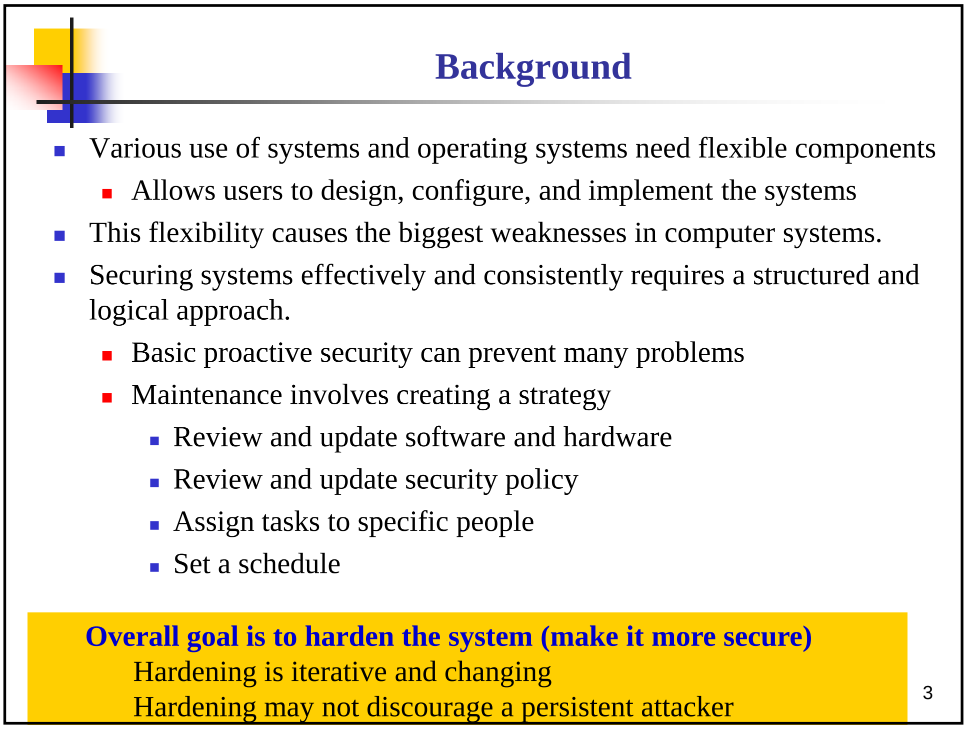
Baselines

Chapter 14

Objectives

- Upon completion of this lesson, the students will be able to:
  - Harden operating systems and network operating systems.
  - Harden applications.
  - Establish group policies.



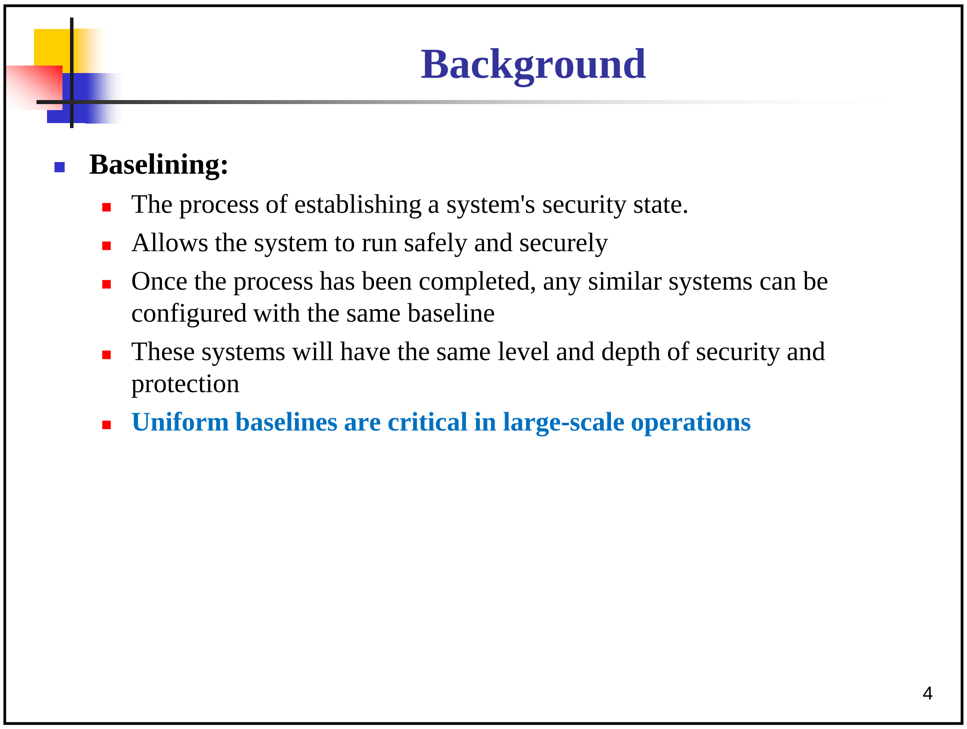
Background

- Various use of systems and operating systems need flexible components
  - Allows users to design, configure, and implement the systems
- This flexibility causes the biggest weaknesses in computer systems.
- Securing systems effectively and consistently requires a structured and logical approach.
  - Basic proactive security can prevent many problems
  - Maintenance involves creating a strategy
    - 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)

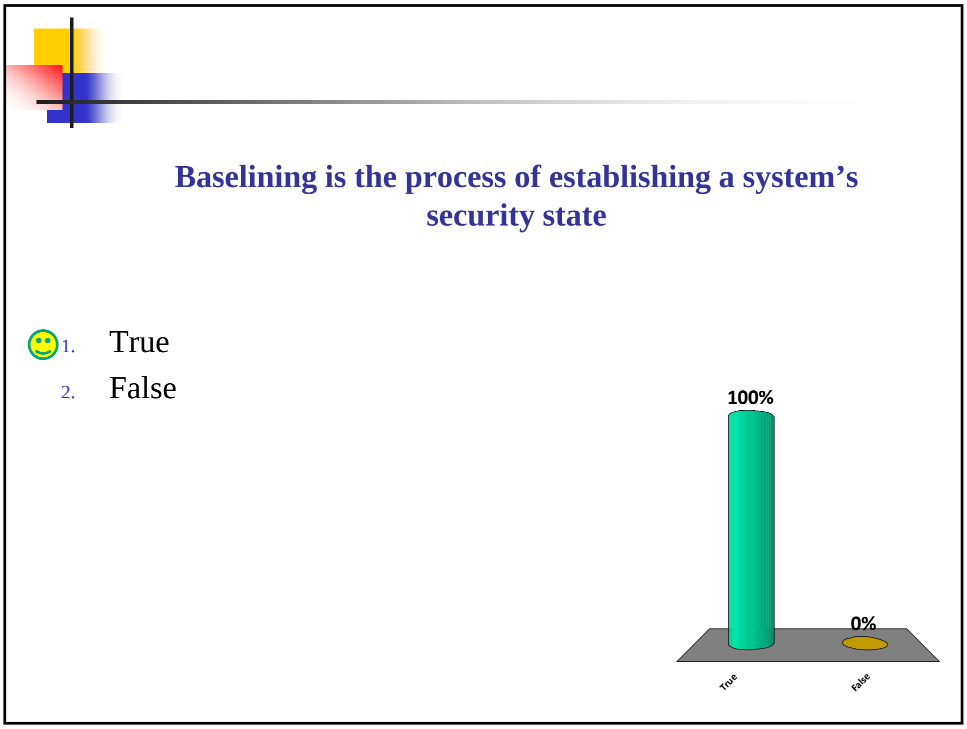
Hardening is iterative and changing

Hardening may not discourage a persistent attacker



Background

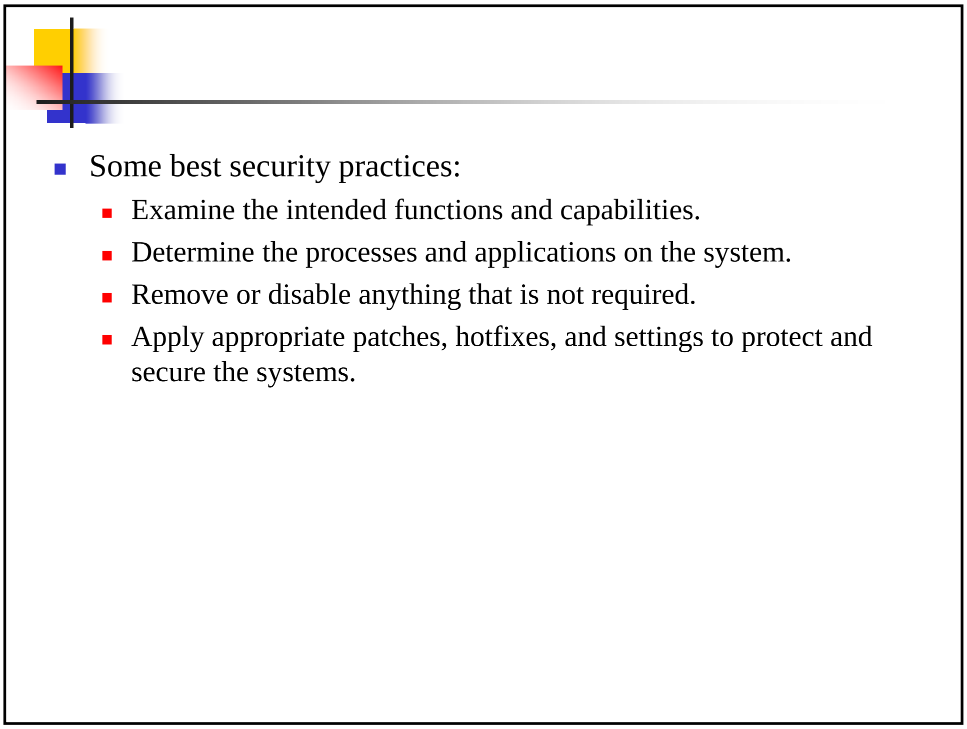
- **Baselining:**
  - The process of establishing a system's security state.
  - Allows the system to run safely and securely
  - Once the process has been completed, any similar systems can be configured with the same baseline
  - These systems will have the same level and depth of security and protection
  - **Uniform baselines are critical in large-scale operations**



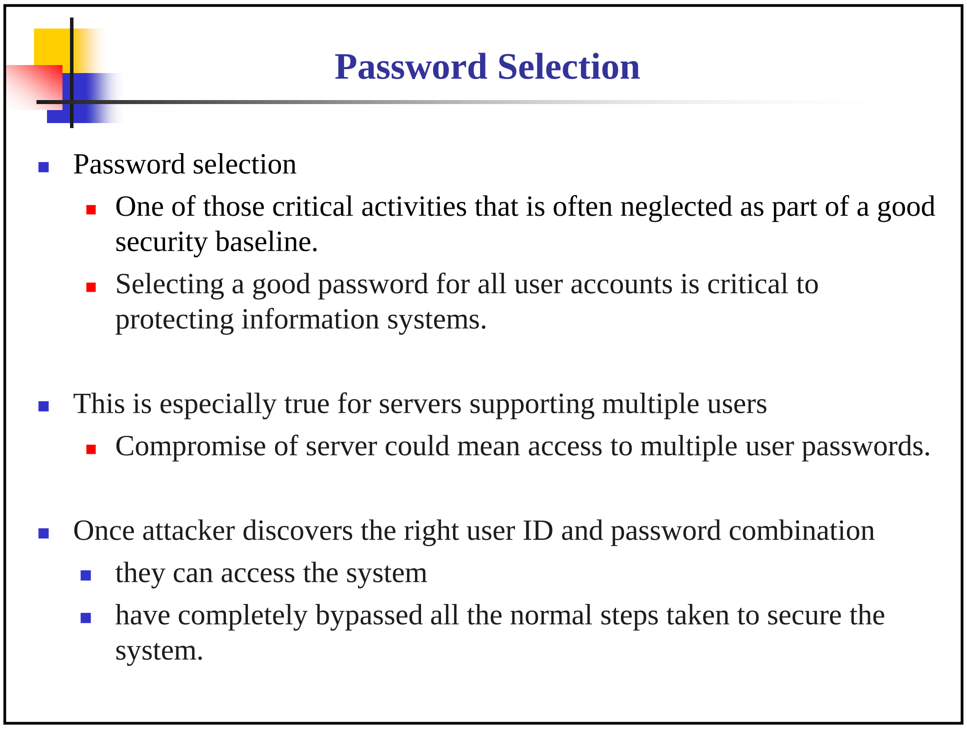
Baselining is the process of establishing a system’s security state

☺ 1. True
2. False

100%
0%
True
False



- Some best security practices:
  - Examine the intended functions and capabilities.
  - Determine the processes and applications on the system.
  - Remove or disable anything that is not required.
  - Apply appropriate patches, hotfixes, and settings to protect and secure the systems.

