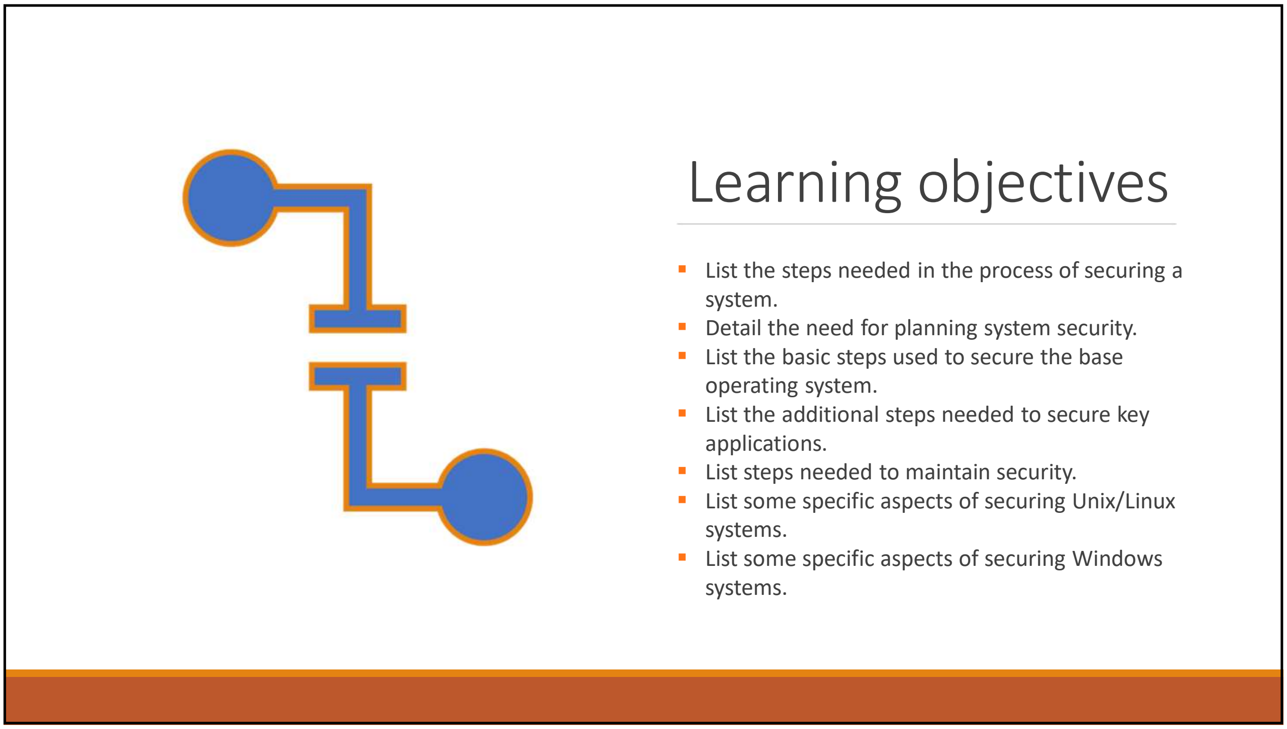
Operating system security

COMPUTER SECURITY – PRINCIPLES AND PRACTICE (PEARSON, FOURTH EDITION)
W. STALLINGS, L. BROWN

* THESE SLIDES ARE AN ADAPTATION OF THE ORIGINAL SLIDES OF THE AUTHORS OF THE BOOK

1

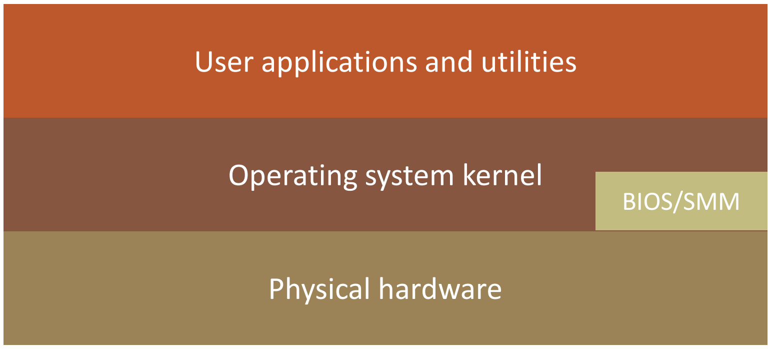


Learning objectives

- List the steps needed in the process of securing a system.
- Detail the need for planning system security.
- List the basic steps used to secure the base operating system.
- List the additional steps needed to secure key applications.
- List steps needed to maintain security.
- List some specific aspects of securing Unix/Linux systems.
- List some specific aspects of securing Windows systems.

2

System Security Layers



User applications and utilities

Operating system kernel

BIOS/SMM

Physical hardware

3

Strategies

- The 2010 Australian Signals Directorate (ASD) lists the “Top 35 Mitigation Strategies”
- Over 85% of the targeted cyber intrusions investigated by ASD in 2009 could have been prevented
- The top four strategies for prevention are:
  - White-list approved applications
  - Patch third-party applications and operating system vulnerabilities
  - Restrict administrative privileges
  - Create a defense-in-depth system
- These strategies largely align with those in the “20 Critical Controls” developed by DHS, NSA, the Department of Energy, SANS, and others in the United States

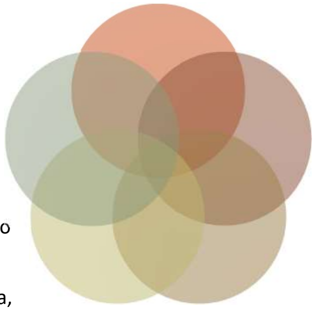
4

Operating System Security

- Possible for a system to be compromised during the installation process before it can install the latest patches
- Building and deploying a system should be a planned process designed to counter this threat
- Process must:
  - Assess risks and plan the system deployment
  - Secure the underlying operating system and then the key applications
  - Ensure any critical content is secured
  - Ensure appropriate network protection mechanisms are used
  - Ensure appropriate processes are used to maintain security

5

System Security Planning



The first step in deploying a new system is **planning**

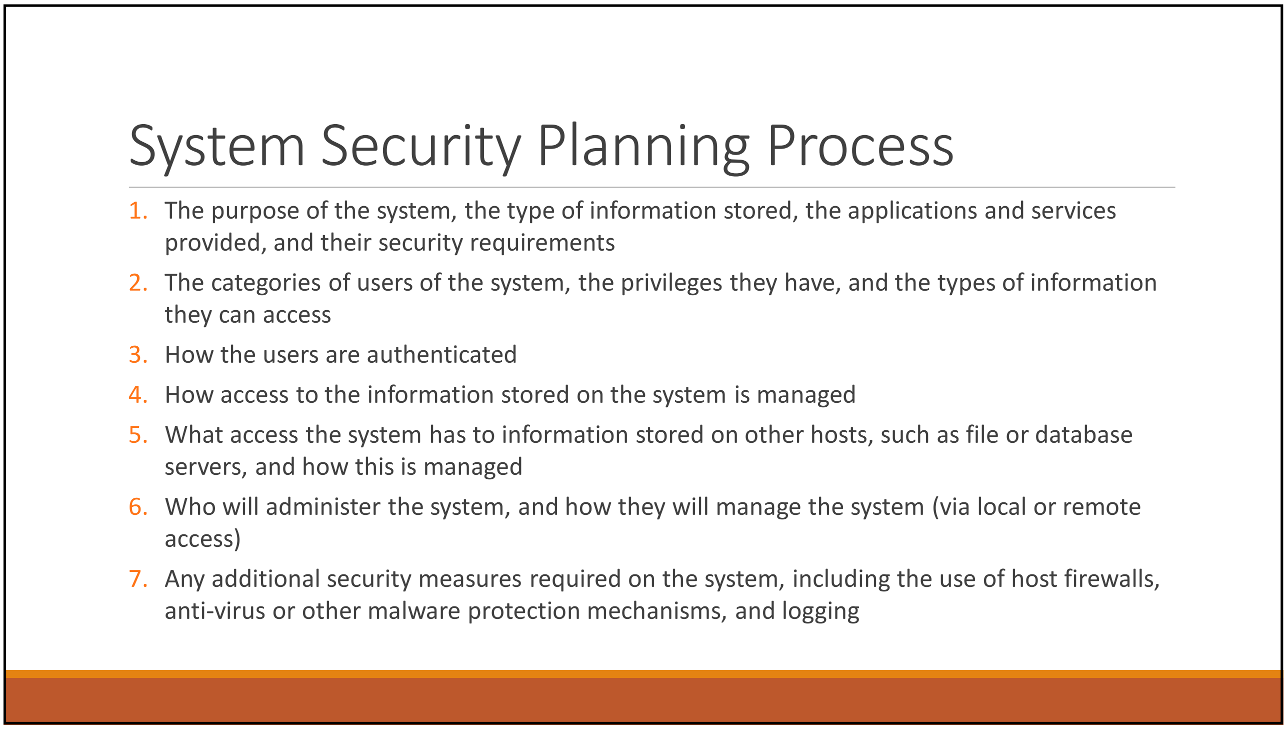
Planning should include a wide and specific **security assessment** of the organization

