Host Hardening
Chapter 6
Panko, Corporate Computer and Network Security
Copyright 2005 Prentice-Hall

Figure 6-1: Hardening Host Computers

- The Problem
  - Computers installed out of the box have known vulnerabilities
    - Not just Windows computers
  - Hackers can take them over easily
  - They must be hardened—a complex process that involves many actions

- Elements of Hardening
  - Physical security (Chapter 2).
  - Secure installation and configuration
  - Fix known vulnerabilities
  - Turn off unnecessary services (applications)
  - Harden all remaining applications (Chapter 9)
  - (more on next page)

- Elements of Hardening (continued)
  - Manage users and groups
  - Manage access permissions
    - For individual files and directories, assign access permissions specific users and groups
  - Back up the server regularly
  - Advanced protections

- Security Baselines Guide the Hardening Effort
  - Specifications for how hardening should be done
  - Different for different operating systems
  - Different for different types of servers (webservers, mail servers, etc.)
  - Needed because it is easy to forget a step

- Server Administrators Are Called Systems Administrators
  - A sysadmin manages one or several servers—not necessarily all of a firm's servers
  - Sometimes, groups of sysadmins manage multiple servers
Windows Computers
- Microsoft Network Operating Systems (NOSs)
  - LAN Manager (LANMAN)
  - Windows NT Server
  - Windows 2000 Server
  - Windows 2003 Server (called .NET in the book)
- Graphical user interface looks like client versions to ease learning (Figure 6-2)

Administrative Tools Group under Programs has Microsoft Management Consoles (MMCs) (Figure 6-3)
- Used to conduct most administrative actions
- Can add snap-ins for specific functionality

Windows 2000 introduced hierarchical domain structure with Active Directory
- Domain is a collection of resources
- Domain contains one or more domain controllers, member servers, client PCs
- Group policy objects (GPOs) on a domain controller can implement policies throughout a domain

UNIX
- Many versions of UNIX
- LINUX is a set of versions for PCs—there are several different distributions
- User can select the user interface—GUI or command-line interface (CLI)
- CLIs are called shells (Bourne, BASH, etc.)
- CLIs have picky syntax, capitalization, and spacing
Figure 6-1: Hardening Host Computers

- Internet Operating System (IOS)
  - For Cisco Routers, Some Switches, Firewalls
- Other Host Operating Systems
  - Macintosh
  - Novell NetWare
  - Firewalls
  - Even cable modems with web-based management interfaces

Figure 6-4: Installation and Patching

- Installation Offers Many Options, Some of Which Affect Security
  - For example, in Windows, the NTFS file system is better for security than FAT32
  - Need a security baseline to guide option choices during installation

Figure 6-4: Installation and Patching

- Known Vulnerabilities
  - Most programs have known vulnerabilities
  - Exploits are programs that take advantage of known vulnerabilities

Figure 6-4: Installation and Patching

- Known Vulnerabilities
  - Vulnerability reporters send vulnerability reports to vendors
  - Vulnerability reporters often say that vendors take too long to fix vulnerabilities
  - Vendors say that vulnerability reporters do not give them enough time, report too much detail to the press

Figure 6-4: Installation and Patching

- Fixes
  - Work-around: A series of actions to be taken; no new software
  - Patches: New software to be added to the operating system
  - Upgrades: Newer versions of programs usually fix older vulnerabilities.

Figure 6-4: Installation and Patching

- Upgrades
  - Often, security vulnerabilities are fixed in new versions
  - If a version is too old, the vendor might stop offering fixes
  - It might be good to wait to upgrade until after the first round of bug and security fixes
Mechanics of Patching

- Microsoft Windows Server
  - Windows Update on Start menu (Figure 6-2) in Windows 2000
  - Automatic notification of update availability in Windows 2003
- LINUX distributions often use rpm for updates

Patches Often Are Not Applied

- Companies get overwhelmed by number of patches
  - Use many products, vendors release many patches per product
  - Especially a problem for application programs
- Cost of Patch installation
  - Mitigated by patch servers that distribute patches to general servers
  - More easy-to-use vendor tools are needed
  - Might simply lack the resources to apply all; might be selective
- Risks of Patch installation
  - Reduced functionality
  - Freeze machines, do other damage—sometimes with no Uninstall possible
  - Should test patch on a test system before deployment
  - Special problem for mission-critical production systems that must work

Unnecessary Services

- Operating system vendors used to install many services by default
- This made them easier to use. When use changes, services do not have to be turned on.
- Attackers have found flaws in many of these rare services
Unnecessary Services
- Vendors now install fewer services by default—lock down mode
- Turn to security baseline to see what services to turn on and off
- Easier to install too few and add than to install too many and remove unwanted services

Turning Off Services In Windows Server
- Go to the Computer Management MMC
- On the tree, select Services and Applications (Figure 6-6)
  - Status tells whether the service is active
  - Startup tells how the service is started (automatic, manual, disabled, etc.)
- Right click on a service or select and choose Action to stop a service, start it, disable it, etc.