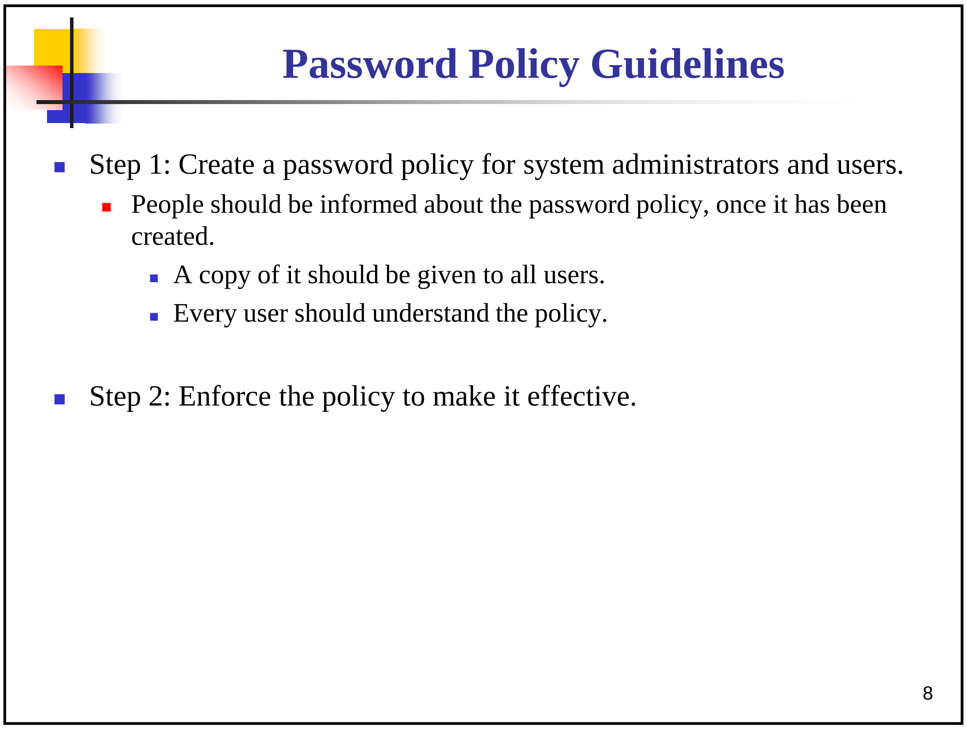


Password Selection

- Password selection
  - One of those critical activities that is often neglected as part of a good security baseline.
  - Selecting a good password for all user accounts is critical to protecting information systems.

- This is especially true for servers supporting multiple users
  - Compromise of server could mean access to multiple user passwords.

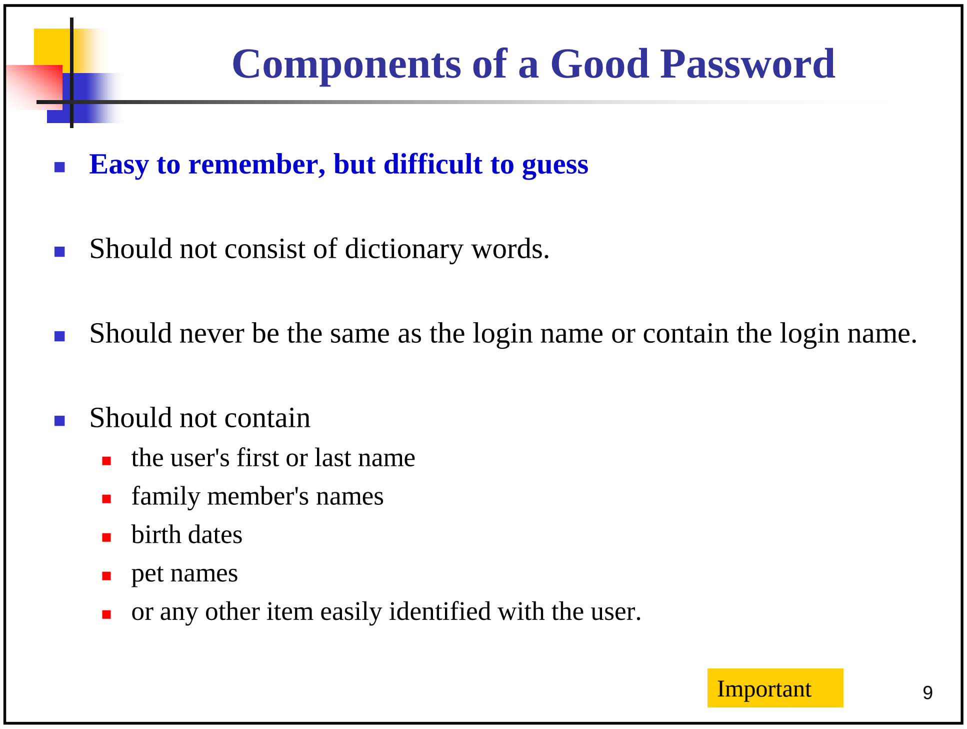
- Once attacker discovers the right user ID and password combination
  - they can access the system
  - have completely bypassed all the normal steps taken to secure the system.



Password Policy Guidelines

- Step 1: Create a password policy for system administrators and users.
  - People should be informed about the password policy, once it has been created.
    - A copy of it should be given to all users.
    - Every user should understand the policy.

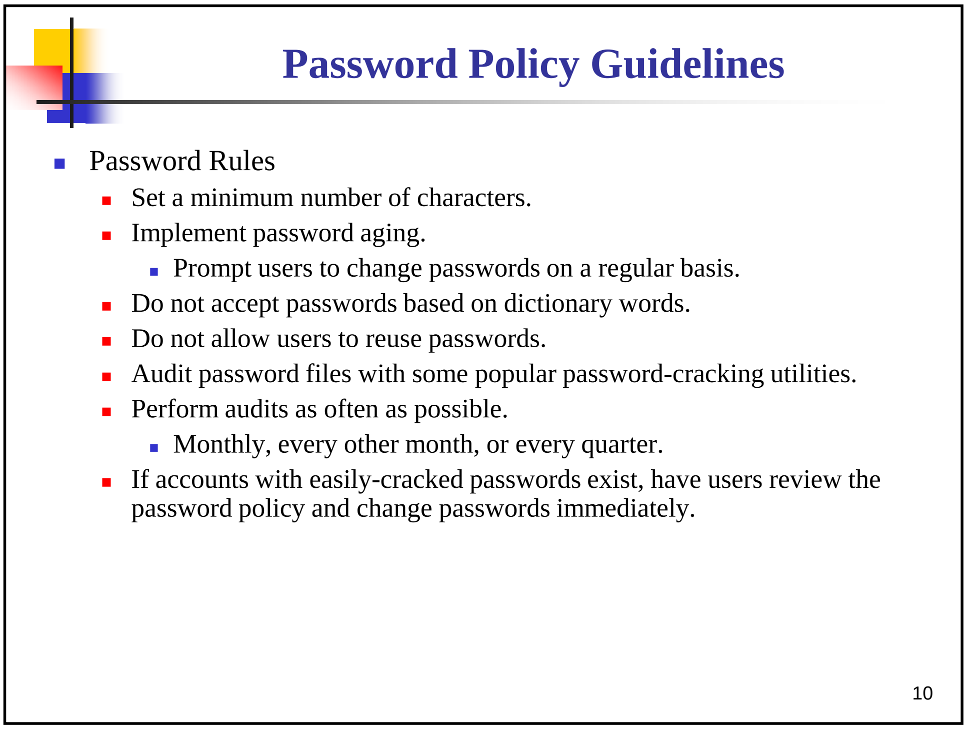
- Step 2: Enforce the policy to make it effective.



Components of a Good Password

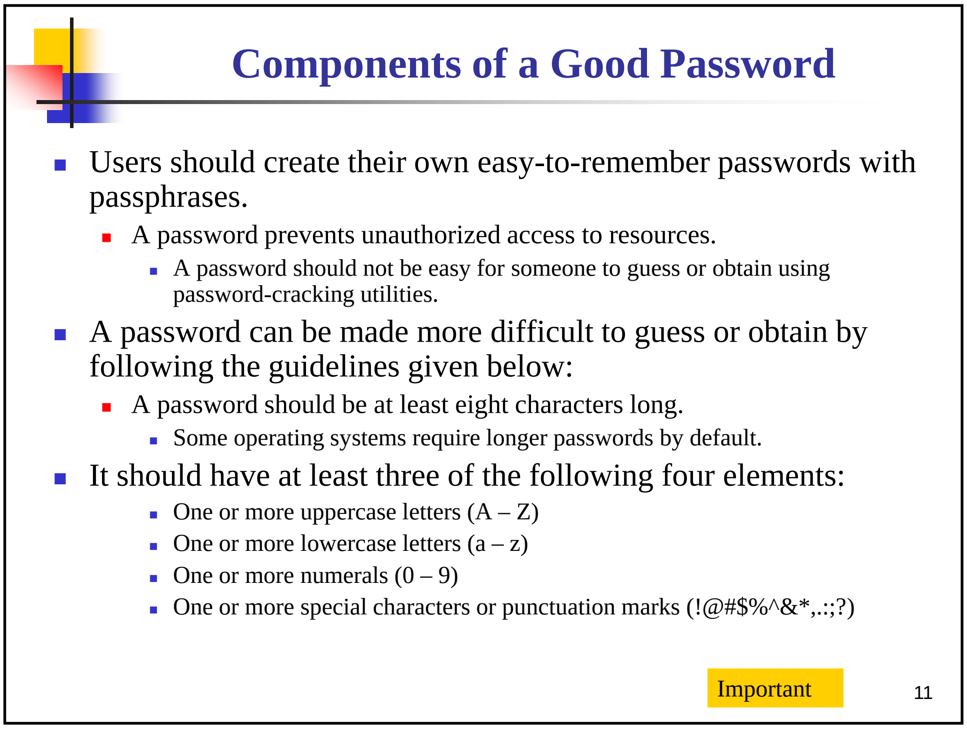
- **Easy to remember, but difficult to guess**
- Should not consist of dictionary words.
- Should never be the same as the login name or contain the login name.
- Should not contain
  - the user's first or last name
  - family member's names
  - birth dates
  - pet names
  - or any other item easily identified with the user.

Important



Password Policy Guidelines

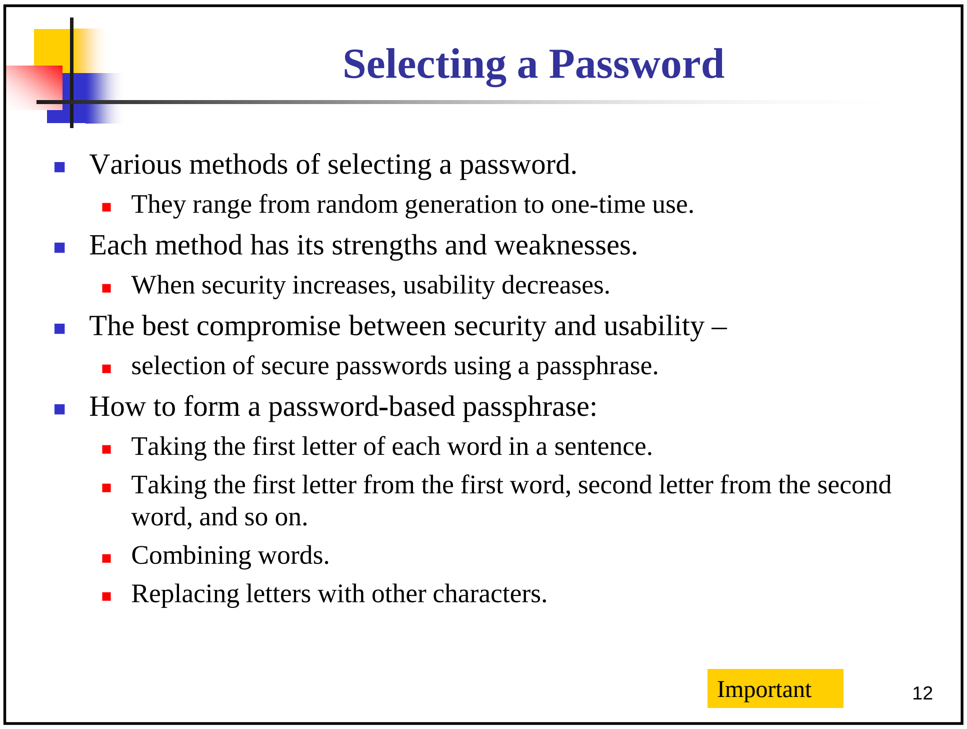
- Password Rules
  - Set a minimum number of characters.
  - Implement password aging.
    - Prompt users to change passwords on a regular basis.
  - Do not accept passwords based on dictionary words.
  - Do not allow users to reuse passwords.
  - Audit password files with some popular password-cracking utilities.
  - Perform audits as often as possible.
    - Monthly, every other month, or every quarter.
  - If accounts with easily-cracked passwords exist, have users review the password policy and change passwords immediately.



Components of a Good Password

- Users should create their own easy-to-remember passwords with passphrases.
  - A password prevents unauthorized access to resources.
    - A password should not be easy for someone to guess or obtain using password-cracking utilities.
- A password can be made more difficult to guess or obtain by following the guidelines given below:
  - A password should be at least eight characters long.
    - Some operating systems require longer passwords by default.
- It should have at least three of the following four elements:
    - One or more uppercase letters (A – Z)
    - One or more lowercase letters (a – z)
    - One or more numerals (0 – 9)
    - One or more special characters or punctuation marks (!@#$%^&*,.:;?)

