  in.ftpd
```

- Restarting the Internet daemon
- Installing the man pages
- Viewing the log file



Configuring Access Control

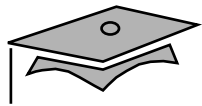
- Using `/etc/hosts.allow` and `/etc/hosts.deny`
- Denying global access – `ALL :ALL`

```
Sep 28 06:18:05 jeeves in.telnetd[4722]: refused  
connect from verdun
```

- Denying partial access – `in.telnetd : verdun`
- Allowing global access – `ALL :ALL`

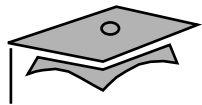
```
Sep 28 06:30:08 jeeves in.telnetd[4750]: connect  
from verdun
```

- Allowing partial access – `in.telnetd :verdun`



Configuring Access Control

- banners
- daemon_list : client_list : option : option
- hosts_access(5)
- hosts_options(5)

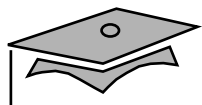


Using banners With TCP_Wrappers

```
# cat /etc/hosts.allow
```

```
in.telnetd :verdun :banners /usr/allow-messages
```

- Message in /usr/allow-messages/in.telnetd



Configuring Access Control

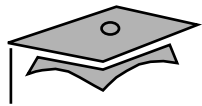
```
# cat /etc/hosts.deny
```

```
in.telnetd :metz :banners /usr/deny-messages
```

- Message in /usr/deny-messages/in.telnetd
- The spawn command

```
# cat /etc/hosts.allow
```

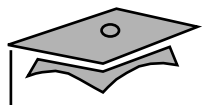
```
ALL :gaul :banners /etc :spawn (echo "intruder \  
%h detected" | /custom-apps/pager (303) 555-1212)
```



Using the tcpdmatch Command

- Performing configuration check
- Using the syntax – **tcpdmatch** *service host*

```
# tcpdmatch in.telnetd metz
```



Module 16

Crack



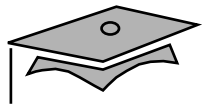
Overview

- Objectives
- Relevance



What Is Crack?

- Crack is a utility which guesses passwords by encrypting words and comparing them to the encrypted password.



Installing Crack

- C compiler
- Compiler flags
- Encryption type
- make
- A dictionary



Using Crack

- Merge shadow and passwd files
- Use Reporter script



Module 17

Security Strategies



Overview

- Objectives
- Relevance



Security Summary

- What action makes sense for your organization?
- Which tools are appropriate?
