Securing Operating Systems

Chapter 10

Lecturer: Pei-yih Ting

Overview

- Security Maintenance Practices and Principles
- Patches, Fixes, Revisions
- Antivirus Software
- Post-Install Security Checklist: Windows/UNIX
- File System Security Issues
- User Accounts and Passwords
- Checksums Catch Unauthorized Changes
- System Logging Utilities

Security Maintenance Practices and Principles

- First step toward a secure system is creating a security policy and constantly revising
- Maintenance involves creating a strategy to
  - Review and update software and hardware
  - Review and update security policy
  - Assign tasks to specific people
  - Set a schedule
- Overall goal is to harden the system (make it more secure)
  - Hardening is iterative and changing
  - Hardening may not dissuade a persistent attacker; An attacker with a grudge against you can be very persistent

Maintaining the OS: Patches, Fixes, and Revisions

- A cracker is a person who attempts to compromise your computer system
  - Hackers don't generally have malicious intent; crackers do
  - Terms are often used interchangeably
- An exploit is a procedure that takes advantage of a vulnerability that can be used to compromise a system
  - Exploits are routinely shared among crackers, and problems will begin to show up on many systems
  - After a period of time (hopefully), the software or hardware manufacture releases a patch to eliminate the problem.

Patches, Fixes, and Revisions

- Make sure you understand what a patch does before installing it
- Make sure you have a valid system backup before installing any new software.
- Never trust a security patch you did not request. Soft ware vendors do not send out patches. Then send notifications.
- Catalog the software packages you have installed on your system and keep them up to date.

Antivirus Software

- Identifies files that contain known viruses
- Antivirus software has a scanning mode that checks files throughout a system to see if they contain a virus signature
  - A virus signature is a set of instructions or data that is unique to a particular virus
- After scanning, the software can remove or quarantine the virus
  - However, the cleaned system might lose some important executables.

Antivirus Software (cont'd)

- A virus shield runs in the background and scans all incoming data/files for viruses
  - Files downloaded, web pages browsed/cached, or emails received (sent)
- The virus signature database must be up to date in order to be effective
- Most antivirus packages offer automatic updates
  - After an update, you should scan your file system to catch any files that have already been infected
- A final precaution is to train users to understand the basics of malicious code attack and report suspicious activities

Applying a Post-Install Security Checklist

- Develop and use a security checklist to ensure that you have achieved all of the required tasks
- A checklist helps you to stay organized under pressure
- A checklist should be based on professional experiences
  - Use standard checklists available from the operating system manufacturer and other resources as basis
  - They contain the summary of past attempts to secure computers and include action items of things to do and things not to do
- Customize the checklist for your own environment

Windows Checklist Elements (1/6)

- Hardening the Windows Registry
  - The registry is a central repository for system values
  - Arranged as a hierarchical database of registry keys that store values
  - Can be edited with the Windows Registry Editor (regedit.exe or regedt32.exe) or 3rd party applications
  - It is important to understand the implications for each key value, changes can be dangerous
  - Create a backup before changing the values in Windows Registry
  - http://www.winguides.com/registry/
  - In WinXP, you can assign 11 permissions to each key

Windows Checklist Elements (2/6)

Table 10.1 Windows Registry Keys That Affect Security

Descriptions	KeyValueNames
Prevent access to the content of selected drives	NoViewOnDrive
Restrict applications users can run	RestrictRun
Disable registry editing tools	DisableRegistryTools
Disable the shutdown command	NoClose
Disable the Windows hotkeys	NoWinKeys
Restrict access to the Windows Update feature	NoWindowsUpdate
Manage system policy updates	UpdateMode, NetworkPath, Verbose, Load Balance
Restrict changes to user folder locations	DisablePersonalDirChange, DisableMyPicturesDirChange, DisableMyMusicDirChange, DisableFavoritesDirChange
Implement a user-based custom shell	Shell

Windows Checklist Elements (3/6)

- Removing Unneeded Services
  - The default Windows installation enables services that may not be needed in many environments
  - Extra services consume resources and provide entry points for attackers
- Securing Networking Protocols and Services
  - Limit access to services that are not disabled
  - Use a firewall if you're connected to the Internet
  - Disable networking protocols that are not used
  - Review services related to remote access and networking, and remove any that are non-essential, Be careful, many services are grouped together, you might be able to remove them but it could be hard to restore