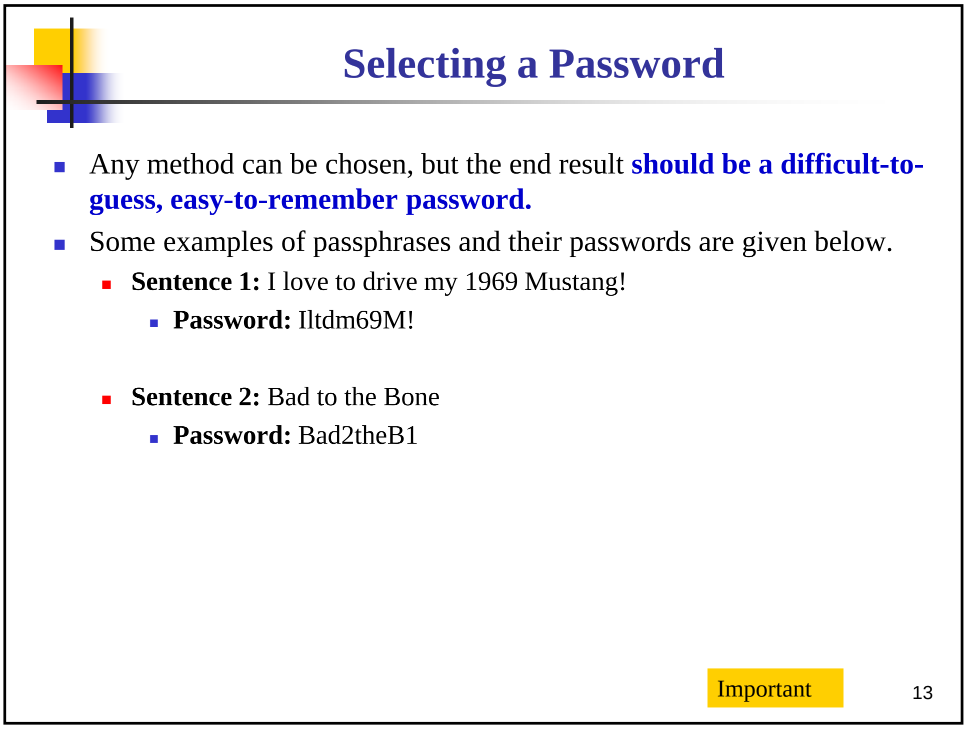
Important



Selecting a Password

- Various methods of selecting a password.
  - They range from random generation to one-time use.
- Each method has its strengths and weaknesses.
  - When security increases, usability decreases.
- The best compromise between security and usability –
  - selection of secure passwords using a passphrase.
- How to form a password-based passphrase:
  - Taking the first letter of each word in a sentence.
  - Taking the first letter from the first word, second letter from the second word, and so on.
  - Combining words.
  - Replacing letters with other characters.

Important

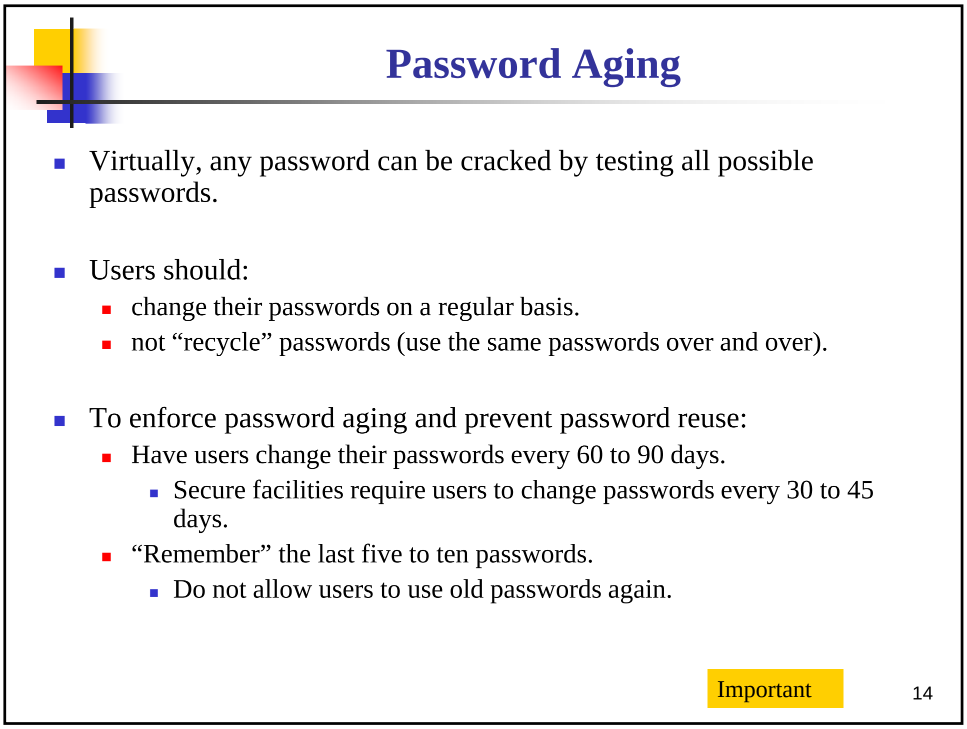


Selecting a Password

- Any method can be chosen, but the end result **should be a difficult-to-guess, easy-to-remember password.**
- Some examples of passphrases and their passwords are given below.
  - **Sentence 1:** I love to drive my 1969 Mustang!
    - **Password:** Iltdm69M!
  - **Sentence 2:** Bad to the Bone
    - **Password:** Bad2theB1

Important

13



Password Aging

- Virtually, any password can be cracked by testing all possible passwords.
- Users should:
  - change their passwords on a regular basis.
  - not "recycle" passwords (use the same passwords over and over).
- To enforce password aging and prevent password reuse:
  - Have users change their passwords every 60 to 90 days.
    - Secure facilities require users to change passwords every 30 to 45 days.
  - "Remember" the last five to ten passwords.
    - Do not allow users to use old passwords again.

Important

14

Hardening Operating Systems

- The operating system (OS) handles tasks such as:
  - Input
  - Output
  - Display
  - Memory management
- Supports the user environment and applications.
- A network operating system (NOS)
  - includes additional functions and capabilities to assist in connecting computers and devices.

- Operating system developers and manufacturers share a common problem.
  - No way to anticipate the configurations and variations users require from their products.
- Instead of spending time and money to meet every need, manufacturers provide a “default” installation for their products.
  - Contain the base operating system and some commonly desirable options, such as drivers, utilities, and enhancements.
- Manufacturer-provided recommendations or tools and settings facilitate securing the system.
- **End users are responsible for securing their systems**.

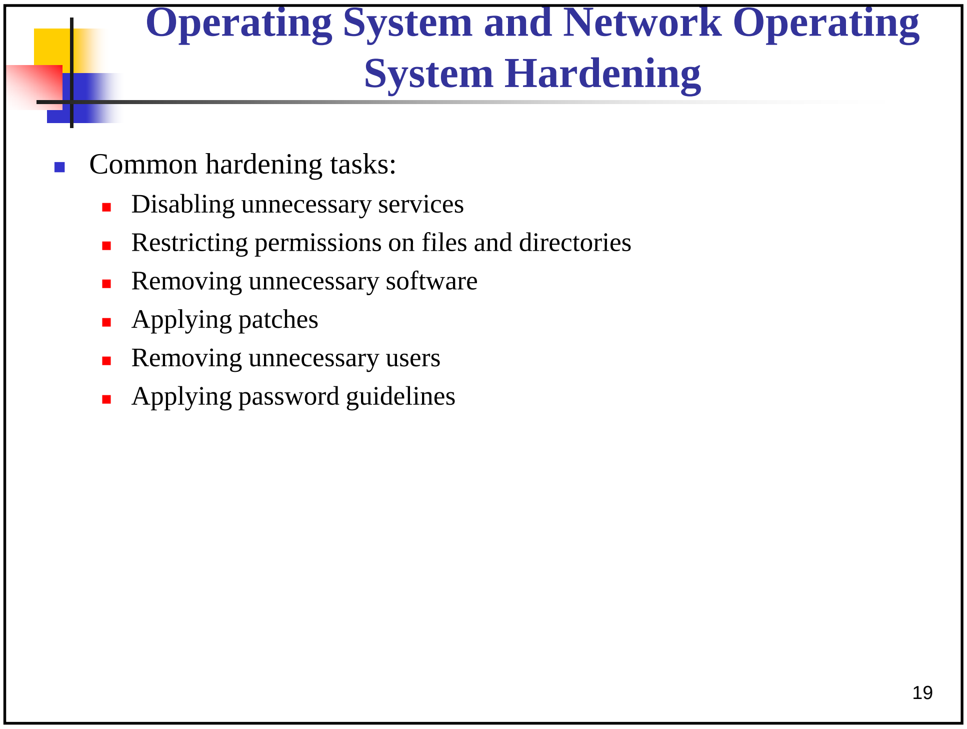
Well-Known Operating System Risks

- Attackers well aware of the security vulnerabilities in operating systems
- The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities is an up-to-date list of known vulnerabilities for Windows and UNIX operating systems
- Current lists along with detailed descriptions of the vulnerabilities available at

  http://www.sans.org/top20/

Hardening Operating Systems

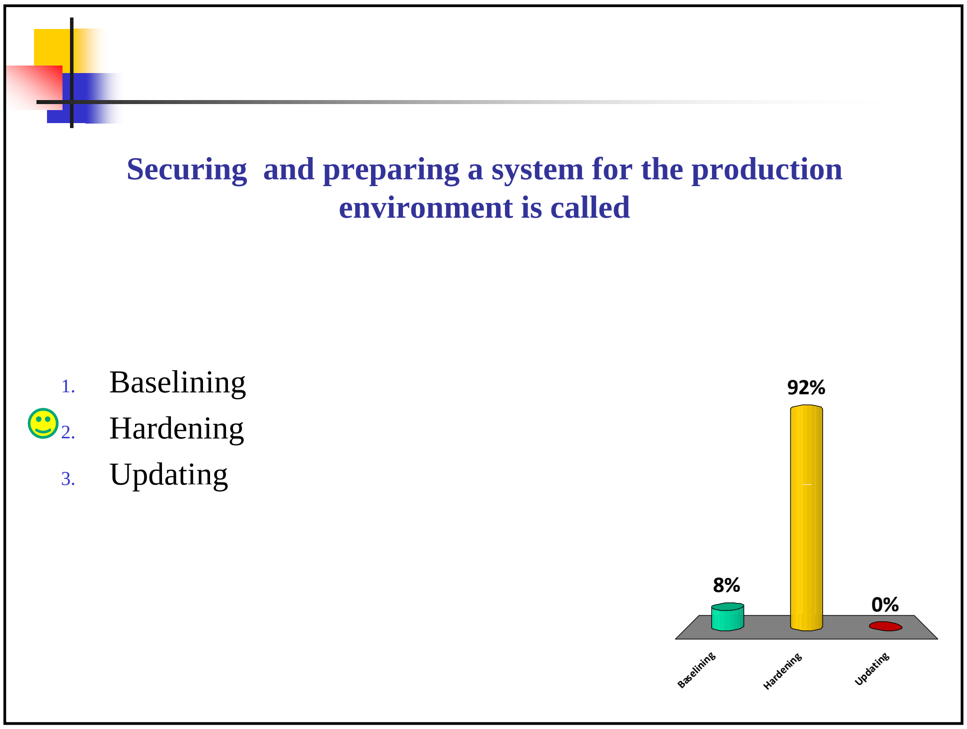
- **Hardening**
  - The process of securing an operating system for production environment is called.
  - Makes the system more resistant to attacks.
- Each operating system has its own approach to security.
  - The process of hardening is the same.
  - Different steps must be taken to secure each operating system.