- How do they fit together?



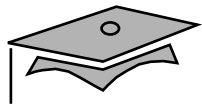
Topic Review

- Terminology and overview
- Basic system security
 - Security policy
 - Good passwords
 - Secure account management



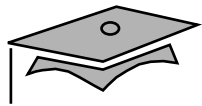
Topic Review

- UNIX vulnerabilities
 - Special files for backdoors
 - Regular process monitoring (ps, who, vmstat, and so on)
- Common security cracks
 - Trojan horses and logic bombs
 - Detection



Topic Review

- `syslog` and Basic Security Module (BSM)
 - Monitor users, `ftp` and `telnet` with `syslog` logging
 - For C2 auditing, use BSM for highest level of detail logging
- Automated Security Enhancement Tool (ASET)
 - Use regularly to insure new security cracks are located promptly
 - Adjust and customize security levels



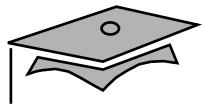
Topic Review

- SATAN and Courtney
 - Use SATAN proactively to defend possible attacks
 - Use Courtney to detect SATAN attacks
- TripWire
 - Create before and after images of file systems to spot the tracks of attacks
- TCP_Wrappers
 - Log, notify, and control users' access to a system



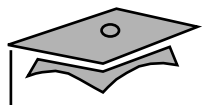
Topic Review

- Crack
 - Use it proactively on your users' password database to insure secure good password quality



Topic Review

- Protecting files and data
 - Set default file permissions with `umask`
 - Scan for SUID / SGID programs and scripts
 - Use ACLs when necessary
 - Establish backup / restore policy
 - Encrypt files with sensitive data
 - Use SKIP for IP level encryption



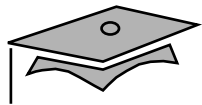
Topic Review

- Remote access and authentication services
 - Limit use of `rlogin`, `rcp`, and `rsh`
 - Do not use `.rhosts` or `hosts.equiv`
 - Use PAM to control and log users' access
- Secure shell
 - Use `ssh` to replace `rlogin`, `rcp`, and `rsh`

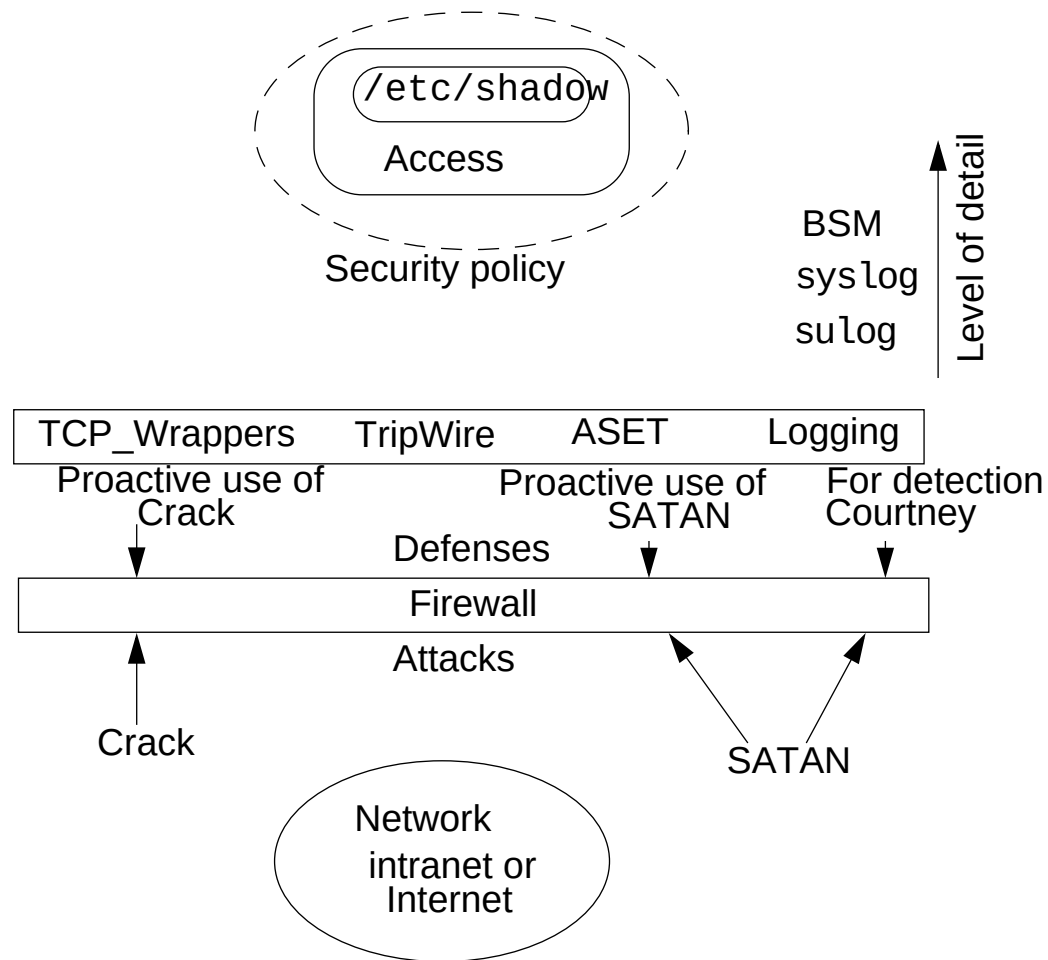


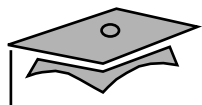
Topic Review

- Using Secure NFS
 - For internal networks, use Secure NFS for user authentication and transmission encryption.