Aim is to **maximize security** while **minimizing costs**

Planning process needs to determine **security requirements** for the system, applications, data, and users

Plan needs to identify appropriate **personnel** and training to install and manage the system

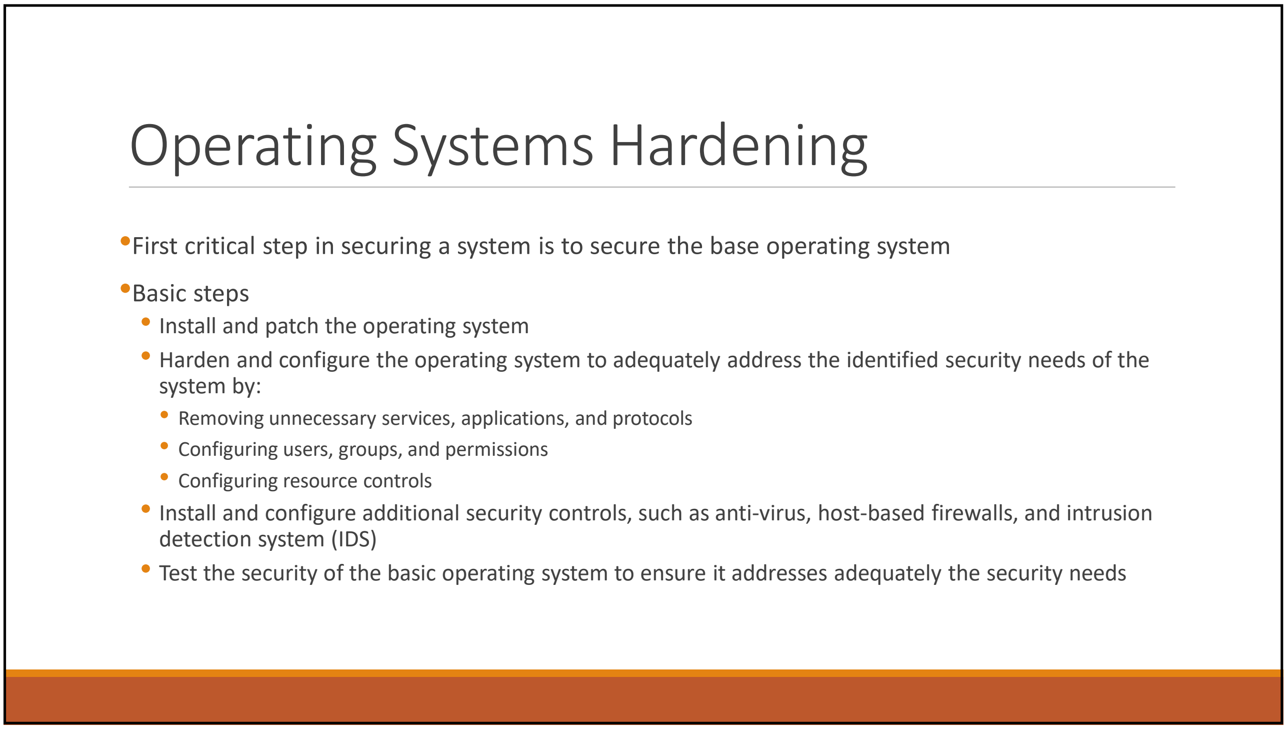
6



System Security Planning Process

1. The purpose of the system, the type of information stored, the applications and services provided, and their security requirements
2. The categories of users of the system, the privileges they have, and the types of information they can access
3. How the users are authenticated
4. How access to the information stored on the system is managed
5. What access the system has to information stored on other hosts, such as file or database servers, and how this is managed
6. Who will administer the system, and how they will manage the system (via local or remote access)
7. Any additional security measures required on the system, including the use of host firewalls, anti-virus or other malware protection mechanisms, and logging

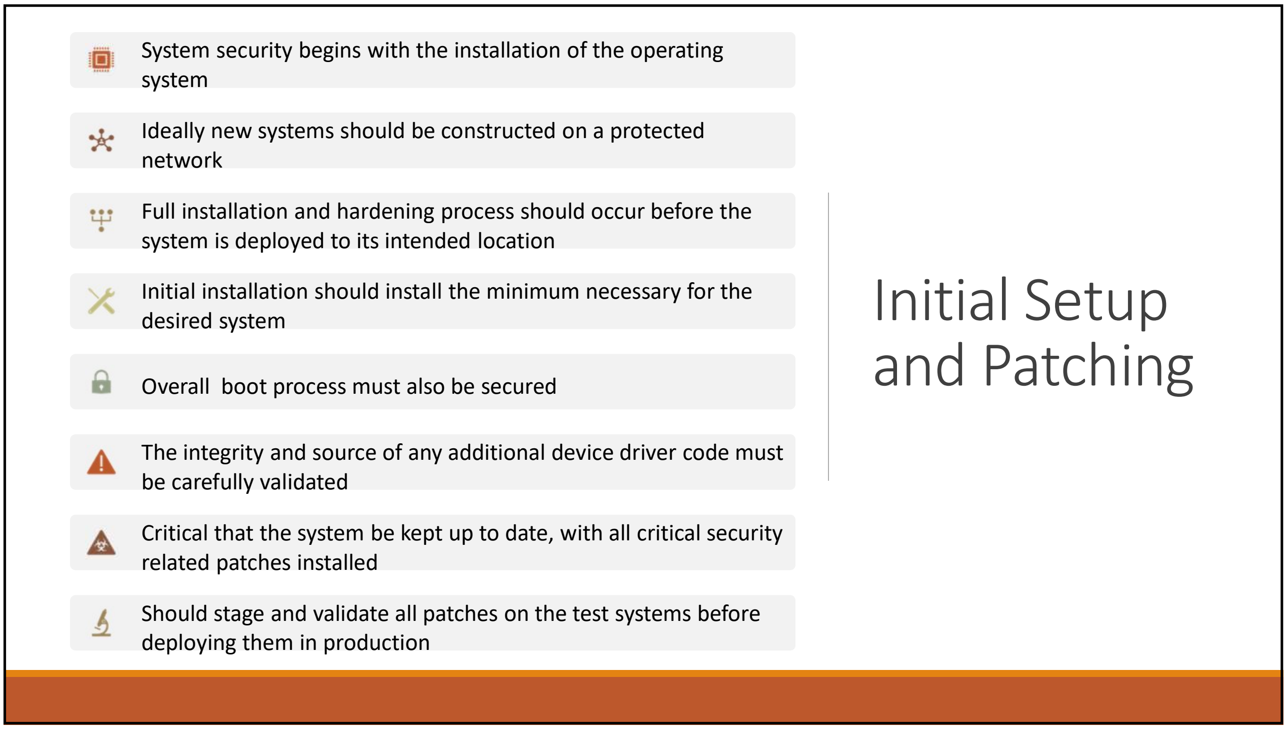
7



Operating Systems Hardening

- First critical step in securing a system is to secure the base operating system
- Basic steps
  - Install and patch the operating system
  - Harden and configure the operating system to adequately address the identified security needs of the system by:
    - Removing unnecessary services, applications, and protocols
    - Configuring users, groups, and permissions
    - Configuring resource controls
  - Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
  - Test the security of the basic operating system to ensure it addresses adequately the security needs