Operating System and Network Operating System Hardening

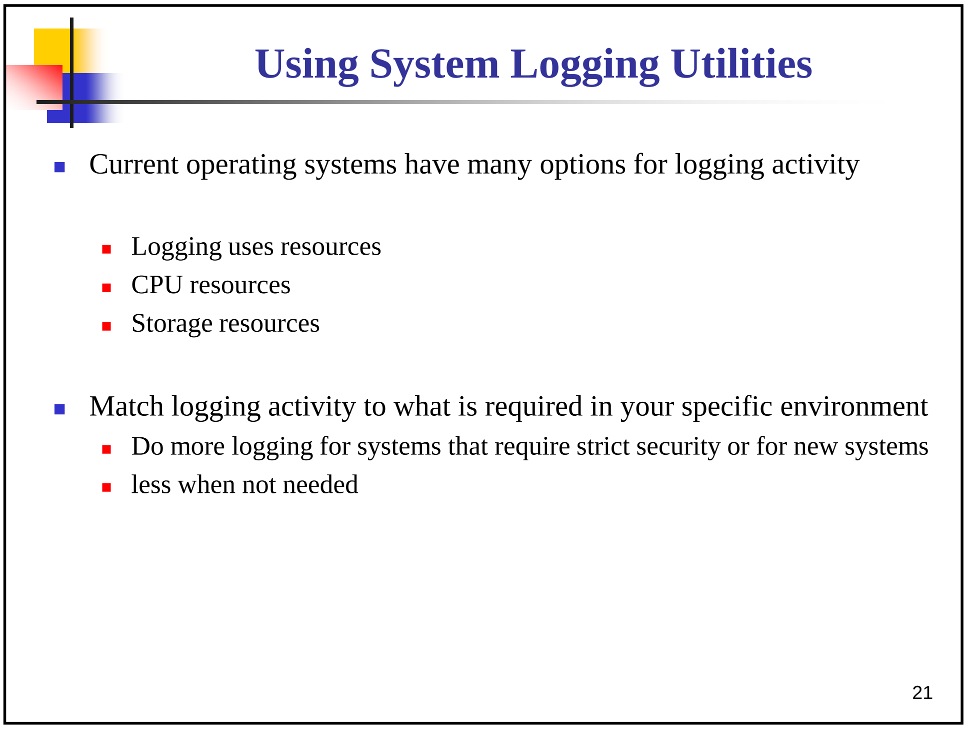
- Common hardening tasks:
  - Disabling unnecessary services
  - Restricting permissions on files and directories
  - Removing unnecessary software
  - Applying patches
  - Removing unnecessary users
  - Applying password guidelines

19



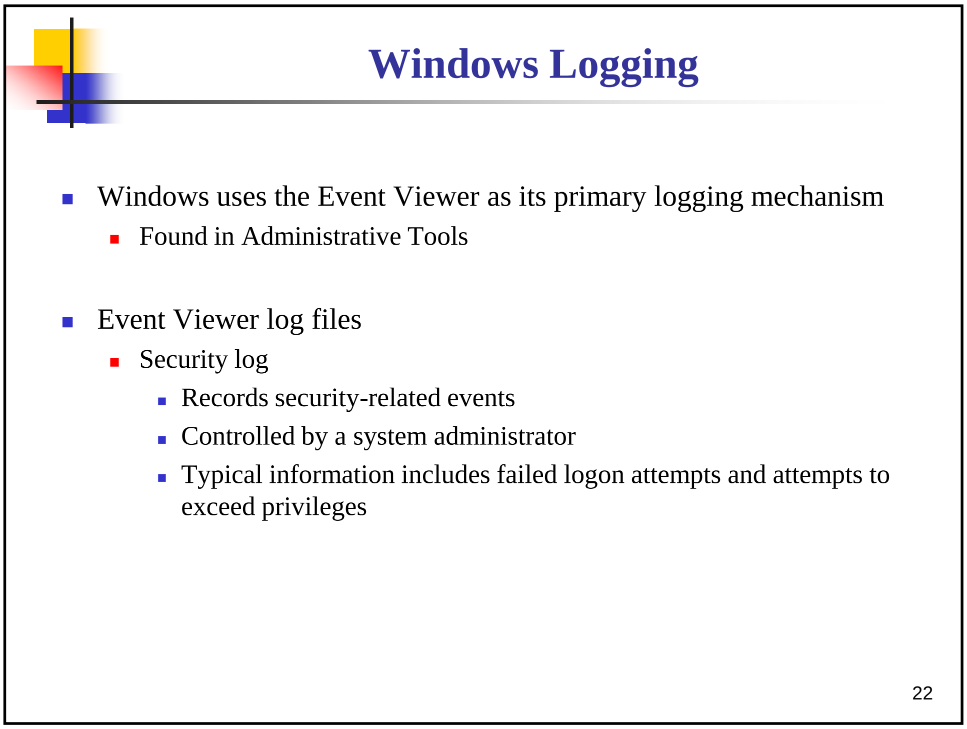
Securing and preparing a system for the production environment is called

1. Baselining
2. ☺ Hardening
3. Updating



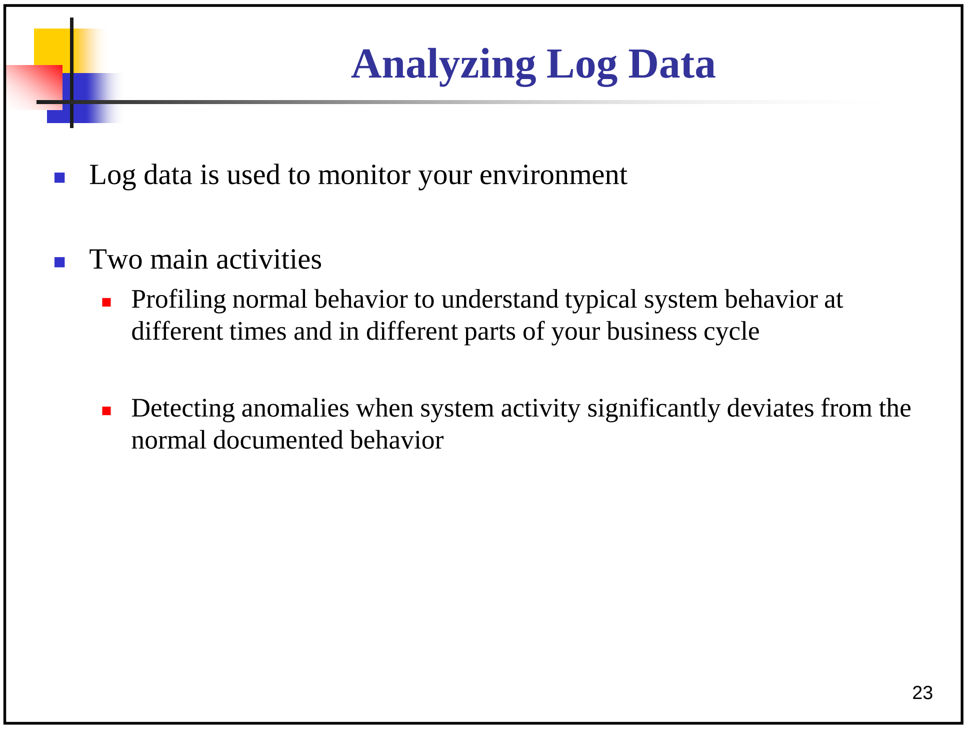
Using System Logging Utilities

- Current operating systems have many options for logging activity
  - Logging uses resources
  - CPU resources
  - Storage 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



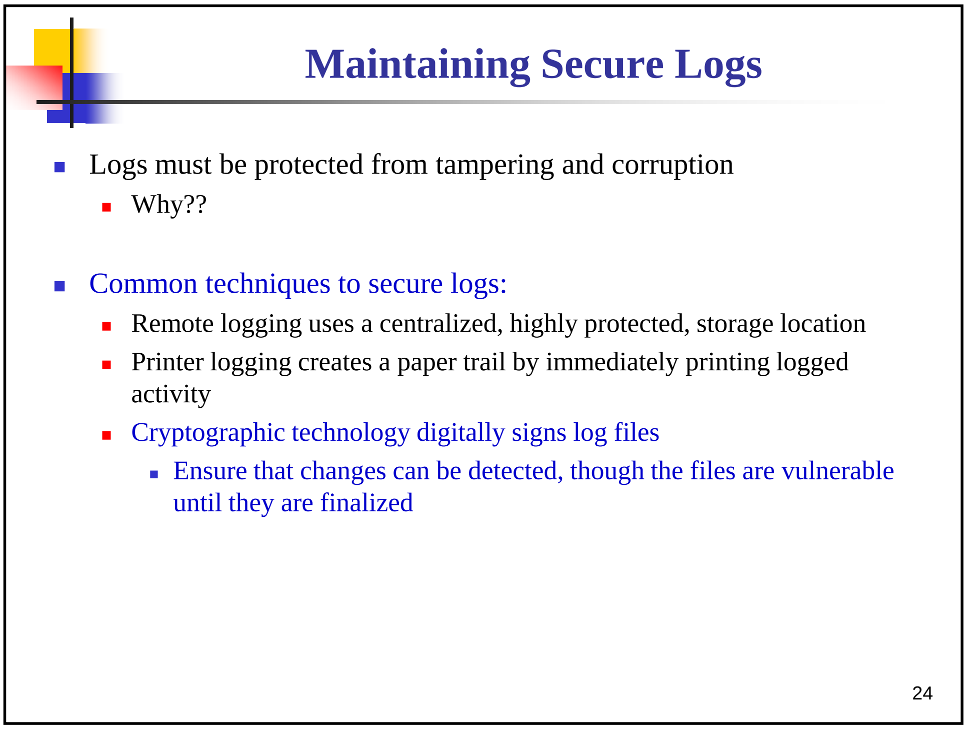
Windows Logging

- Windows uses the Event Viewer as its primary logging mechanism
  - Found in Administrative Tools
- Event Viewer log files
  - Security log
    - Records security-related events
    - Controlled by a system administrator
    - Typical information includes failed logon attempts and attempts to exceed privileges



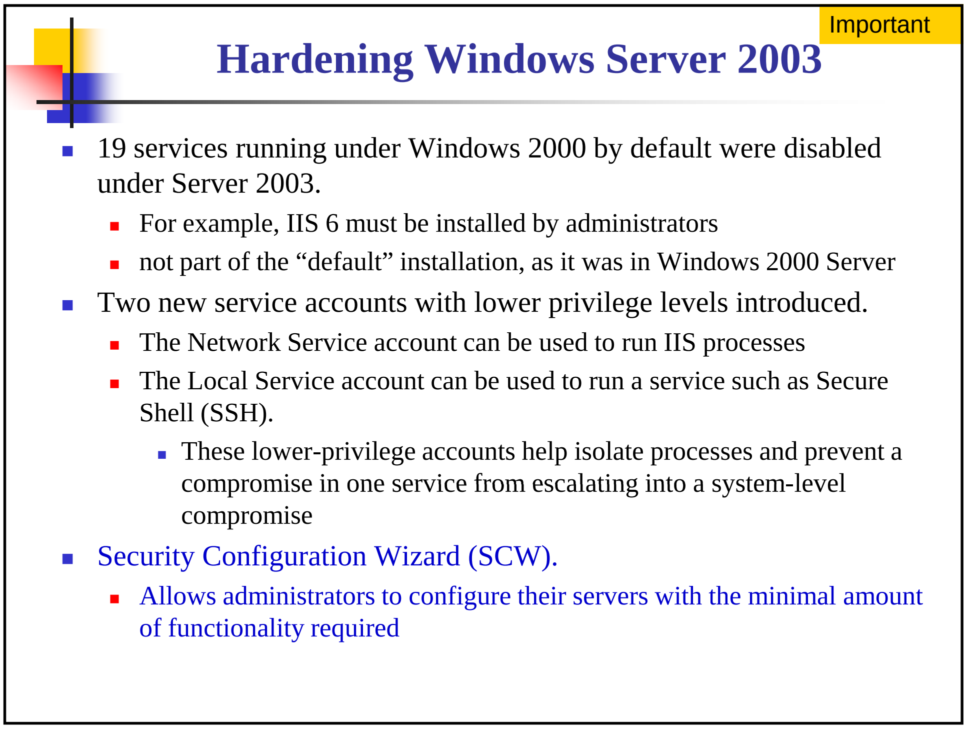
Analyzing Log Data

- Log data is used to monitor your environment
- Two main activities
  - Profiling normal behavior to understand typical system behavior at different times and in different parts of your business cycle
  - Detecting anomalies when system activity significantly deviates from the normal documented behavior



Maintaining Secure Logs

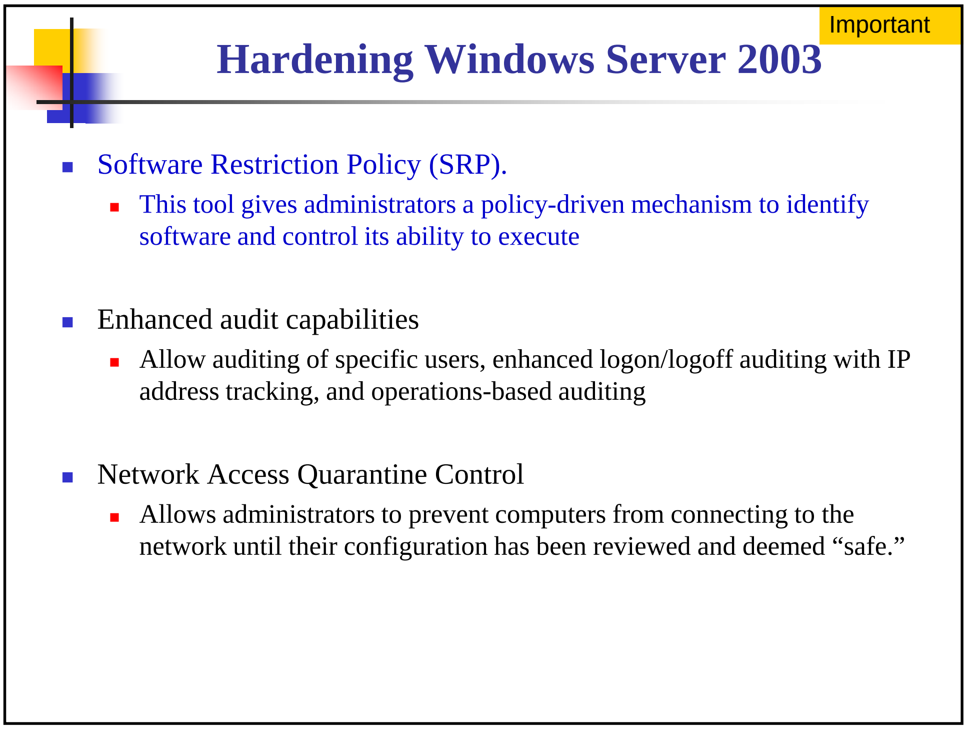
- Logs must be protected from tampering and corruption
  - Why??
- Common techniques to secure logs:
  - Remote logging uses a centralized, highly protected, storage location
  - Printer logging creates a paper trail by immediately printing logged activity
  - Cryptographic technology digitally signs log files
    - Ensure that changes can be detected, though the files are vulnerable until they are finalized