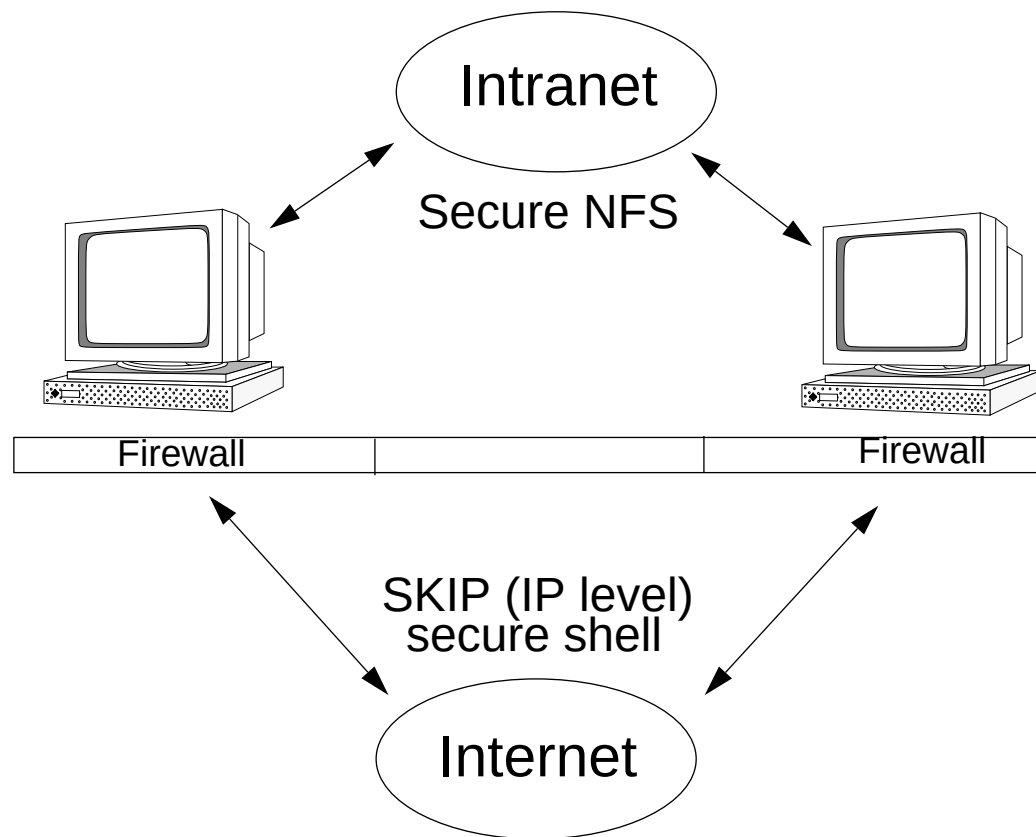


Securing a Host



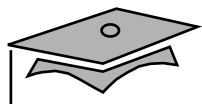


Securing a Network

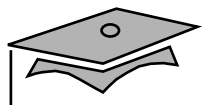


Course Contents

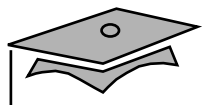
<i>About This Course</i>	<i>About This Course-1</i>
Course Goal	About This Course-2
Course Overview	About This Course-3
Course Map	About This Course-4
Module by Module Overview	About This Course-5
Course Objectives	About This Course-8
Skills Gained by Module	About This Course-11
Guidelines for Module Pacing	About This Course-12
Topics Introduced	About This Course-14
How Prepared Are You?	About This Course-15
Introductions	About This Course-16
How to Use Course Materials	About This Course-17
Typographical Conventions and Symbols	About This Course-18
 <i>Terminology and Overview</i>	 <i>1-1</i>
Overview	1-2
What Is Security?	1-3
Common Causes of Damage to Data	1-4
Types and Perpetrators of Computer Crimes	1-5
Security Standards	1-8
Secure Operating Systems Standards	1-9
The DoD Seven Layers of Trust	1-10
System Security	1-11



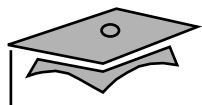
<i>Basic System Security</i>	2-1
Overview	2-2
Security Policy	2-3
Passwords	2-4
Passwords	2-5
Password and Shadow Files	2-6
Password Aging and Expiration	2-7
Secure Account Management	2-8
Guest Accounts	2-9
Restricted Shells	2-10
Search Paths and Startup Files	2-11
Superuser	2-12
EEPROM Security	2-13
 <i>UNIX Vulnerabilities</i>	 3-1
Overview	3-2
Security of Disk Files	3-3
Denial of Service	3-4
The who Command	3-5
The ps Command	3-6
The whodo and w Commands	3-7
The kill Command	3-8
The swap Command	3-9
The vmstat Command	3-10
The sar Command	3-11
Process Accounting Tools	3-12
Temporary File Systems (tmpfs)	3-13
Important System Log Files	3-14



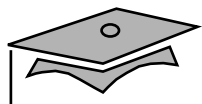
<i>Common Security Cracks</i>	4-1
Overview	4-2
Common Security Cracks	4-3
 <i>Protecting Files and Data</i>	5-1
Overview	5-2
File Permissions	5-3
The chmod Command	5-4
umask – Creation Mask	5-5
Sticky Bit on Directories	5-6
SUID and SGID	5-7
Access Control Lists (ACLs)	5-8
Backup / Restore	5-9
Encrypting Files	5-10
Encrypting Transmissions (SKIP)	5-11
SKIP Commands	5-12
SKIP Advantages	5-13
 <i>Controlling Root Access With sudo</i>	6-1
Overview	6-2
What Is sudo?	6-3
sudo Configuration File	6-4
sudo Configuration File	6-5
Using sudo Commands.....	6-6
sudo Aliases	6-7
Enabling syslogd Logging for sudo	6-8



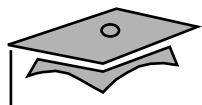
<i>Secure Shell</i>	7-1
Overview	7-2
Describing the Secure Shell (ssh)	7-3
Working With the sshd Daemon	7-4
Installing the Secure Shell	7-5
Configuring the Secure Shell	7-6
Creating the Server Keys	7-7
Starting the Secure Shell From the Client	7-8
Creating Alternative Configurations	7-9
 <i>Remote Access and Authentication Services</i>	8-1
Overview	8-2
Remote Access System Files	8-3
Restricting Connectivity Commands and Services	8-4
Berkeley “r” Commands	8-5