Turning Off Services In UNIX
- Three ways to start services
  - inetd to start services when requests come in from users (Figure 6-7)
  - rc scripts to start services automatically at boot up (Figure 6-8)
  - Start a service manually by typing its name or executing a batch file that does so
Figure 6-8 The UNIX rc.d Method of Automatically Starting Services

- rc1.d
- rc2.d
- rc3.d
- rc4.d
- rc5.d
- rc6.d [scripts to run during System Mode 6—startup]
- S1 . . . [Run the Start portion of Script 1: Starts Service A]
- S2 . . . [Run the Start portion of Script 2: Starts Service B]
- . . .
- rcs.d [scripts to run during System Mode s—single-user mode]

Figure 6-5: Turning Off Unnecessary Services

- Turning Off Services In UNIX
  - Identifying services that are running at any moment
    - `ps` (processor status), usually with `–aux` parameters, lists running programs
      - Shows process name and process ID (PID)
    - `netstat` tells what services are running on what ports

Figure 6-9: Managing Users and Groups

- Creating and Managing Groups in Windows
  - Computer Management: Local Users and Groups snap-in (Figure 6-10)
  - Select Users
    - Select user from list
      - Right click on user and select Properties: password restrictions, disable box
      - Or select Action: change password, etc.
      - Add, delete users
Figure 6-9: Managing Users and Groups

- Creating and Managing Groups in Windows
  - Select user from list
    - Administrator is the super account
      - Change its name and create a new Administrator account with no permissions
      - Administrators should not log in as Administrators; log in as their own account, use RunAs to get temporary Administrator status when needed

- Creating and Managing Groups in Windows
  - Select user from list
    - Guest account should be disabled (the default during installation)

- Creating and Managing Groups in Windows
  - Select Groups
    - Assign rights to groups
    - Standard groups: Administrators, Power Users, Backup Operators, etc.
      - Have appropriate permissions by default for their tasks

- Managing Users and Groups in UNIX
  - Different versions of UNIX do this differently, so it is difficult to talk in general terms
  - The super account is root
    - su (switch user) allows administrators to log in as regular accounts, su to get root privileges when desired
  - Guest account should be disabled
Principle of Least Permissions: Give Users the Minimum Permissions Needed for Their Job
- More feasible to add permissions selectively than to start with many, reduce for security

Assigning Permissions in Windows (Figure 6-14)
- Right click on file or directory in My Computer
- Select Properties, then Security tab
- Select a user or group
- NOT done through the start menu, selecting Administrative Tools

Assigning Permissions in Windows (Figure 6-14)
- Click on or off the 6 standard policies (permit or deny)
  - List Folder Contents (see what is in a directory)
  - Read (read only)
  - Read and Execute (for programs)
  - Write (change files)
  - Modify (Write plus delete)
  - Full control: all permissions

Assigning Permissions in UNIX
- ls -l shows details of files and directories in long format
  - First character is - for a file, d for a directory
  - Ends with name of file or directory

```
-rwxr-x--1 root . . . purple.exe
-dw-r-----1 brows . . . reports
-w-rw-r--1 lighter . . . bronze.txt
```

Note: purple.exe is a file; reports is a directory. What is bronze.txt?
Assigning Permissions in UNIX

- `ls -l` shows files in a directory in long format
- Only three permissions: read (only), write (change), and execute (run program)
- Format is `rwx` for all or various combinations (e.g., `r-x` is read and execute but not write)

```
-rwxr-x---1 root . . . purple.exe
drw-r---- 1 brows . . . reports
-rw-rw-r--1 lighter . . . bronze.txt
```

- Next three characters are permissions (rwx possible) for the file owner
- Next three are permissions (rwx possible) for the group
- Next three are permissions for the rest of the world

Purple's group has read and execute permissions.
Purple has no permissions for the rest of the world.

**Changing permissions**

- `umask` (user mask) command sets the default permissions for future assignments
- `chmod` (change mode) changes permissions for the file
- `chown` (change owner) changes the ownership of a file

**Reading Event Logs (Chapter 10)**

- The importance of logging to diagnose problems
- Failed logins, changing permissions, starting programs, kernel messages, etc.
- `Windows 2000 Event Viewer (Figure 6-17)`
UNIX has many logging facilities controlled by the syslog program (Figure 6-18). The syslog program sends log entries of different types to specific directories on the host or on other hosts. The file syslog.config specifies which log entries and which severity levels should go to which directories on which hosts.