Important

Hardening Windows Server 2003

- 19 services running under Windows 2000 by default were disabled under Server 2003.
  - For example, IIS 6 must be installed by administrators
  - not part of the “default” installation, as it was in Windows 2000 Server
- Two new service accounts with lower privilege levels introduced.
  - The Network Service account can be used to run IIS processes
  - The Local Service account can be used to run a service such as Secure Shell (SSH).
    - These lower-privilege accounts help isolate processes and prevent a compromise in one service from escalating into a system-level compromise
- Security Configuration Wizard (SCW).
  - Allows administrators to configure their servers with the minimal amount of functionality required



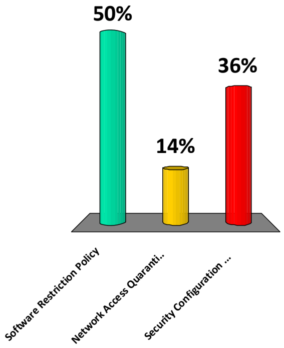
Important

Hardening Windows Server 2003

- Software Restriction Policy (SRP).
  - This tool gives administrators a policy-driven mechanism to identify software and control its ability to execute
- Enhanced audit capabilities
  - Allow auditing of specific users, enhanced logon/logoff auditing with IP address tracking, and operations-based auditing
- Network Access Quarantine Control
  - Allows administrators to prevent computers from connecting to the network until their configuration has been reviewed and deemed “safe.”

________gives administrators a policy-driven mechanism to identify software and control its ability to execute

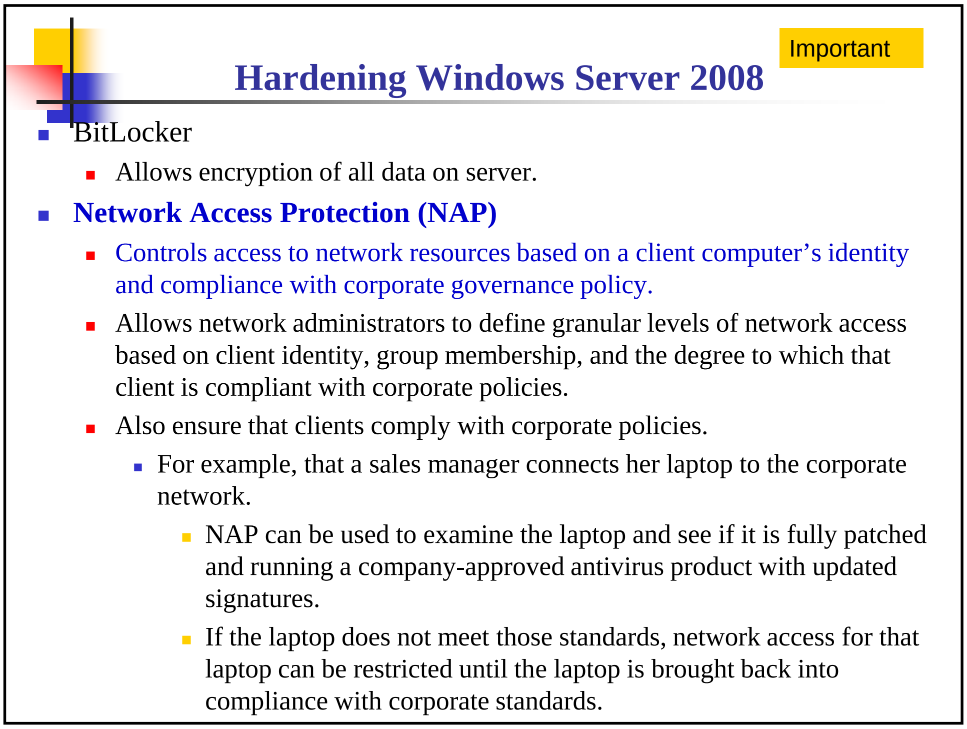
☺ 1. Software Restriction Policy
2. Network Access Quarantine Control
3. Security Configuration Wizard



Hardening Windows Vista

Important

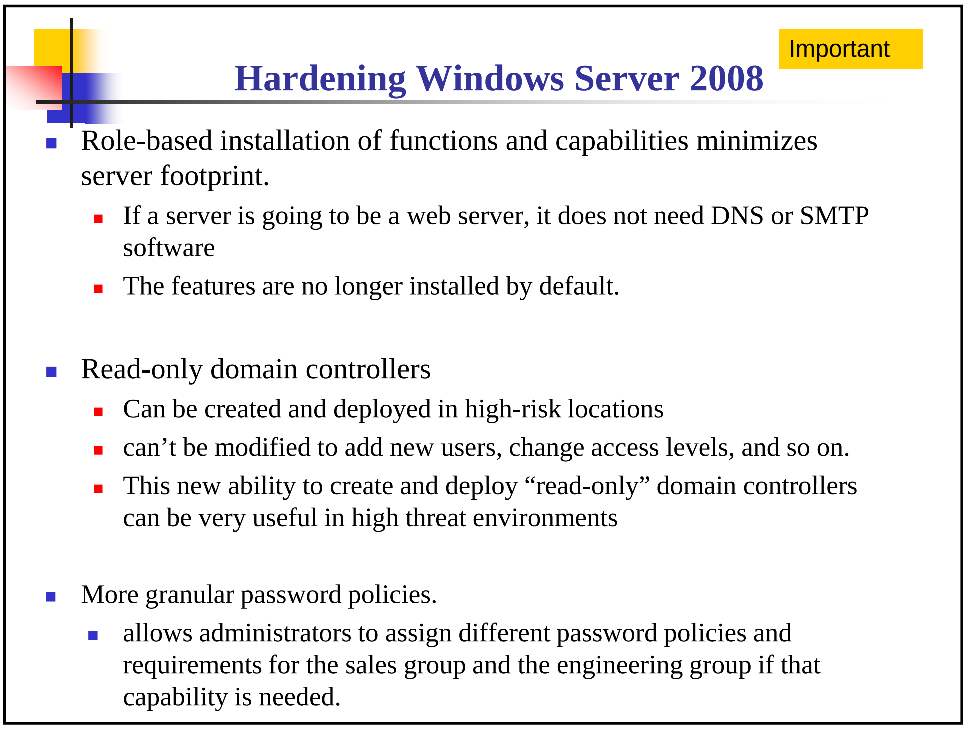
- User Account Control
  - allows users to operate the system without requiring administrative privileges.
- An outbound filtering capability added to Windows Firewall.
  - Allows filtering of traffic coming into and leaving the system, which is useful for controlling things like peer-to-peer applications.
- BitLocker
  - allows encryption of all data on a server, including any data volumes.
- Vista clients work with Network Access Protection (NAP).
  - Refer Hardening Windows Server 2008
- Windows Defender
  - A built-in malware detection and removal tool.
- A new, more-secure version of Internet Explorer.



Important

Hardening Windows Server 2008

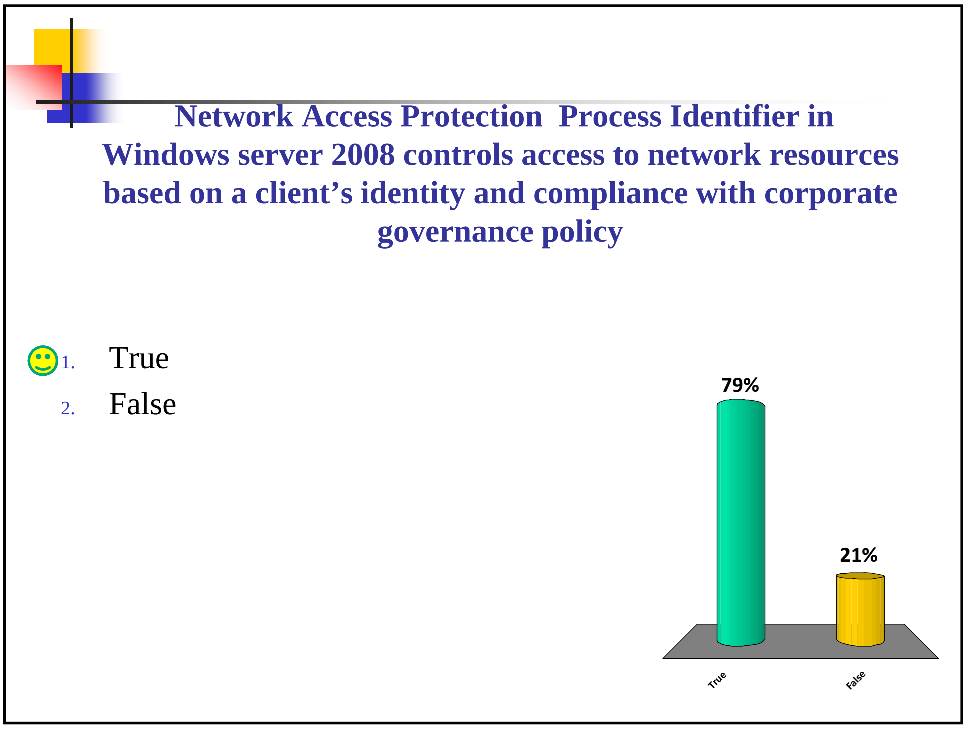
- BitLocker
  - Allows encryption of all data on server.
- **Network Access Protection (NAP)**
  - Controls access to network resources based on a client computer's identity and compliance with corporate governance policy.
  - Allows network administrators to define granular levels of network access based on client identity, group membership, and the degree to which that client is compliant with corporate policies.
  - Also ensure that clients comply with corporate policies.
    - For example, that a sales manager connects her laptop to the corporate network.
      - NAP can be used to examine the laptop and see if it is fully patched and running a company-approved antivirus product with updated signatures.
      - If the laptop does not meet those standards, network access for that laptop can be restricted until the laptop is brought back into compliance with corporate standards.



Important

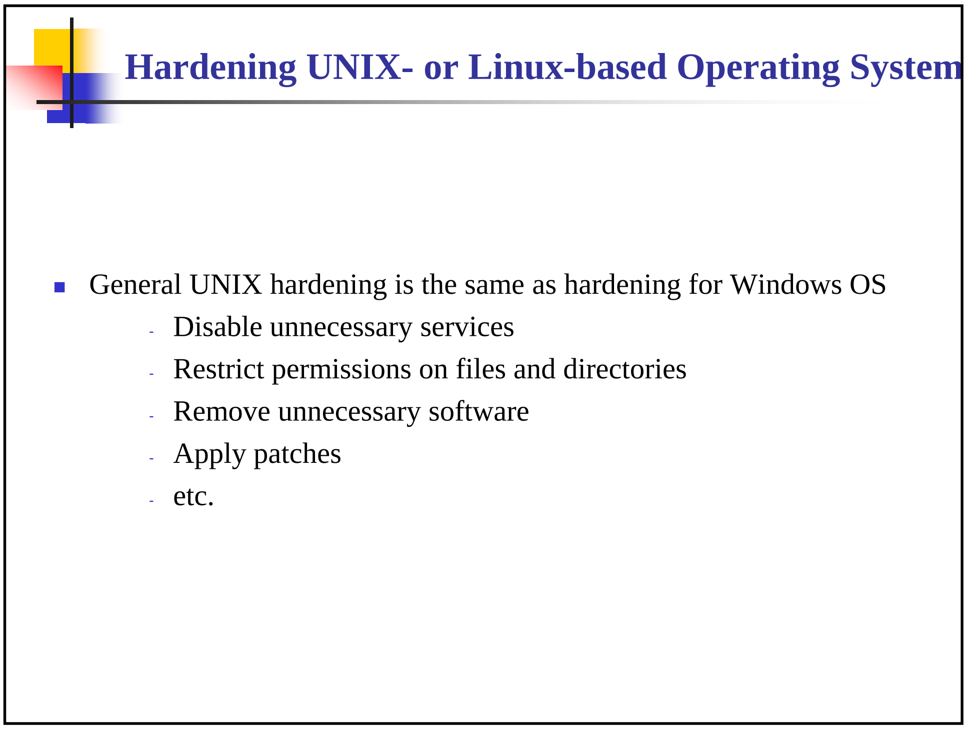
Hardening Windows Server 2008

- Role-based installation of functions and capabilities minimizes server footprint.
  - If a server is going to be a web server, it does not need DNS or SMTP software
  - The features are no longer installed by default.
- Read-only domain controllers
  - Can be created and deployed in high-risk locations
  - can't be modified to add new users, change access levels, and so on.
  - This new ability to create and deploy "read-only" domain controllers can be very useful in high threat environments
- More granular password policies.
  - allows administrators to assign different password policies and requirements for the sales group and the engineering group if that capability is needed.