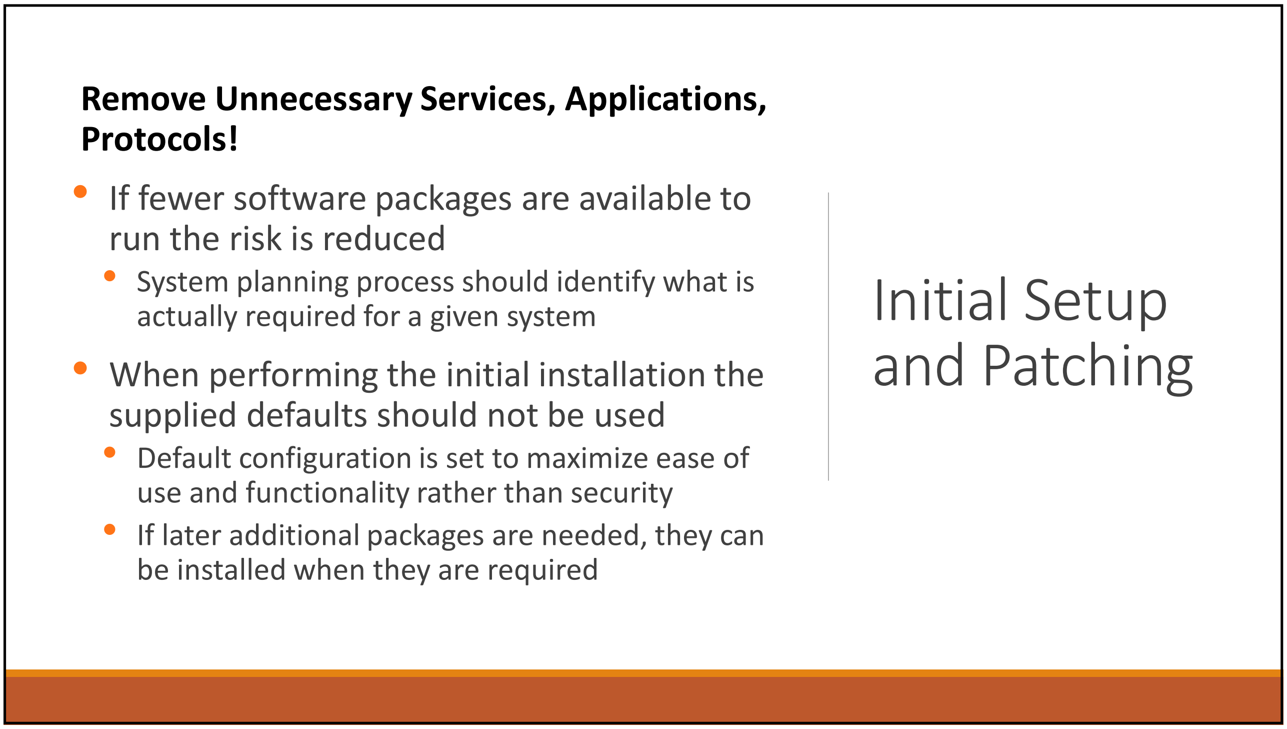
8



Initial Setup and Patching

- System security begins with the installation of the operating system
- Ideally new systems should be constructed on a protected network
- Full installation and hardening process should occur before the system is deployed to its intended location
- Initial installation should install the minimum necessary for the desired system
- Overall boot process must also be secured
- The integrity and source of any additional device driver code must be carefully validated
- Critical that the system be kept up to date, with all critical security related patches installed
- Should stage and validate all patches on the test systems before deploying them in production

9



Initial Setup and Patching

Remove Unnecessary Services, Applications, Protocols!

- If fewer software packages are available to run the risk is reduced
  - System planning process should identify what is actually required for a given system
- When performing the initial installation the supplied defaults should not be used
  - Default configuration is set to maximize ease of use and functionality rather than security
  - If later additional packages are needed, they can be installed when they are required

10

Configure Users, Groups, and Authentication

- Not all users with access to a system will have the same access to all data and resources on that system
- Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

Initial Setup and Patching

11

Configure Users, Groups, and Authentication

- System planning process should consider:
  - Categories of users on the system
  - Privileges they have
  - Types of information they can access
  - How and where they are defined and authenticated
- Default accounts included as part of the system installation should be secured
  - Those that are not required should be either removed or disabled
  - Policies that apply to authentication credentials configured (auth. method, passwd expiration, …)

Initial Setup and Patching

12

Configure Resource Access Controls

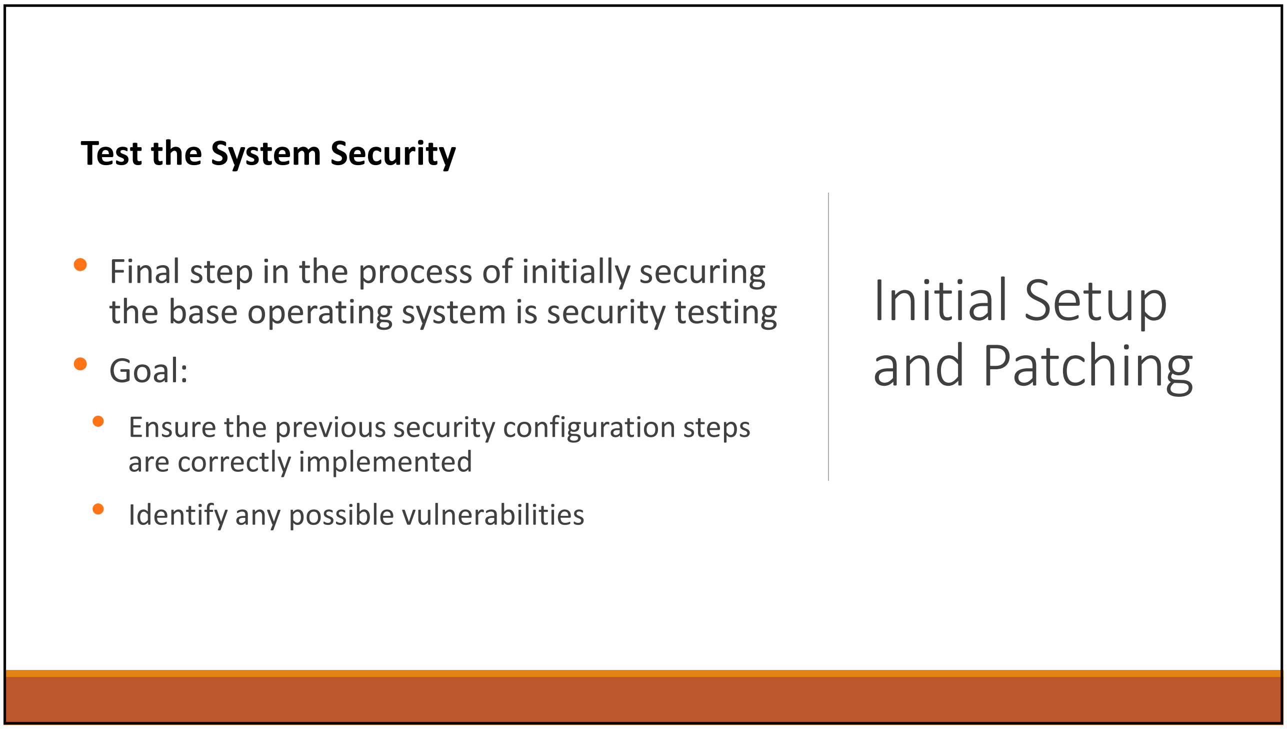
- Once the users and groups are defined, appropriate permissions can be set on data and resources
- Many of the security hardening guides provide lists of recommended changes to the default access configuration

Initial Setup and Patching

Install Additional Security Controls

- Further security possible by installing and configuring additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS or IPS software
  - Application white-listing