Windows Checklist Elements (4/6)

Table 10.2 Windows Services That May Be Unneeded

Service	Descriptions	Comments
File Sharing	Allows remote users to access local drives and files	Disable this service
Printer Sharing	Allows remote users to print to a local printer	Disable this service
Internet Information Services (IIS)	Microsoft's Web server	Unless you are hosting a Web site, do not install this service
NetMeeting Remote Desktop Sharing	Allows others to share your desktop	Unless you need it, disable this service
Remote Desktop Help Session Manager	Allows remote support	Unless you need to perform or support remote support, disable this service
Remote Registry	Allows remote users to modify and maintain the registry	If you do not plan to manage the registry remotely, disable this service

Windows Checklist Elements (5/6)

Table 10.2 Windows Services That May Be Unneeded

Service	Descriptions	Comments
Routing and Remote Access	**Allows for remote access to our system**	**Unless you need to dial in to your system, disable this service**
SSDP Discovery Service	**Supports the Universal PnP Service**	**Disable this service; closes port 5000**
Universal Plug and Play Device Host	**Allows your system to connect to network-enabled appliances**	**Because there are no practical applications for this service yet, disable this service**
Telnet	**Allows remote users to log in to your system**	**Because all information, including passwords, is transmitted in the clear, disable this service. Use ssh instead**

Windows Checklist Elements (6/6)

- Windows Security Miscellany
  - Physically secure your computer
  - Stay up-to-date with operating system patches, through Windows Update Web site
  - Download and use the Microsoft Baseline Security Analyzer (MBSA) and enable the Encrypting File System for Windows XP
  - Do not use the Administrator account for daily usage
  - Disable the Guest account
  - Enable strong password policy
  - Disable the CDROM auto-run feature, use antivirus S/W
  - Enable system auditing, protect backup

UNIX Checklist Elements (1/4)

- Security philosophy is similar for Windows and UNIX but the details are substantially different
- Removing Unneeded UNIX Protocols and Services
  - Disable any non-essential services and daemons
  - Some services can be disabled by editing the /etc/inet.d
- Working with the TCPWrapper
  - TCPWrapper is a common name for the **tcpd** daemon
  - Can accept or deny any packet before it is passed to its target
  - Uncover spoofed address through double-reverse lookup
  - Suspicious requests can be dropped, logged, and/or an administrator can be notified

UNIX Checklist Elements (2/4)

Table 10.3 UNIX Services and Daemons That May Be Unneeded

Service	Descriptions	Comments
Telnetd	**Allows remote user access**	**Disable this Telnet daemon. Use ssh instead**
Fingerd	**Provides information about users on your system**	**Disable this daemon unless it is considered essential**
R-commands (rlogin, rsh, rcp, …)	**Allow remote users to interact with your system**	**Disable the commands to reduce password and other data disclosure**
Cron	**Executes commands at specified times**	**Consider disallowing cron for regular users**
RPC	**Remote Procedure Call**	**Disable this service if not needed**
Ftpd	**Transfers files using the File Transfer Protocol (FTP) daemon**	**Disable it if you don't need to provide FTP access**

UNIX Checklist Elements (3/4)

Table 10.3 UNIX Services and Daemons That May Be Unneeded

Service	Descriptions	Comments
Trivial ftp (TFTP)	Transfers files using a simpler version of FTP	Disable this program
UNIX to UNIX copy (UUCP)	Transfers files (older method)	Disable this service
Sendmail	Sends and forwards e-mail	Disable this service unless your computer processes e-mail. If you need e-mail processing, consider alternatives (qmail or postfix)
NFS, SAMBA, AFS, DFS	Provide network access to files and volumes	Use these only if absolutely necessary. Use with care.