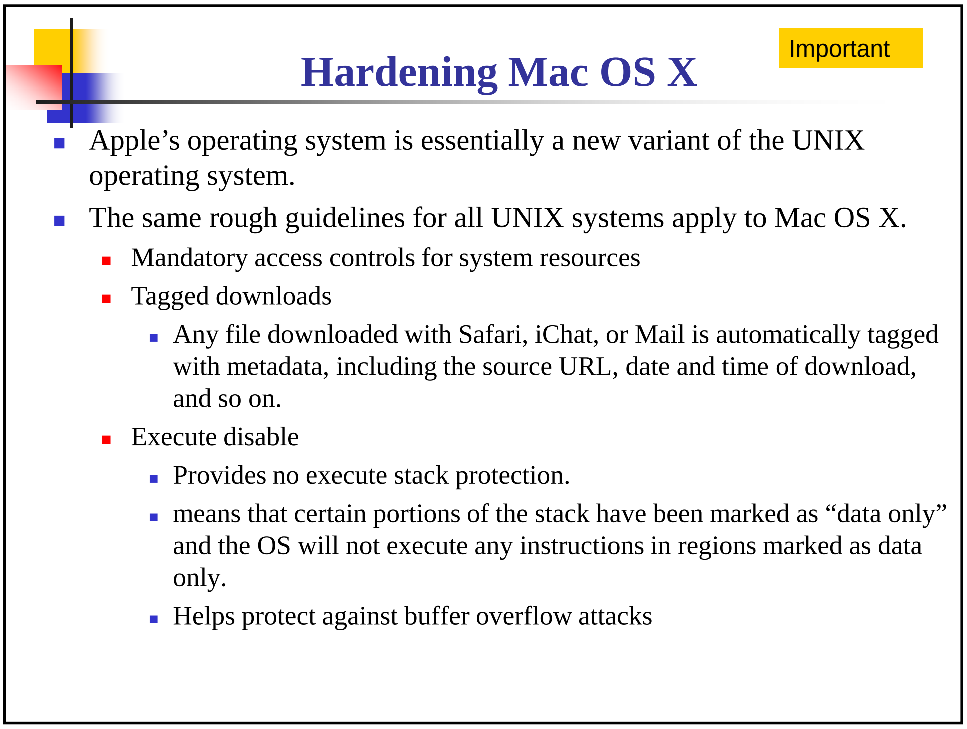
Network Access Protection Process Identifier in Windows server 2008 controls access to network resources based on a client's identity and compliance with corporate governance policy

☺ 1. True
2. False



Hardening UNIX- or Linux-based Operating System

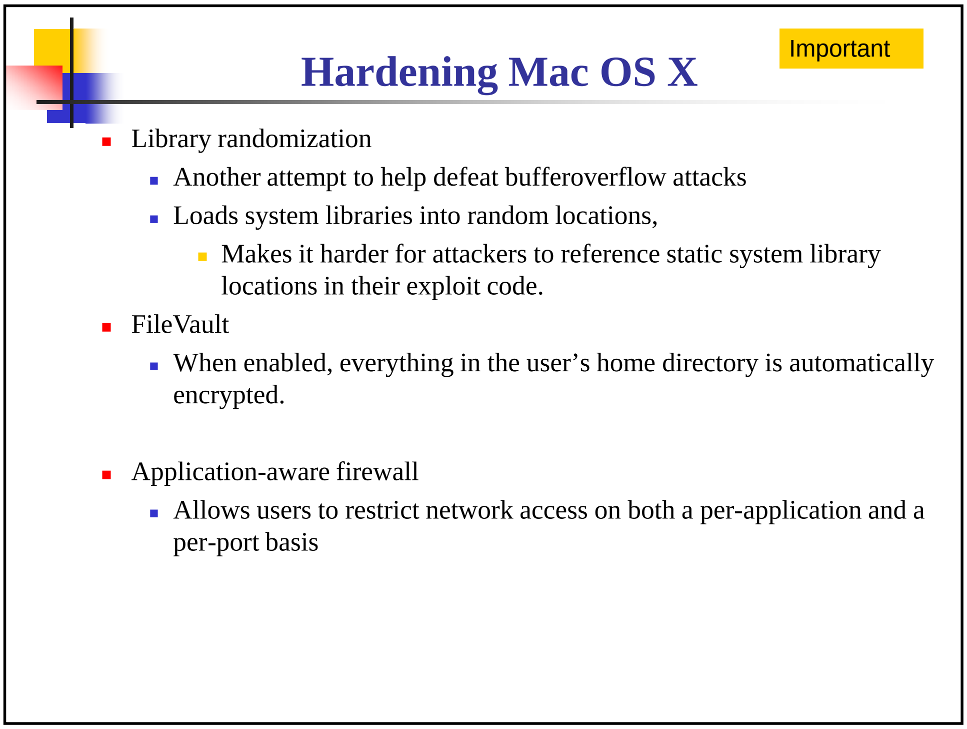
- General UNIX hardening is the same as hardening for Windows OS
  - Disable unnecessary services
  - Restrict permissions on files and directories
  - Remove unnecessary software
  - Apply patches
  - etc.



Important

Hardening Mac OS X

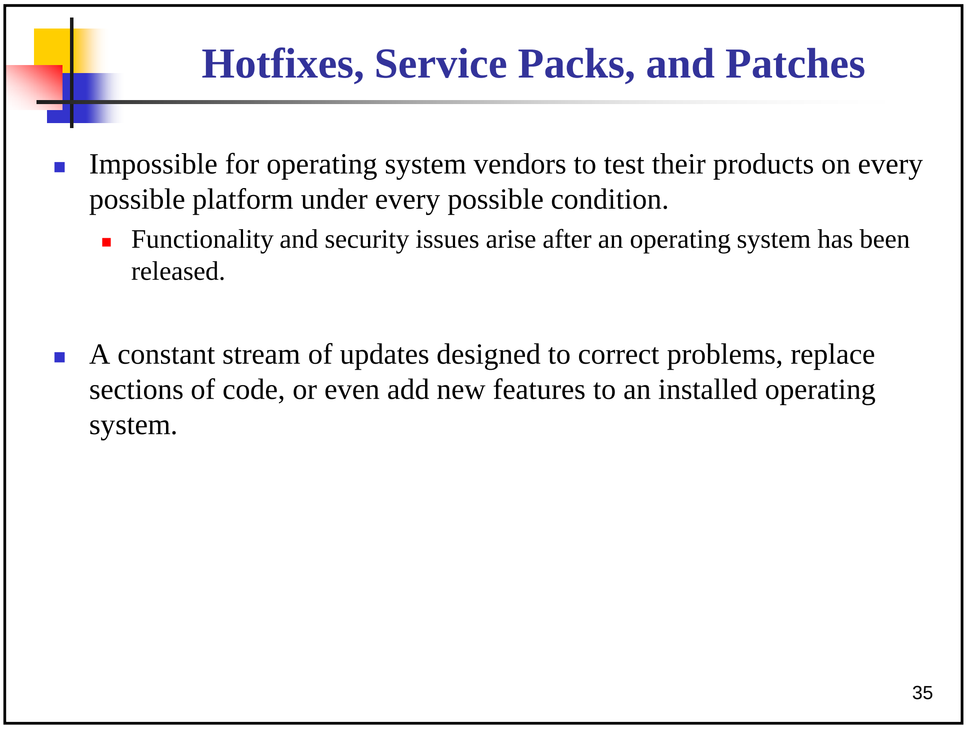
- Apple's operating system is essentially a new variant of the UNIX operating system.
- The same rough guidelines for all UNIX systems apply to Mac OS X.
  - Mandatory access controls for system resources
  - Tagged downloads
    - Any file downloaded with Safari, iChat, or Mail is automatically tagged with metadata, including the source URL, date and time of download, and so on.
  - Execute disable
    - Provides no execute stack protection.
    - means that certain portions of the stack have been marked as "data only" and the OS will not execute any instructions in regions marked as data only.
    - Helps protect against buffer overflow attacks



Important

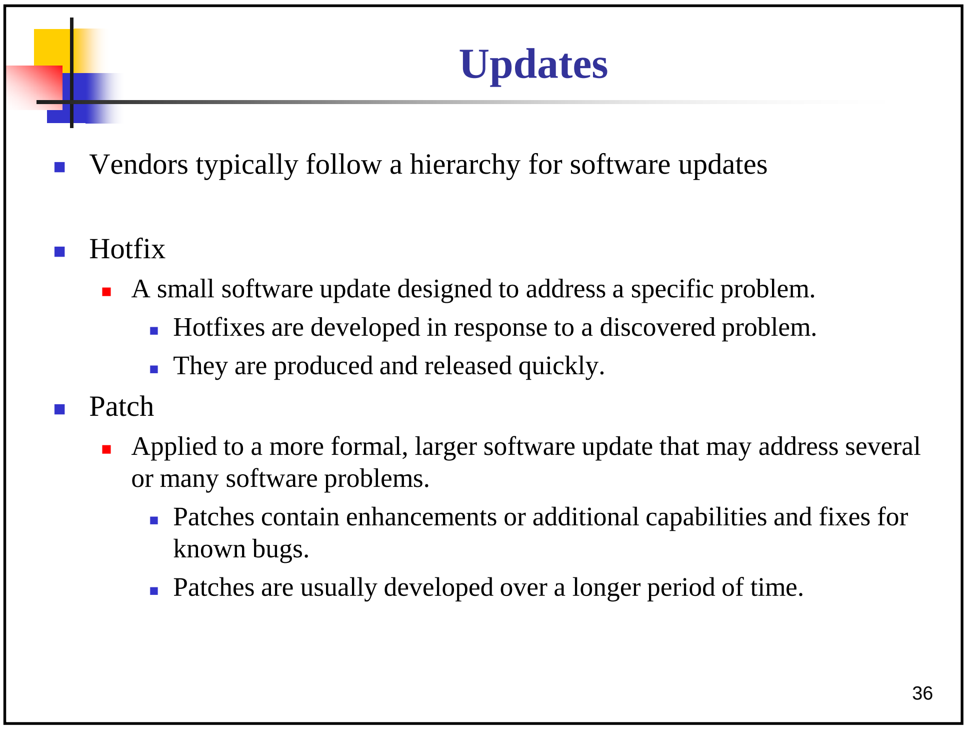
Hardening Mac OS X

- Library randomization
  - Another attempt to help defeat bufferoverflow attacks
  - Loads system libraries into random locations,
    - Makes it harder for attackers to reference static system library locations in their exploit code.
- FileVault
  - When enabled, everything in the user's home directory is automatically encrypted.
- Application-aware firewall
  - Allows users to restrict network access on both a per-application and a per-port basis



Hotfixes, Service Packs, and Patches

- Impossible for operating system vendors to test their products on every possible platform under every possible condition.
  - Functionality and security issues arise after an operating system has been released.
- A constant stream of updates designed to correct problems, replace sections of code, or even add new features to an installed operating system.



Updates

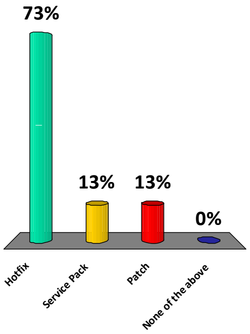
- Vendors typically follow a hierarchy for software updates
- Hotfix
  - A small software update designed to address a specific problem.
    - Hotfixes are developed in response to a discovered problem.
    - They are produced and released quickly.
- Patch
  - Applied to a more formal, larger software update that may address several or many software problems.
    - Patches contain enhancements or additional capabilities and fixes for known bugs.
    - Patches are usually developed over a longer period of time.