UNIX backup:
- tar command (tape archive)
- Create tape archive of a file, group of files, directory tree in a .tar file
- Can use tar to look at table of contents of files in the .tar file
- Can use tar to restore one, some, or all files

Windows backup:
- Start, Programs, Accessories, System Tools, Backup
- Note that Backup is under Accessories rather than under Administrative Tools like most MMCs
- GUI to create backups, restore backups

File Encryption
- Protects files even if attacker breaks in
- Key escrow: Copy of encryption key is kept elsewhere to protect in case of key loss
- Windows Encrypting File System (EFS)
  - Select file in Windows Explorer, select Properties
  - Click on General tab’s Advanced button
  - Click on the box Encrypt contents to secure data
File Encryption
- Windows Encrypting File System (EFS)
  - Encryption is transparent: Save, retrieve, copy files as usual
  - Encrypted files generally cannot be sent over the network
  - There is a Recovery agent (usually on the domain controller) for key escrow

File Integrity Checker
- Tripwire
  - Creating snapshot of files: a hashed signature (message digest) for each file
  - After an attack, compares post-hack signature with snapshot
  - This allows systems administrator to determine which files were changed
  - Tripwire is the usual file integrity checker for UNIX (Figure 6-19)

File Integrity Checker
- If applied to too many files, too many false alarms will occur
  - Must be selective—core programs likely to be Trojanized during attacks

Server Host Firewalls
- Rules can be specific to the server's role (e-mail, etc.)

Importance of Clients
- Contain important information
- If taken over, can get in as user, passing through firewalls and other protections
Figure 6-21: Hardening Clients

- **Enforcing Good Practice**
  - Patching
  - Antivirus software
  - Firewall software
  - Limiting client software to an approved list (e.g., forbidding P2P file exchange products)
  - Save passwords?
  - File encryption

- **Central Control is Desirable for Clients**
  - For example, Microsoft Group Policy Objects (GPOs) for home clients
  - Require certain programs (antivirus, etc.), forbid programs not on list
  - Even lock down desktop so use cannot add new software or even change the interface
  - Central vulnerability scanning
  - Difficult to enforce on personally owned home computers

---

Topics Covered

- **Firewalls and other protections sometimes break down**
- **Computers must be hardened to survive when attackers reach them**
- **Defense in depth**

---

Topics Covered

- **Elements of Hardening**
  - Physical security (Chapter 2).
  - Secure installation and configuration
  - Fix known vulnerabilities
  - Turn off unnecessary services (applications)
  - Harden all remaining applications (Chapter 9)
  - Manage users and groups
  - Manage access permissions
  - Back up the server regularly
  - Advanced protections

---

Topics Covered

- **Baselines are needed to specify everything that must be done to harden a server**
- **Server administrators are called systems administrators**
  - Each server has one or more sysadmins

---

Topics Covered

- **Microsoft Network Operating Systems (NOSs)**
  - LAN Manager (LANMAN)
  - Windows NT Server
  - Windows 2000 Server
  - Windows 2003 Server (called .NET in the book)
  - Familiar Windows interface gives ease of learning and use
Topics Covered

- UNIX
  - Many versions of UNIX
  - LINUX distributions
  - CLIs are difficult to use

- Other
  - Novell NetWare
  - Cisco IOS for routers and switches
  - Firewalls, cable modems, etc.

- Installation
  - Many options affect security
  - Need a baseline to guide installation

- Patching vulnerabilities
  - The most critical hardening step
  - Fixes, patches, and upgrades
  - Often not applied because of sysadmin overload
  - Need to test patches before roll out
  - Linux uses rpm to get patches
  - Windows 2000 uses the Windows Update item on the start menu
  - Automatic notification in Windows 2003

- Turn Off Unnecessary Services
  - To give attackers fewer targets
  - Windows Server
    - Computer management MMC GUI
  - Unix
    - inetd.config modification
    - rc scripts
    - ps –aux, netstat show process IDs (PIDs)
    - kill PID kills the process with that PID

- Managing Users and Groups
  - Assign permission to users
  - Can also assign permissions to groups
    - Group members receive all assigned permissions
  - Assign permissions for individuals and groups to individual directories

- Managing Users and Groups
  - Windows Server Computer Management: Local Users and Groups snap-in to manage users and groups
  - Assign permission to directories by right clicking on them
  - Windows has 6 standard permissions which can be subdivided into 13 special permissions
  - Windows can assign permissions in a directory to many users and groups
Topics Covered

- Permissions in Unix
  - Only three (read, write, and execute)
  - Can only be assigned to a file or directory owner, a single group, and the rest of the world
  - `ls -l` shows permissions
  - `chmod` changes permissions for a file or directory
  - `chown` changes the owner of a file or directory

- File Integrity Checking
  - Tripwire for Unix and Windows

- Host Firewall
  - Protections tailored to host’s specific services

- Vulnerability Assessment
  - Unix external audit, network monitoring, and host assessment tools

Hardening Clients

- Good Practice
  - Many Aspects
    - Patching
    - Antivirus software
    - Firewall software
    - Limiting client software to an approved list
    - Etc.
  - Difficult to enforce
    - Centralized management (e.g., Microsoft GPOs) can enforce policies