Network Authentication – rlogin, rcp, and rsh	8-6
Netgroups	8-7
Authentication Services Used With Secure RPC	8-9
What Is PAM?	8-11
PAM Runtime Module Types	8-12
PAM Configuration File	8-14
The /etc/pam.conf File	8-16
Configuring PAM	8-19
Preventing Unauthorized Remote Access With PAM	8-20
 <i>Using Secure NFS</i>	9-1
Overview	9-2
Secure NFS	9-3
Secure RPC	9-4
DES Authentication Protocol	9-5



Common Key Creation	9-6
Conversation Key Generation	9-7
Conversation Key Decryption	9-8
Secure RPC / NFS Enabled	9-9
Secure NFS Setup	9-10
Problems With Secure NFS	9-11
The fsirand Command	9-12
 <i>Solaris Operating Environment syslog</i>	 <i>10-1</i>
Overview	10-2
Why Use syslog?	10-3
Configuring /etc/syslog.conf	10-4
Using Different syslog Severity Levels	10-5
Using syslog With telnet	10-6
Using syslog With ftp	10-7
The logger Utility	10-8
 <i>Basic Security Module (BSM)</i>	 <i>11-1</i>
Overview	11-2
Basic Security Module (BSM) Auditing	11-3
Viewing Audit Data	11-4
Major Components of Auditing	11-5
Auditing Startup	11-6
Device Allocation	11-7
Device Allocation Files	11-8
User Commands	11-9



<i>Automated Security Enhancement Tool (ASET)</i>	12-1
Overview	12-2
What Is ASET?	12-3
The aset Command	12-4
Interactive and Periodic Modes	12-5
ASET Reports	12-6
Changing Security Levels	12-7
 <i>SATAN and Courtney</i>	13-1
Overview	13-2
What Is SATAN?	13-3
Utilities for SATAN	13-4
Procuring a Web Browser	13-5
Testing the Web Browser Installation	13-6
Utilities for SATAN	13-7
Procuring a C Compiler	13-8
Procuring make	13-9
Procuring and Installing SATAN	13-10
Installing and Configuring SATAN	13-11
Using SATAN	13-12
SATAN Summary	13-25
What Is Courtney?	13-26
 <i>TripWire</i>	14-1
Overview	14-2
An Indicator of Intrusions – File Integrity	14-3
What Is TripWire?	14-4
Installing TripWire	14-5



Generating a TripWire Database	14-8
Checking the Integrity of the System	14-9
Updating the Database	14-10
 <i>TCP_Wrappers</i>	 15-1
Overview	15-2
What Are TCP_Wrappers?	15-3
Installing TCP_Wrappers	15-4
Configuring Access Control	15-8
Using the tcpdmatch Command	15-12
 <i>Crack</i>	 16-1
Overview	16-2
What Is Crack?	16-3
Installing Crack	16-4
Using Crack	16-5
 <i>Security Strategies</i>	 17-1
Overview	17-2
Security Summary	17-3
Topic Review	17-4
Securing a Host	17-12
Securing a Network	17-13

Copyright 2000 Sun Microsystems Inc., 901 San Antonio Road, Palo Alto, California 94303, Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley 4.3 BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company Ltd.

Sun, Sun Microsystems, le logo Sun, Solaris, et NFS sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.

Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

UNIX est une marques déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

L'accord du gouvernement américain est requis avant l'exportation du produit.

Le système X Window est un produit de X Consortium, Inc.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.