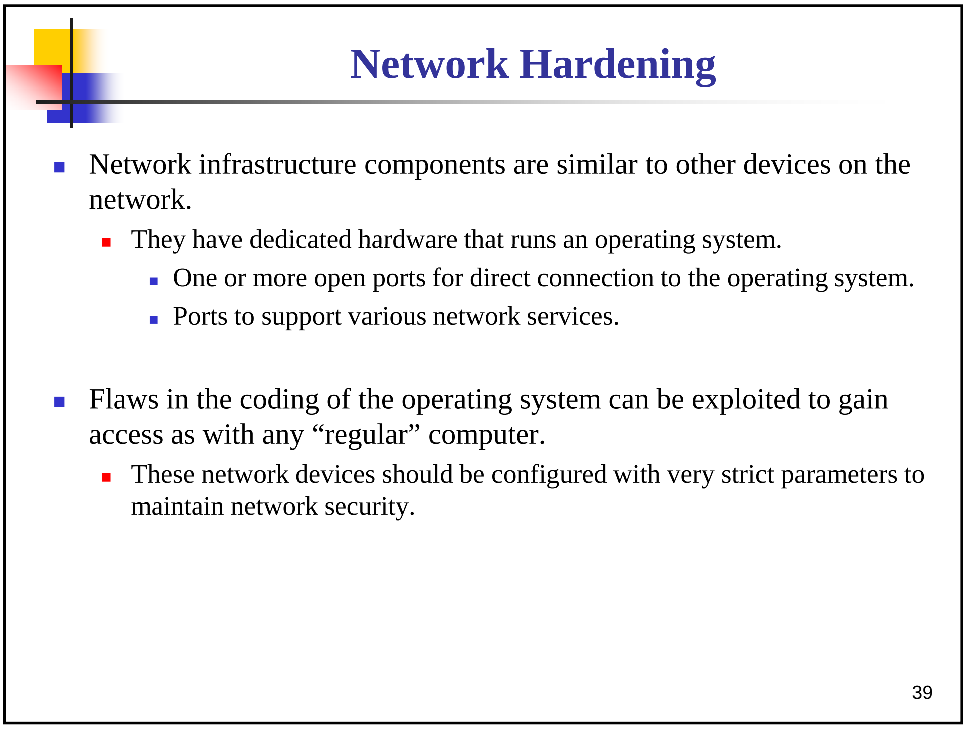
Hotfixes, Service Packs, and Patches

- Service Pack
  - A collection of patches and hotfixes rolled into a single, large package.
    - Service packs are designed to bring a system up to the latest known, good level all at once.
    - The system administrator does not have to download updates separately.
- Independent of the method used to update the operating system, it is important to keep systems up to date.
  - Keeping every system patched and up to date is critical to protecting the system and the information.

A small software update designed to address an urgent or specific problem is

☺ 1. Hotfix
2. Service Pack
3. Patch
4. None of the above

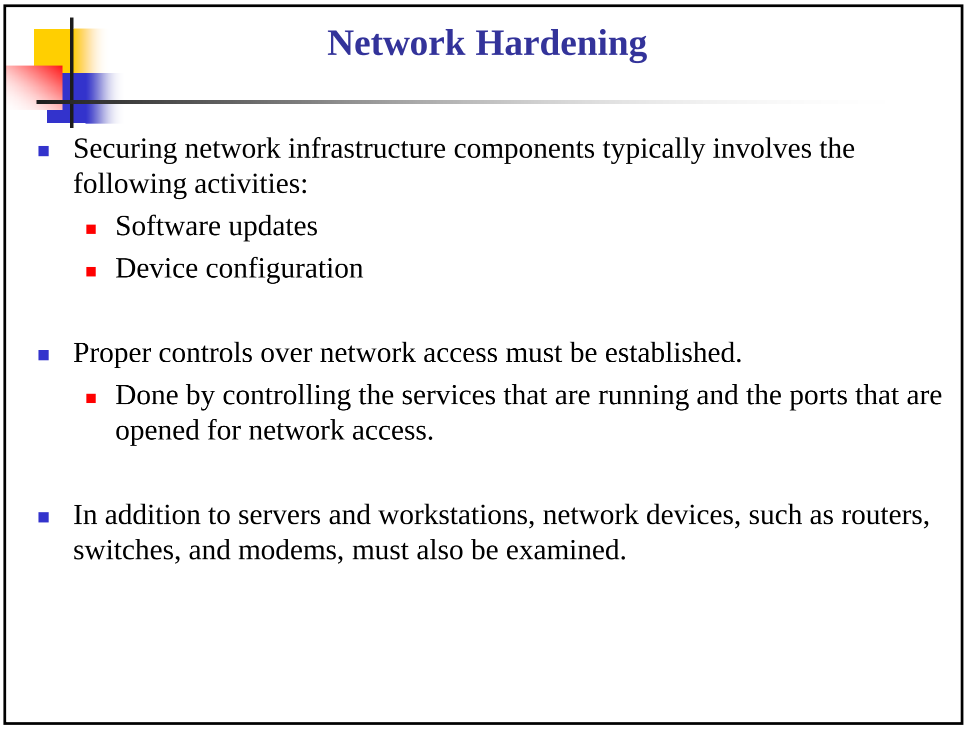




Network Hardening

- Network infrastructure components are similar to other devices on the network.
  - They have dedicated hardware that runs an operating system.
    - One or more open ports for direct connection to the operating system.
    - Ports to support various network services.
- Flaws in the coding of the operating system can be exploited to gain access as with any “regular” computer.
  - These network devices should be configured with very strict parameters to maintain network security.

39



Network Hardening

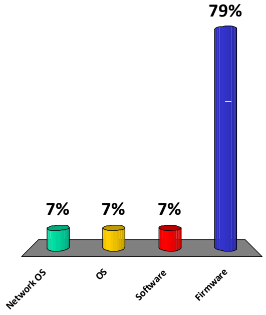
- Securing network infrastructure components typically involves the following activities:
  - Software updates
  - Device configuration
- Proper controls over network access must be established.
  - Done by controlling the services that are running and the ports that are opened for network access.
- In addition to servers and workstations, network devices, such as routers, switches, and modems, must also be examined.

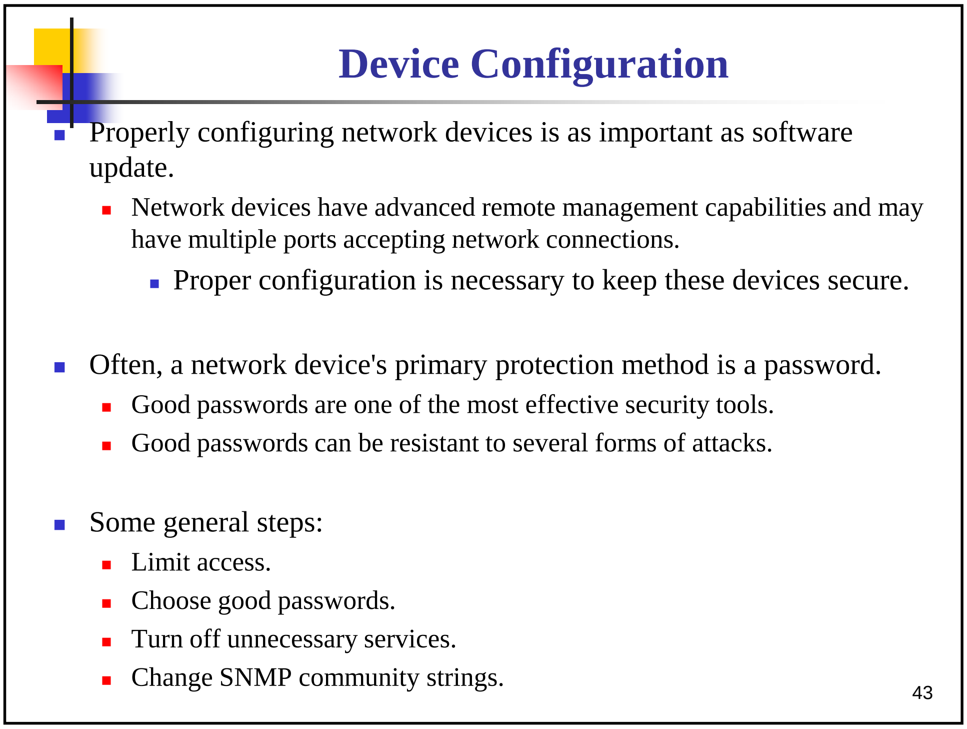
Software Updates

- Maintaining current vendor patch levels is one of the most important to maintain security.
- The different vendors for the different software and hardware must be tracked.
- Software and **firmware** for each device must be kept current.
  - **Firmware:**
    - The fixed, usually rather small, programs and/or data structures (loaded on non volatile RAM) that internally control various electronic devices
    - Updating the software loaded on non volatile RAM is called Firmware update

The fixed programs and/or data structures (loaded on non volatile RAM) that internally control various electronic devices are known as _________

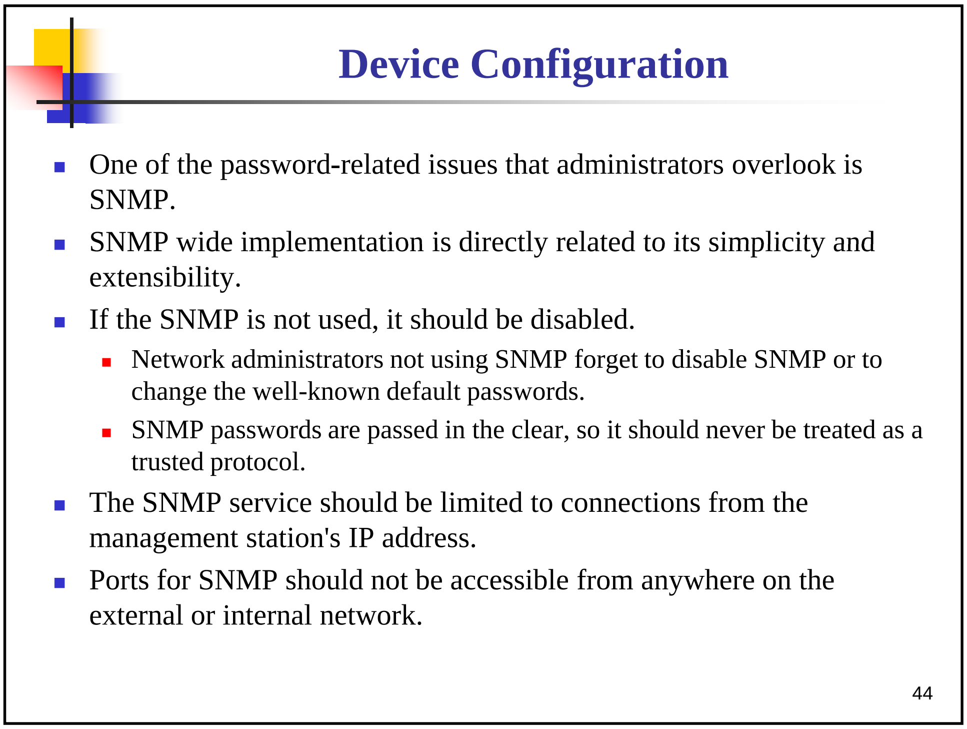
1. Network OS
2. OS
3. Software
4. ☺ Firmware





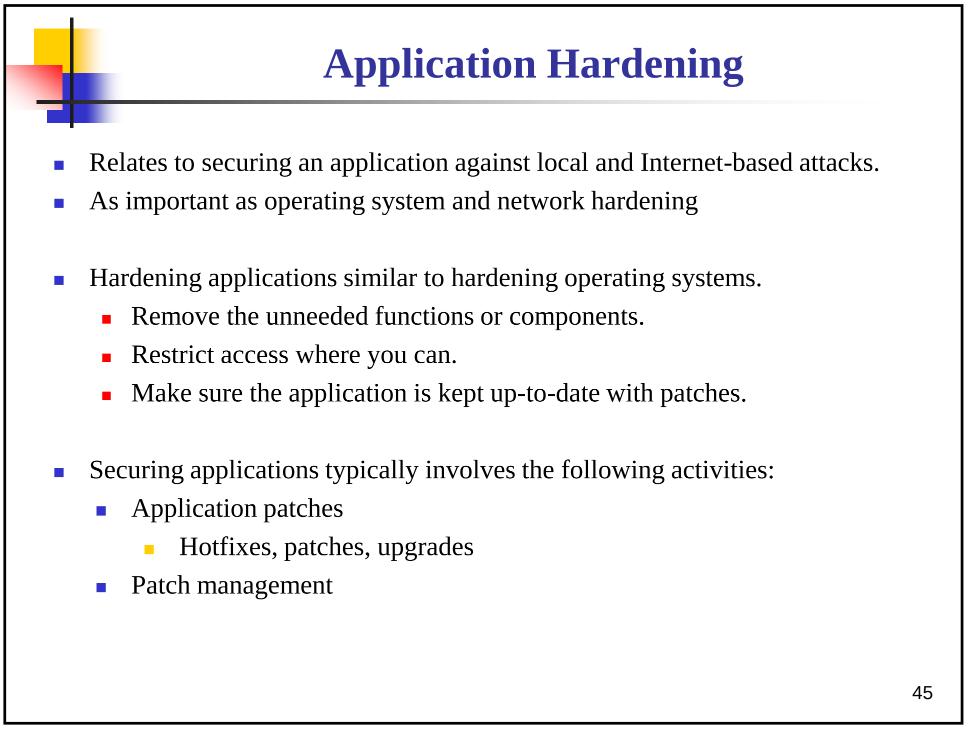
Device Configuration

- Properly configuring network devices is as important as software update.
  - Network devices have advanced remote management capabilities and may have multiple ports accepting network connections.
    - Proper configuration is necessary to keep these devices secure.
- Often, a network device's primary protection method is a password.
  - Good passwords are one of the most effective security tools.
  - Good passwords can be resistant to several forms of attacks.
- Some general steps:
  - Limit access.
  - Choose good passwords.
  - Turn off unnecessary services.
  - Change SNMP community strings.