Initial Setup and Patching

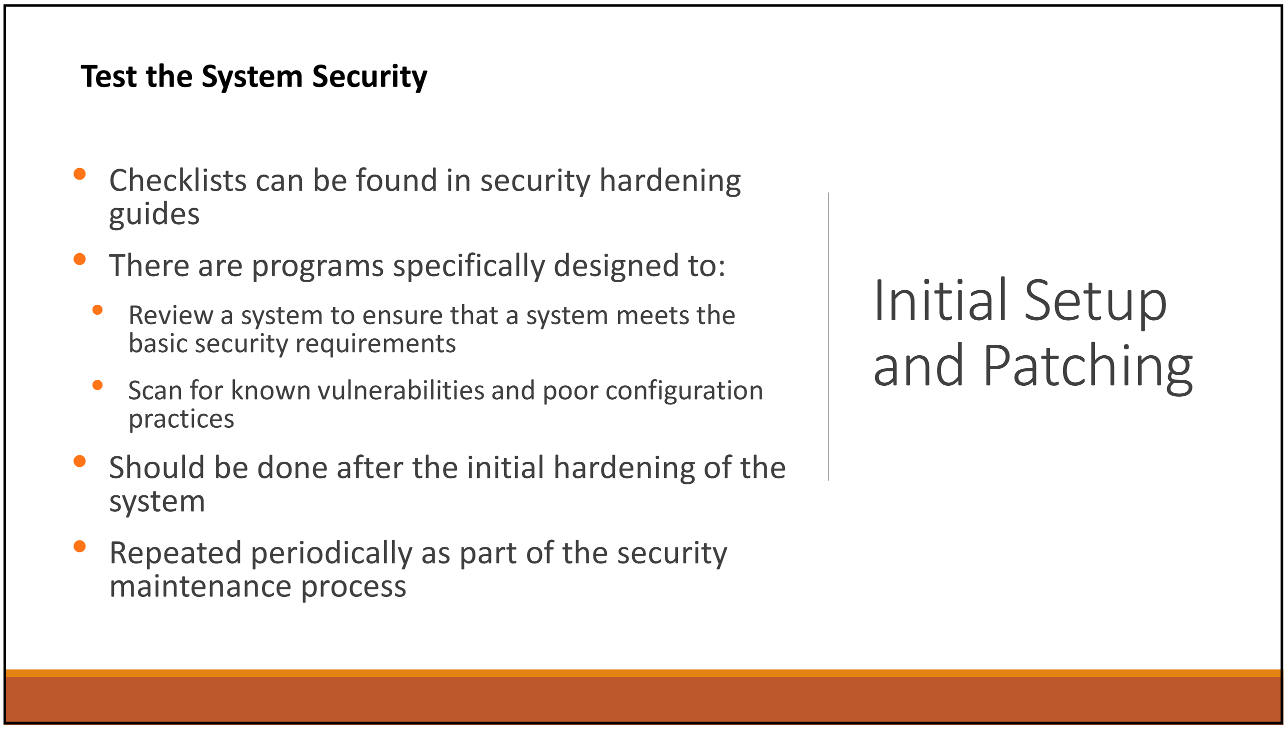


Test the System Security

- Final step in the process of initially securing the base operating system is security testing
- Goal:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities

Initial Setup and Patching

15



Test the System Security

- Checklists can be found in security hardening guides
- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices
- Should be done after the initial hardening of the system
- Repeated periodically as part of the security maintenance process

Initial Setup and Patching

16

Application Configuration

May include:

- Creating and specifying appropriate data storage areas for application
- Making appropriate changes to the application or service default configuration details

Some applications or services may include:

- Default data
- Scripts
- User accounts

Of particular concern with remotely accessed services such as Web and file transfer services

- Risk from this form of attack is reduced by ensuring that most of the files can only be read, but not written, by the server

17

Use of encryption

Is a key enabling technology that may be used to secure data both in transit and when stored

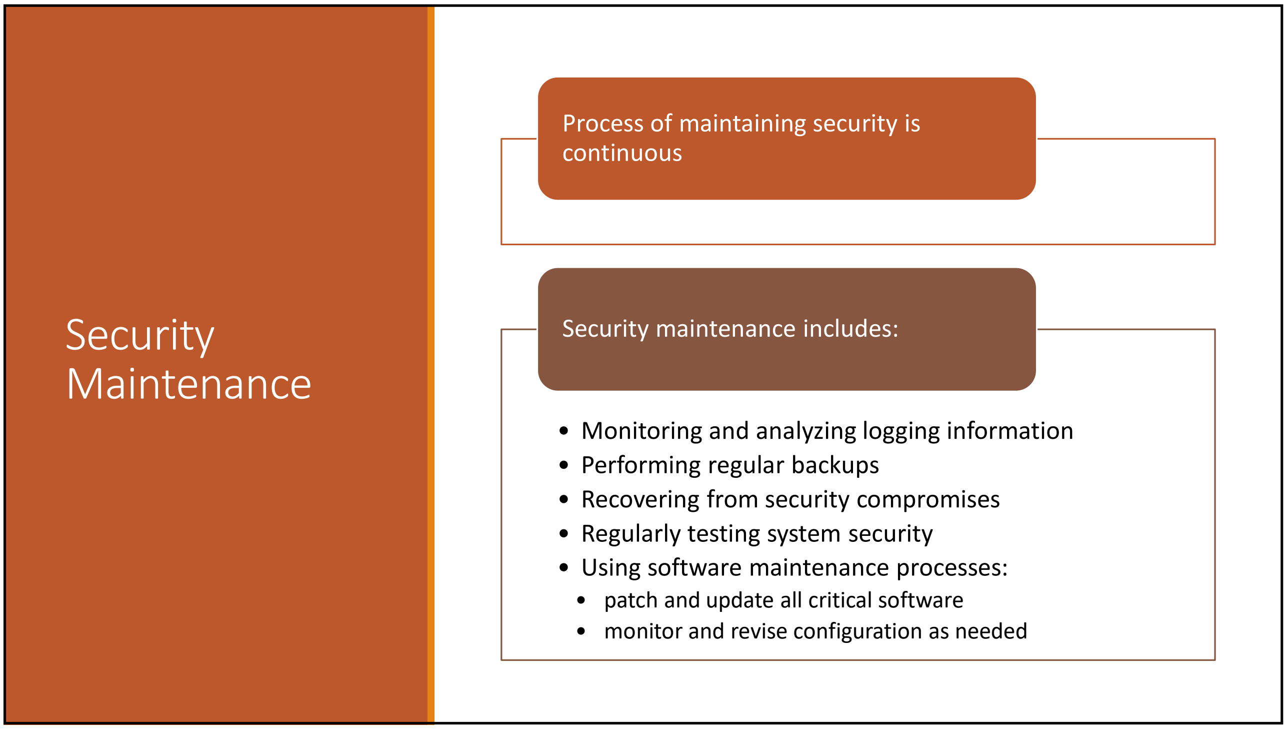
Must be configured and appropriate cryptographic keys created, signed, and secured

If secure network services are provided using TLS or IPsec suitable public and private keys must be generated for each of them

If secure network services are provided using SSH, appropriate server and client keys must be created

Cryptographic file systems are another use of encryption

18



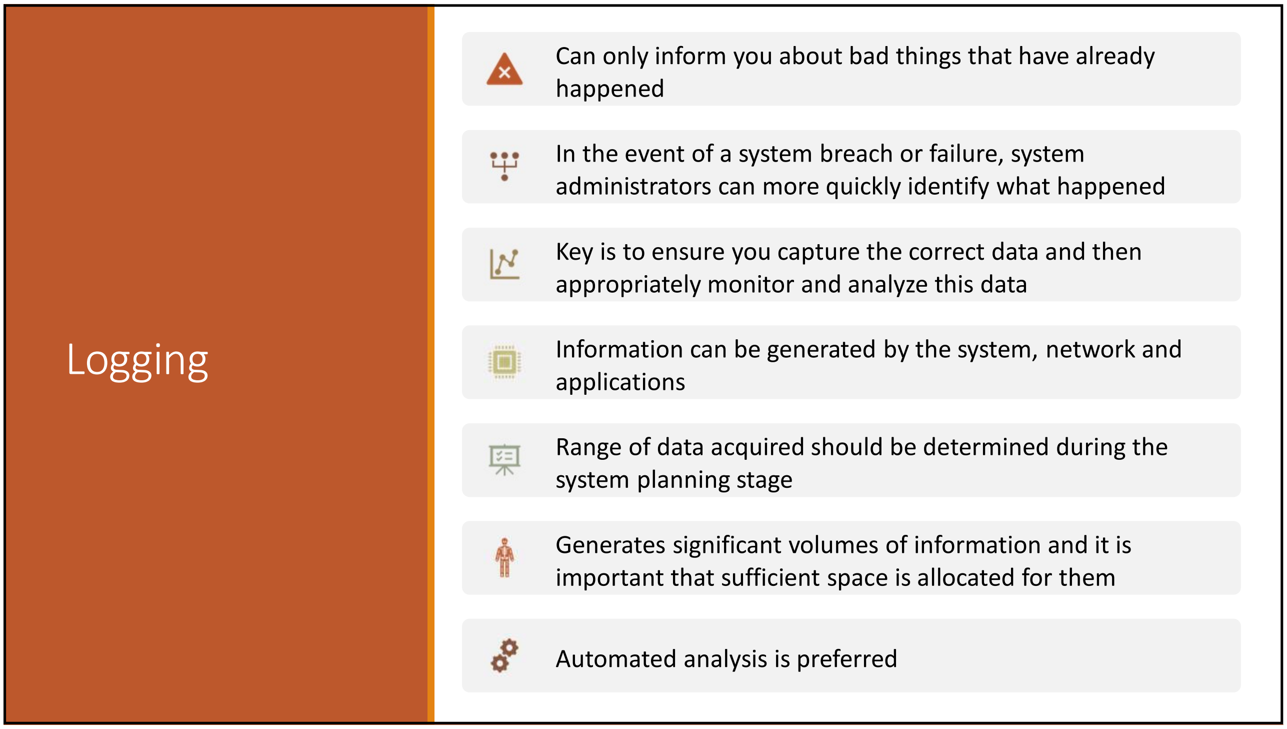
Security Maintenance

Process of maintaining security is continuous

Security maintenance includes:

- Monitoring and analyzing logging information
- Performing regular backups
- Recovering from security compromises
- Regularly testing system security
- Using software maintenance processes:
  - patch and update all critical software
  - monitor and revise configuration as needed

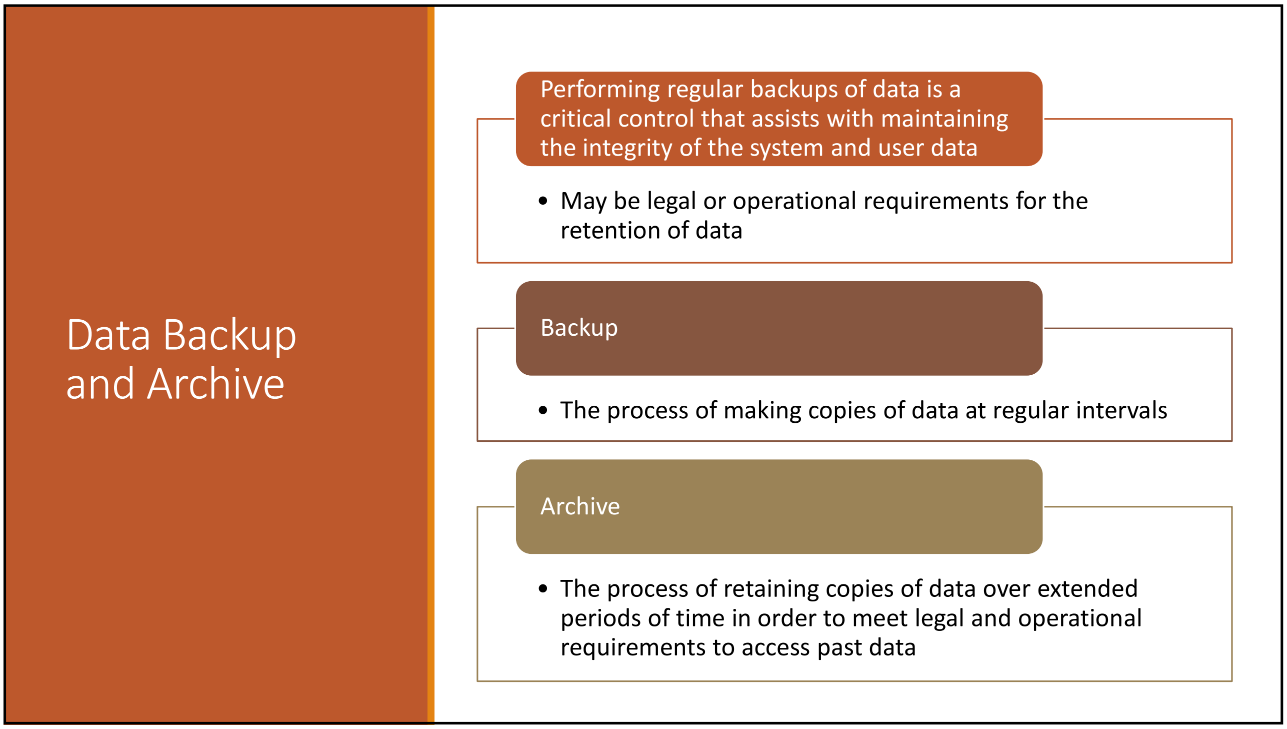
19



Logging

- Can only inform you about bad things that have already happened
- In the event of a system breach or failure, system administrators can more quickly identify what happened
- Key is to ensure you capture the correct data and then appropriately monitor and analyze this data
- Information can be generated by the system, network and applications
- Range of data acquired should be determined during the system planning stage
- Generates significant volumes of information and it is important that sufficient space is allocated for them
- Automated analysis is preferred