UNIX Checklist Elements (4/4)

- UNIX Security Miscellany
  - Physically secure your computer
  - Stay up-to-date with operating system patches
  - Protect superuser Ids
  - Ensure strong user passwords and train users on passwords
  - Use antivirus software
  - Protect backups
  - Enable system auditing and review logs
  - Run vulnerability scanners against your system

Understanding File System Security Issues

- The file system is the set of programs that manage and store data on secondary storage
- The file system is presented as a hierarchical tree structure
  - The top of the tree is the root directory (the entry point)
- Disks can be divided into sections called partitions
  - Each partition has its own file system and root directory
- In Windows, each file system has a drive letter
- In UNIX, each file system has a mount point

Securing NT File System (NTFS)

- NTFS is the preferred file system for Windows servers
- Designed for file protection in a multi-user environment
- Each file or folder has associated access control lists
- File systems offer 6 to 13 possible permissions for files and folders, attributes, and extended attributes
  - Stored in an access control entry (an ACL consists of multiple ACEs)
- NTFS gives administrators very precise access control for files and folders

Securing NTFS (cont'd)

Table 10.4 NTFS Permissions in Windows NT/2000/XP

Permission	File Permission Granted	Folder Permission Granted
Read (R)	**Read a file's contents**	**Read a folder's contents**
Write (W)	**Modify a file's contents**	**Modify a folder's contents**
Execute (X)	**Execute a program file**	**Traverse a folder or subfolder**
Delete (D)	**Delete a file**	**Delete a folder**
Change Permission (P)	**Change a file's permission setting**	**Change a folder's permission setting**
Take Ownership (O)	**Take file ownership**	**Take folder ownership**

Windows *Share* Security

- Windows files and printers can be shared with remote users
  - File and Printer Sharing enabled by default
- Three security levels for each share
  - Global level: anyone can access the share
  - Share level: requires a password for access
  - User level: access is restricted to specific users

Understanding User Accounts and Passwords

- A user account is the primary access requirement for modern systems
- The most common vulnerability in a user account is a weak password
- Educate users to create strong passwords
  - Don't use dictionary words, common phrases, personal information
  - Use a different password for each account
  - Don't write down passwords, and change them periodically
  - Use combinations of letters, numbers, punctuation, uppercase, and lowercase

Windows Account Security Mechanisms

- Users are typically created at the domain level
- In newer Windows operating systems, all security permissions can be centralized
  - Users can log into any computer in a domain
- Must have administrator privileges to create user accounts
- User accounts can be added to security groups
- Permissions can be set at group level
  - Easier to assign group permissions
  - Plan and organize account strategy before implementing

UNIX Account Security Mechanisms

- UNIX accounts are typically local
- Two levels of account security
  - User and group
- File permissions can be set for users or groups
- Overall security concepts are similar to Windows but details are different

Checksums Catch Unauthorized Changes

- A checksum is a mathematically generated number that is unique for a particular input
  - For the same input, the checksum will not change unless the input changes
- Used to ensure that files haven't changed without authorization
- Commonly used in collecting forensic evidence
- Most operating systems implement utilities for generating checksums
  - md5sum utility is popular
  - tripwire

Using System Logging Utilities

- Current operating systems allow many events to be logged for later inspection
  - Login attempts, authorization changes, resource accesses, print job activity, application and utility activity, and performance metrics
- Logging uses resources
  - CPU resources, Storage resources, Manpower resources
- Match logging activity to what is required in your specific environment
  - Do more logging for systems that require strict security or for new systems, less when not needed

Summary

- Security maintenance requires a strategic plan for
  - Reviewing and updating hardware, software, and policies
  - Assigning and scheduling tasks
- Crackers try to compromise systems by finding and sharing exploits
  - System is most vulnerable when a new exploit is discovered
- To minimize risk, stay up-to-date on
  - Operating system patches, fixes, and revisions
  - Antivirus software
- Antivirus software scans existing files and shields incoming files

Summary (cont'd)

- Checklists should be used to maintain thorough and disciplined security practices
  - should be customized for the operating system and the environment
- File systems generally allow some level of permissions to be assigned to each file/directory to control access
- User accounts are most vulnerable to weak passwords
- Checksums are used to tell if a file has been changed
- System logging is a powerful tool to be used judiciously

Assignments

- Reading: Chapter 10
- Practice 10.11 Challenge Questions

- Turn in Challenge Exercise 10.1 next week