Device Configuration

- One of the password-related issues that administrators overlook is SNMP.
- SNMP wide implementation is directly related to its simplicity and extensibility.
- If the SNMP is not used, it should be disabled.
  - Network administrators not using SNMP forget to disable SNMP or to change the well-known default passwords.
  - SNMP passwords are passed in the clear, so it should never be treated as a trusted protocol.
- The SNMP service should be limited to connections from the management station's IP address.
- Ports for SNMP should not be accessible from anywhere on the external or internal network.

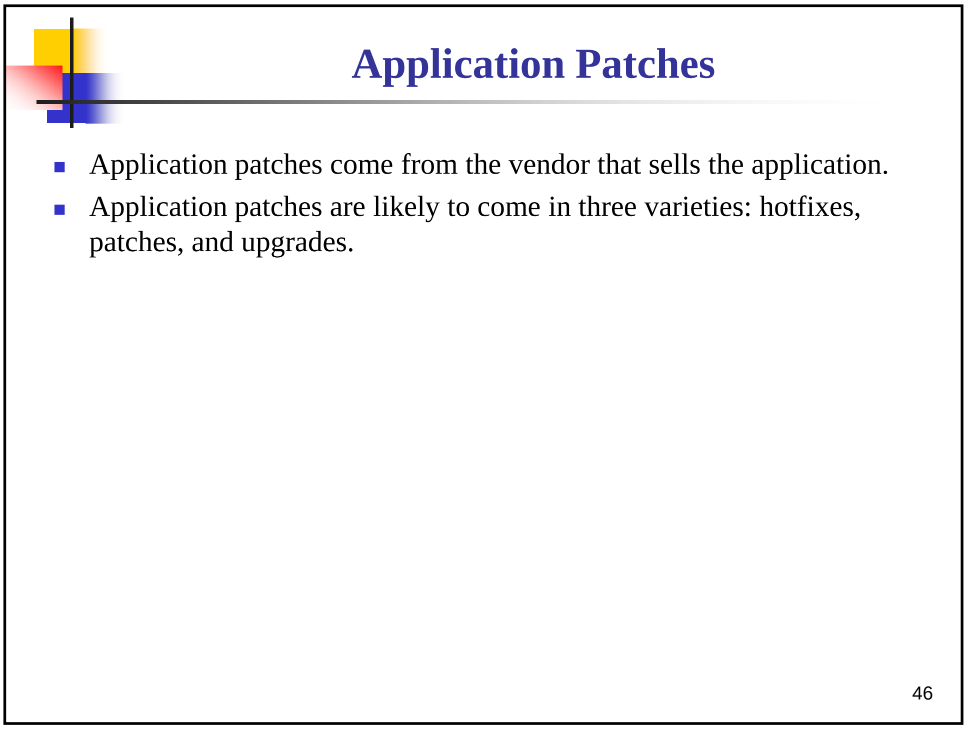


Application Hardening

- Relates to securing an application against local and Internet-based attacks.
- As important as operating system and network hardening

- Hardening applications similar to hardening operating systems.
  - Remove the unneeded functions or components.
  - Restrict access where you can.
  - Make sure the application is kept up-to-date with patches.

- Securing applications typically involves the following activities:
  - Application patches
    - Hotfixes, patches, upgrades
  - Patch management



Application Patches

- Application patches come from the vendor that sells the application.
- Application patches are likely to come in three varieties: hotfixes, patches, and upgrades.

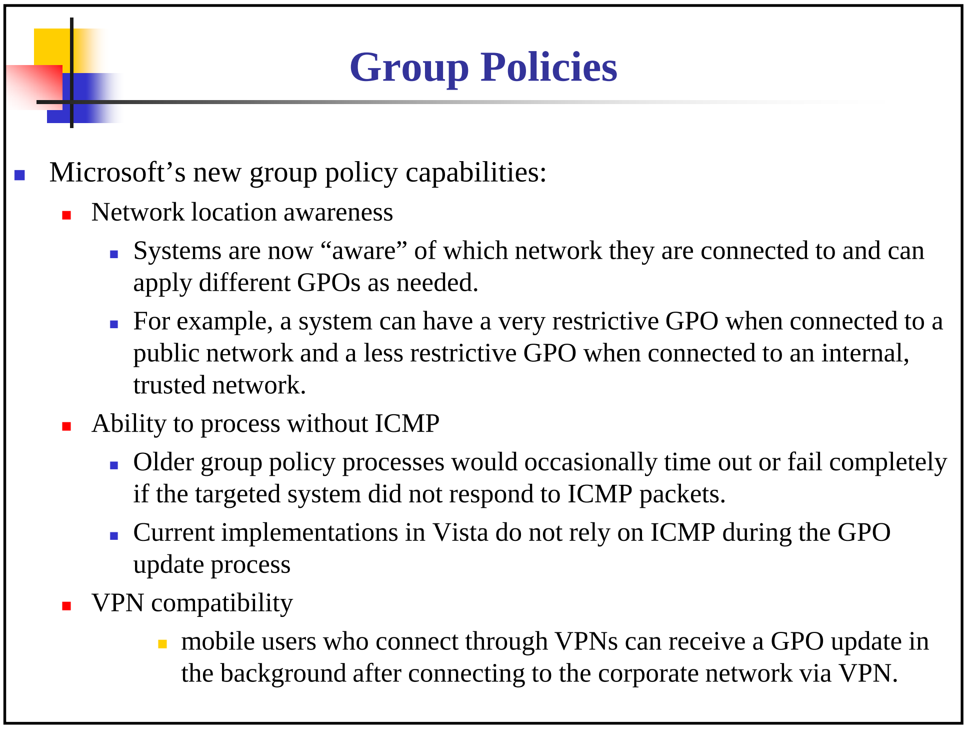
Patch Management

- A disciplined approach to the acquisition, testing, and implementation of patches.
- Ability to inventory applications and operating systems in use
  - Notification of patches
  - Continual scanning of systems patch status
  - Select which patches to apply
  - Push patches to systems
  - Ability to report patch success or failure
  - Ability to report patch status on any or all systems in the environment

Group Policies

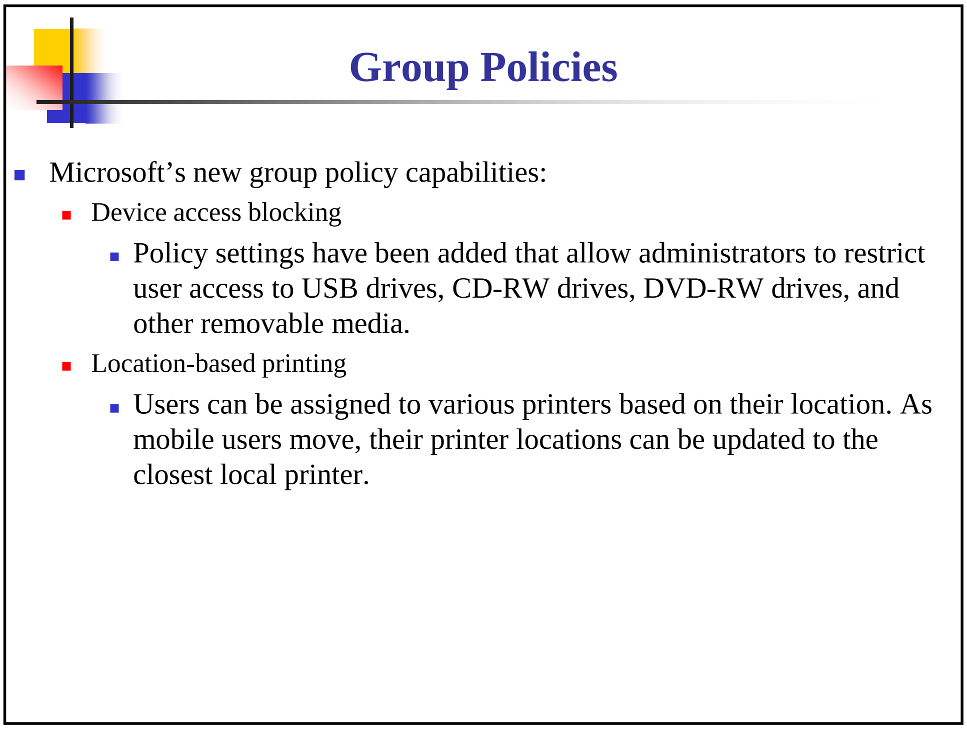
- Group policy
  - "An infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment.

    -Microsoft
- Group policy object (GPO)
  - Policy settings stored in a group policy object are referenced internally by the OS using a globally unique identifier (GUID)



Group Policies

- Microsoft’s new group policy capabilities:
  - Network location awareness
    - Systems are now “aware” of which network they are connected to and can apply different GPOs as needed.
    - For example, a system can have a very restrictive GPO when connected to a public network and a less restrictive GPO when connected to an internal, trusted network.
  - Ability to process without ICMP
    - Older group policy processes would occasionally time out or fail completely if the targeted system did not respond to ICMP packets.
    - Current implementations in Vista do not rely on ICMP during the GPO update process
  - VPN compatibility
      - mobile users who connect through VPNs can receive a GPO update in the background after connecting to the corporate network via VPN.

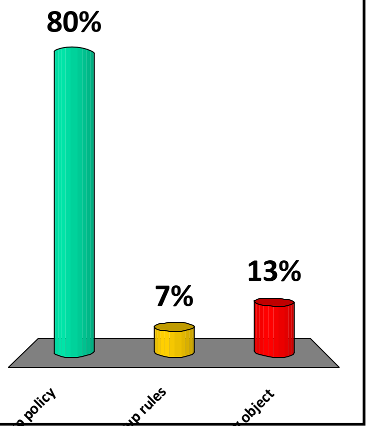


Group Policies

- Microsoft’s new group policy capabilities:
  - Device access blocking
    - Policy settings have been added that allow administrators to restrict user access to USB drives, CD-RW drives, DVD-RW drives, and other removable media.
  - Location-based printing
    - Users can be assigned to various printers based on their location. As mobile users move, their printer locations can be updated to the closest local printer.

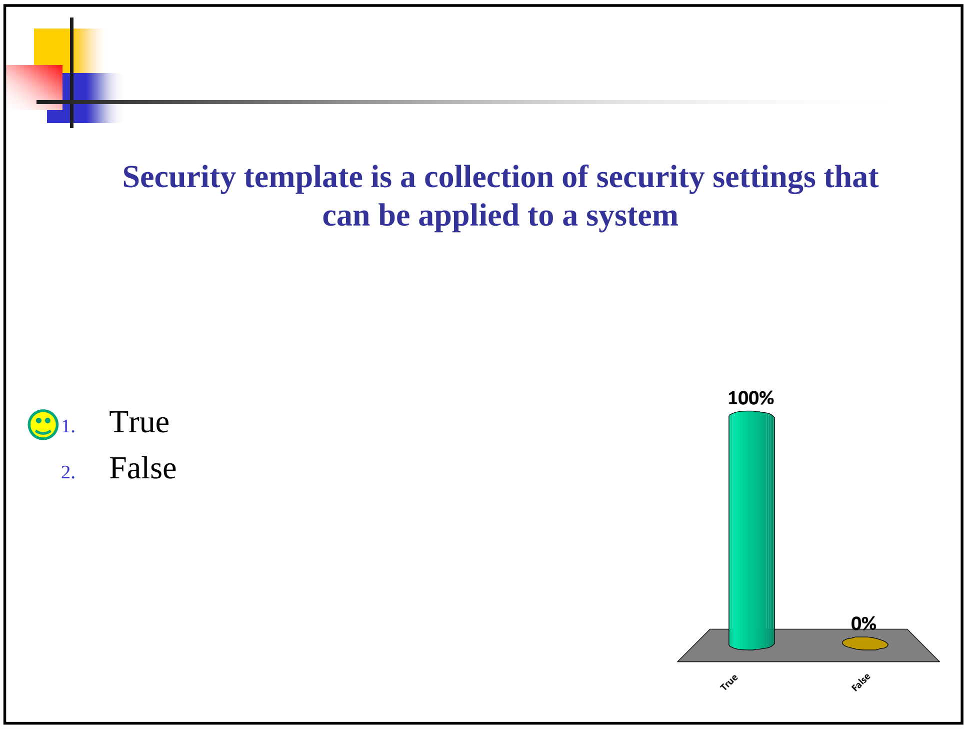
______ is defined as “an infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers.

☺ 1. Group policy
2. Group rules
3. Group policy object



Security Templates

- A collection of security settings that can be applied to a system.
- As an administrator, when you are creating a security template, all settings are initially “not configured,” which means the template will make no changes to whatever settings are already in place.
- By selecting the settings you want to modify, you can fine-tune the template to create a more (or less) secure system.
- They configure the following areas:
  - Account policies
  - Event log settings
  - File permissions
  - Registry permissions
  - Restricted groups
  - System services
  - User rights



Security template is a collection of security settings that can be applied to a system

☺ 1. True
2. False