20



Data Backup and Archive

Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data

- May be legal or operational requirements for the retention of data

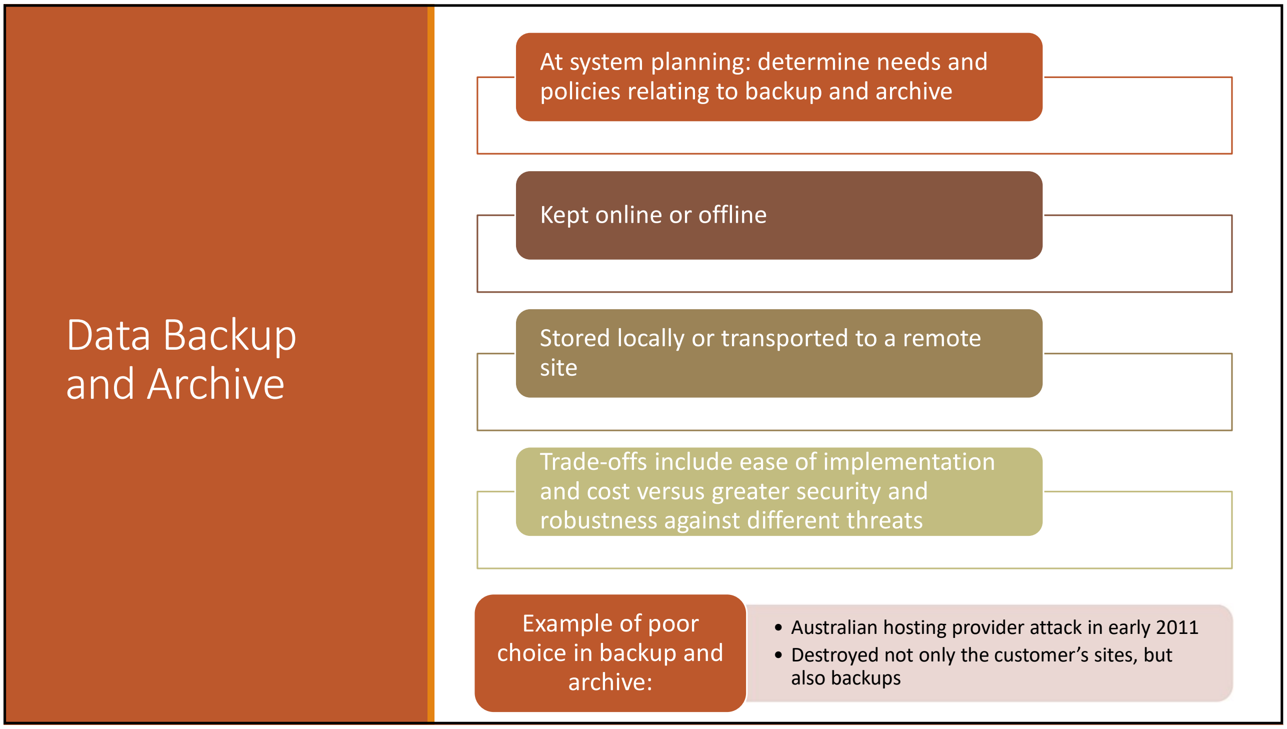
Backup

- The process of making copies of data at regular intervals

Archive

- The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

21



Data Backup and Archive

At system planning: determine needs and policies relating to backup and archive

Kept online or offline

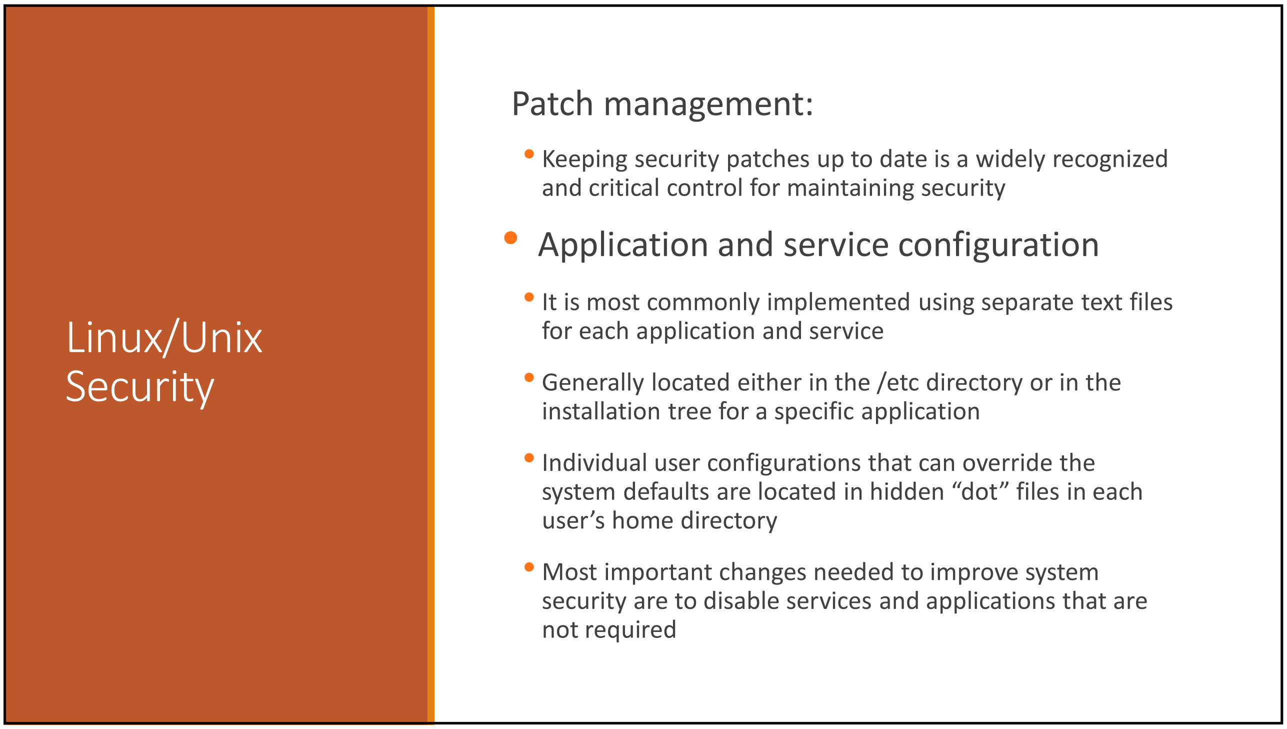
Stored locally or transported to a remote site

Trade-offs include ease of implementation and cost versus greater security and robustness against different threats

Example of poor choice in backup and archive:

- Australian hosting provider attack in early 2011
- Destroyed not only the customer’s sites, but also backups

22



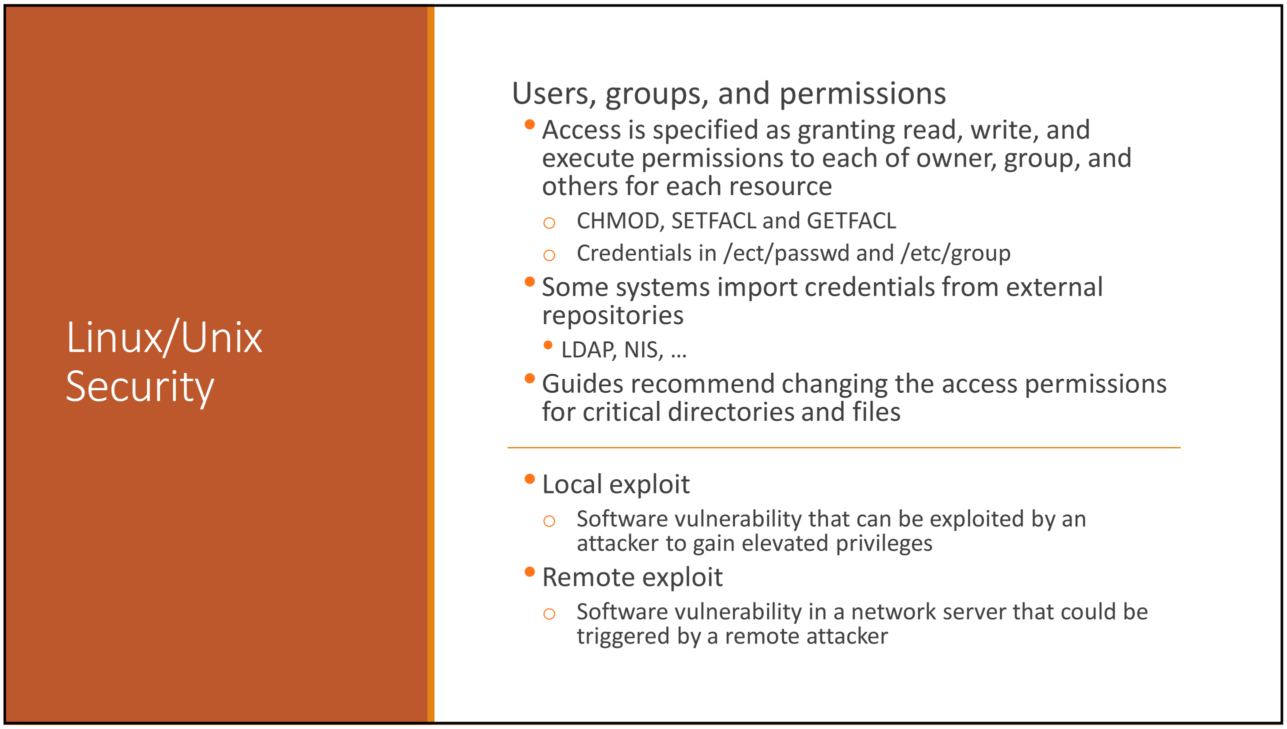
Linux/Unix Security

Patch management:

- Keeping security patches up to date is a widely recognized and critical control for maintaining security

- Application and service configuration
  - It is most commonly implemented using separate text files for each application and service
  - Generally located either in the /etc directory or in the installation tree for a specific application
  - Individual user configurations that can override the system defaults are located in hidden “dot” files in each user’s home directory
  - Most important changes needed to improve system security are to disable services and applications that are not required

23



Linux/Unix Security

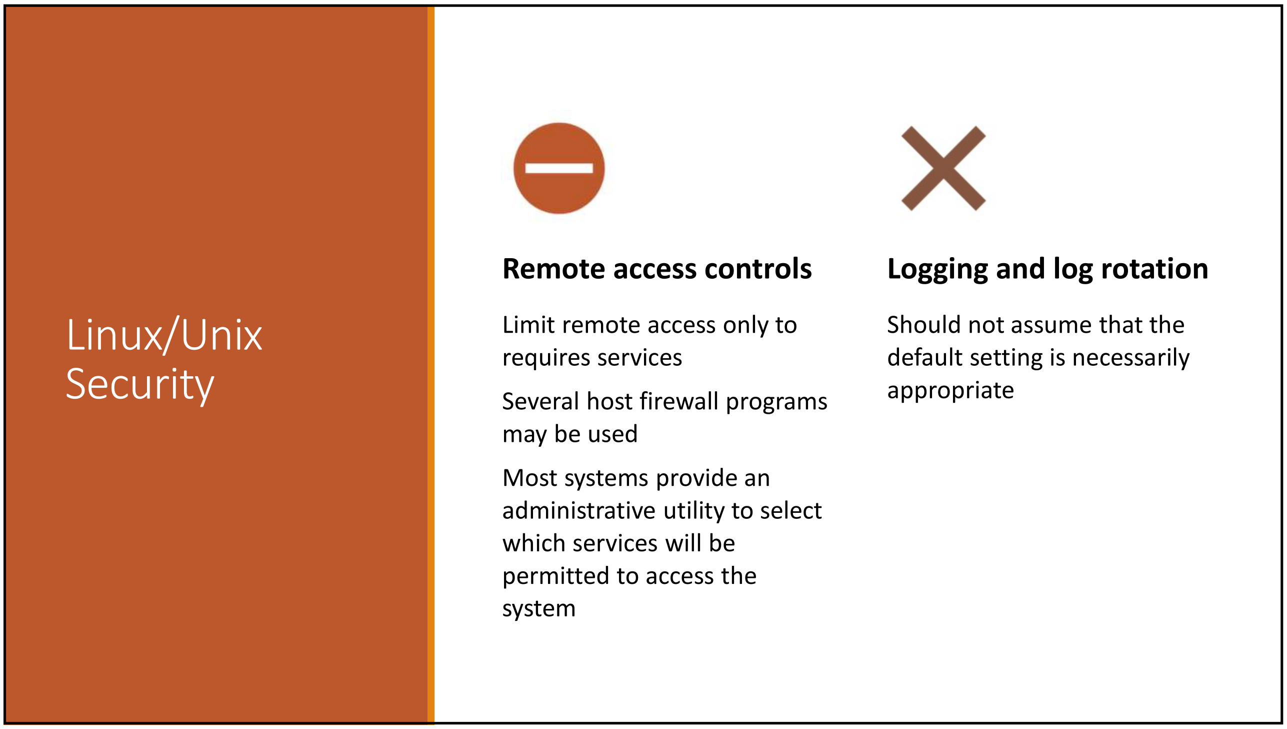
Users, groups, and permissions

- Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
  - ○ CHMOD, SETFACL and GETFACL
  - ○ Credentials in /ect/passwd and /etc/group
- Some systems import credentials from external repositories
  - LDAP, NIS, …
- Guides recommend changing the access permissions for critical directories and files

---

- Local exploit
  - ○ Software vulnerability that can be exploited by an attacker to gain elevated privileges
- Remote exploit
  - ○ Software vulnerability in a network server that could be triggered by a remote attacker

24



Linux/Unix Security

Remote access controls

Limit remote access only to requires services

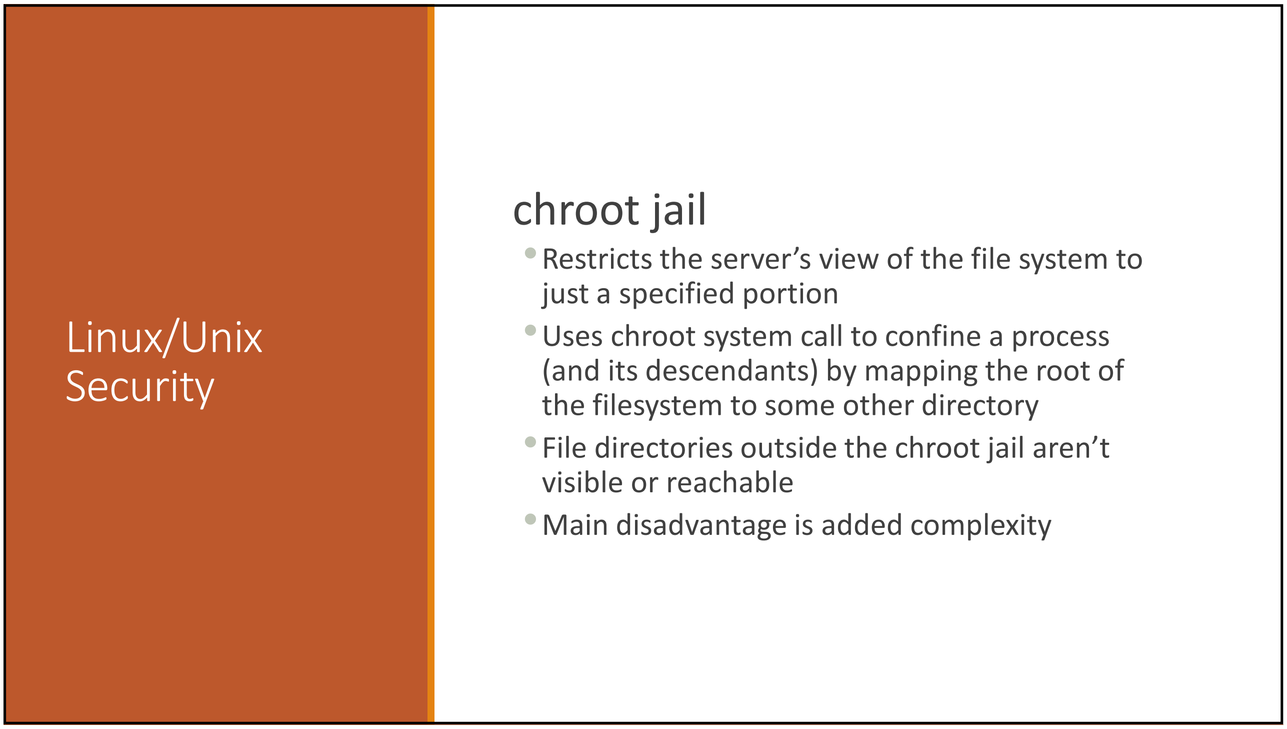
Several host firewall programs may be used

Most systems provide an administrative utility to select which services will be permitted to access the system

Logging and log rotation

Should not assume that the default setting is necessarily appropriate

25

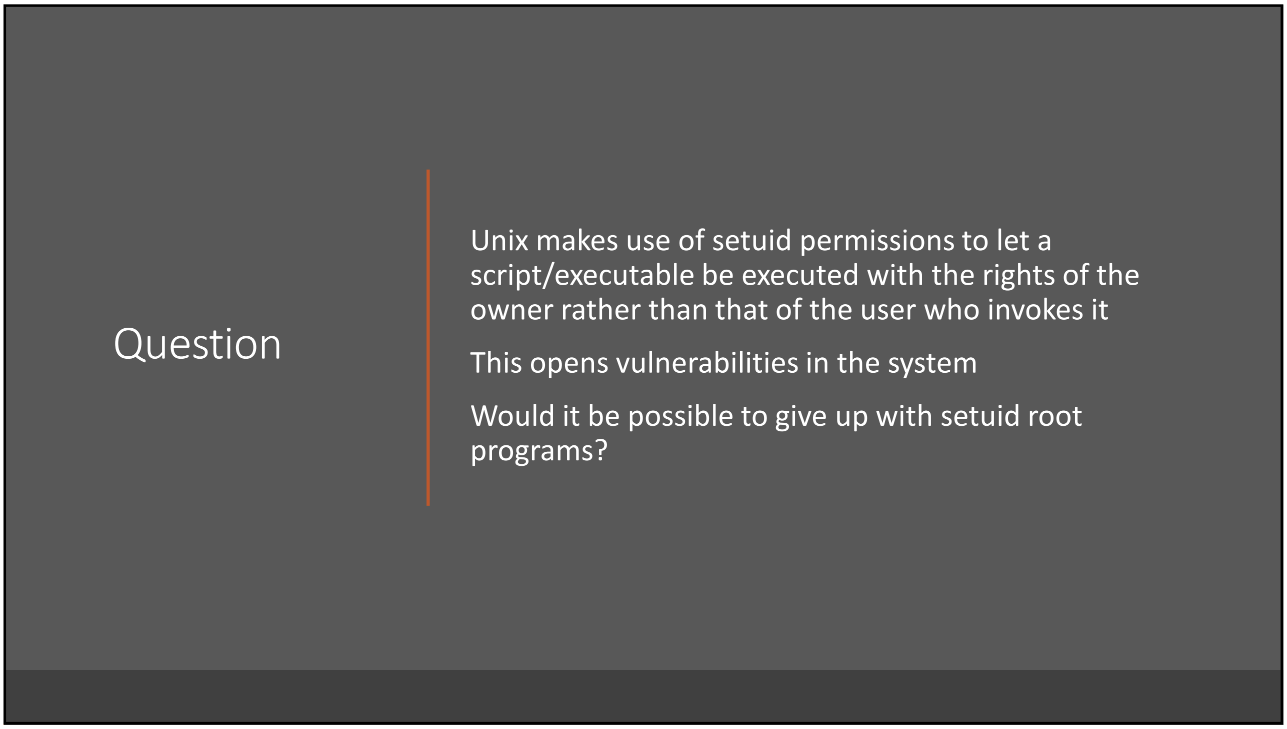


Linux/Unix Security

chroot jail

- Restricts the server’s view of the file system to just a specified portion
- Uses chroot system call to confine a process (and its descendants) by mapping the root of the filesystem to some other directory
- File directories outside the chroot jail aren’t visible or reachable
- Main disadvantage is added complexity

26



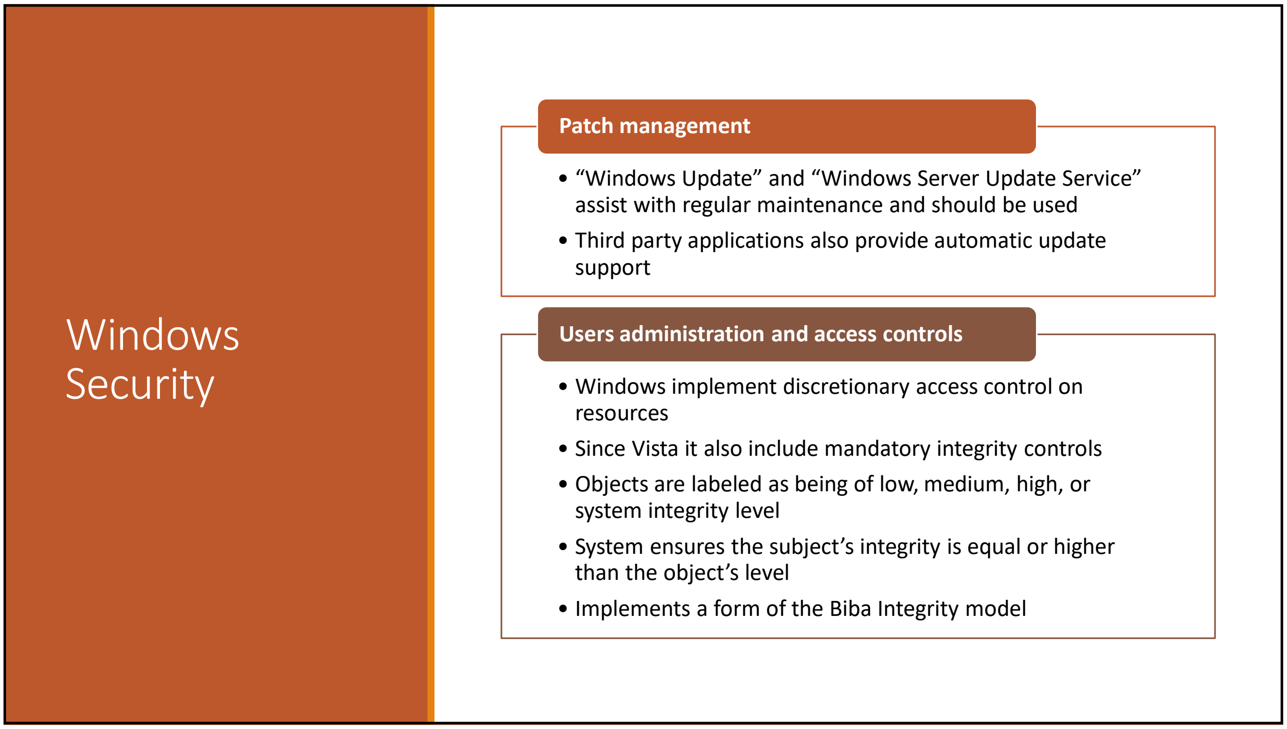
Question

Unix makes use of setuid permissions to let a script/executable be executed with the rights of the owner rather than that of the user who invokes it

This opens vulnerabilities in the system

Would it be possible to give up with setuid root programs?

27



Windows Security

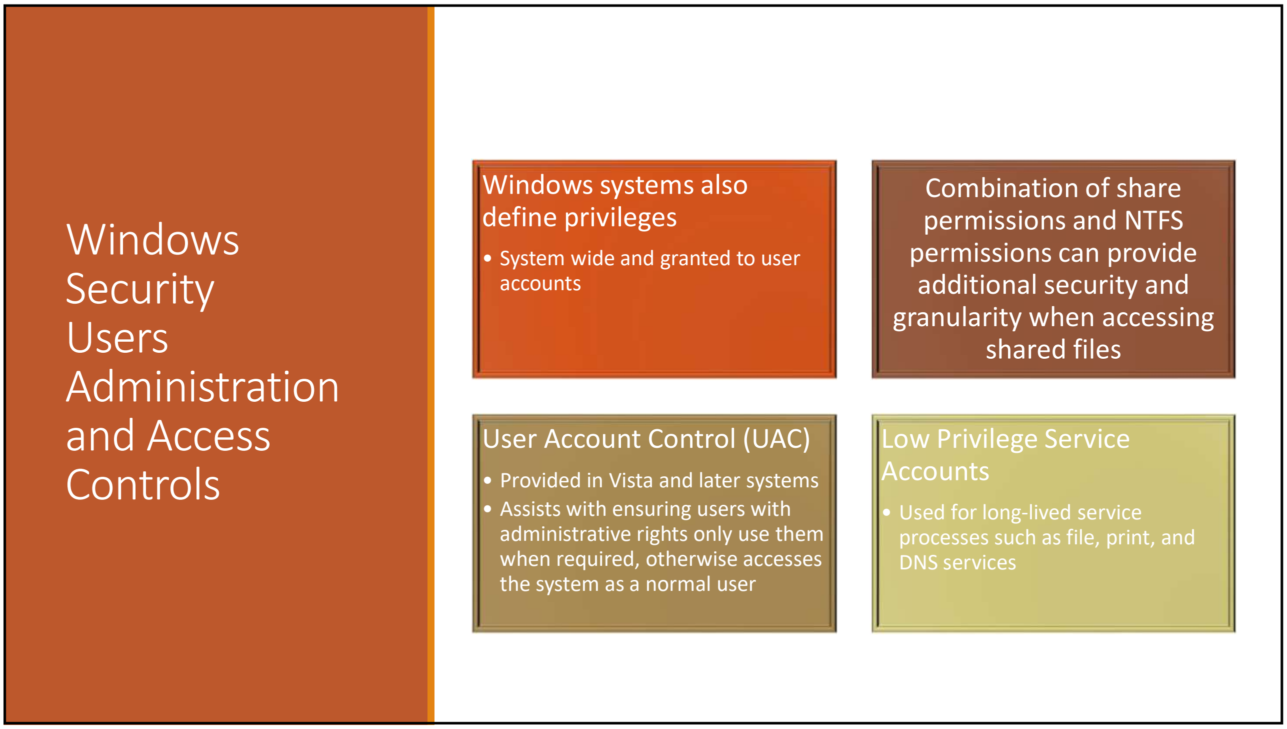
Patch management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
- Third party applications also provide automatic update support

Users administration and access controls

- Windows implement discretionary access control on resources
- Since Vista it also include mandatory integrity controls
- Objects are labeled as being of low, medium, high, or system integrity level
- System ensures the subject’s integrity is equal or higher than the object’s level
- Implements a form of the Biba Integrity model

28



Windows Security Users Administration and Access Controls

Windows systems also define privileges

- System wide and granted to user accounts

Combination of share permissions and NTFS permissions can provide additional security and granularity when accessing shared files

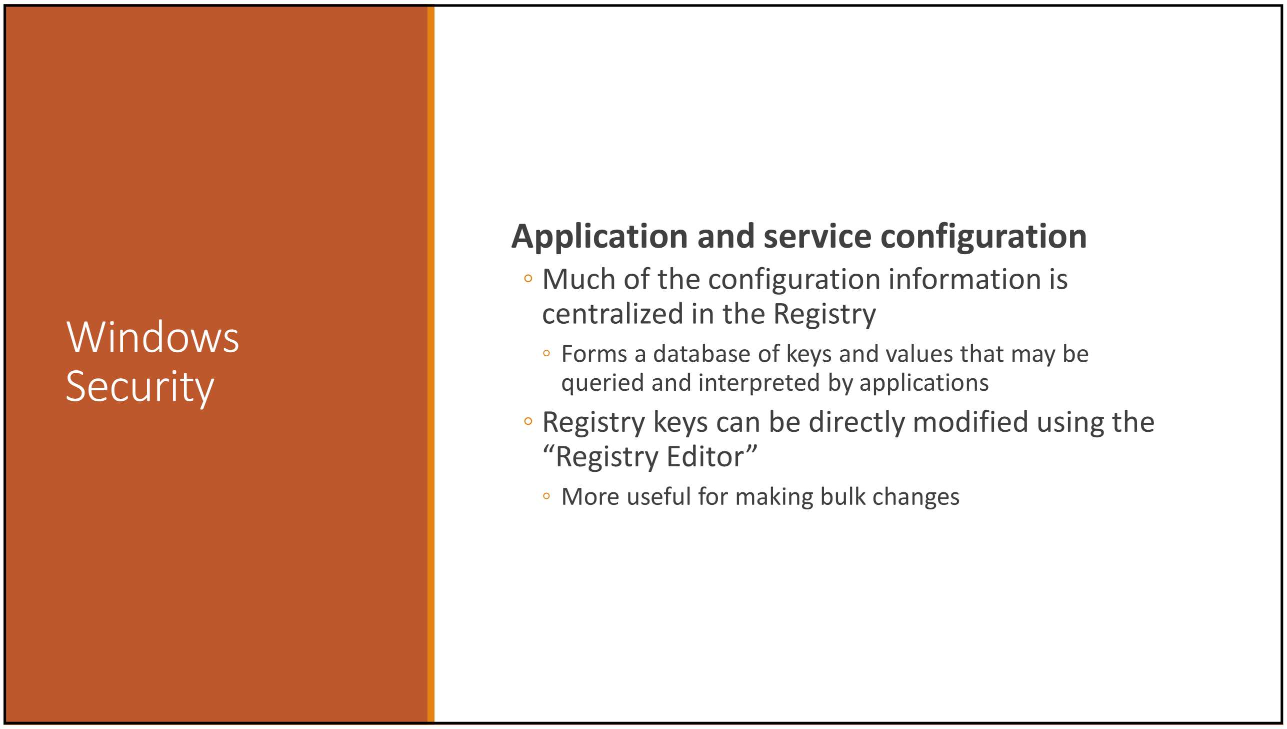
User Account Control (UAC)

- Provided in Vista and later systems
- Assists with ensuring users with administrative rights only use them when required, otherwise accesses the system as a normal user

Low Privilege Service Accounts

- Used for long-lived service processes such as file, print, and DNS services

29

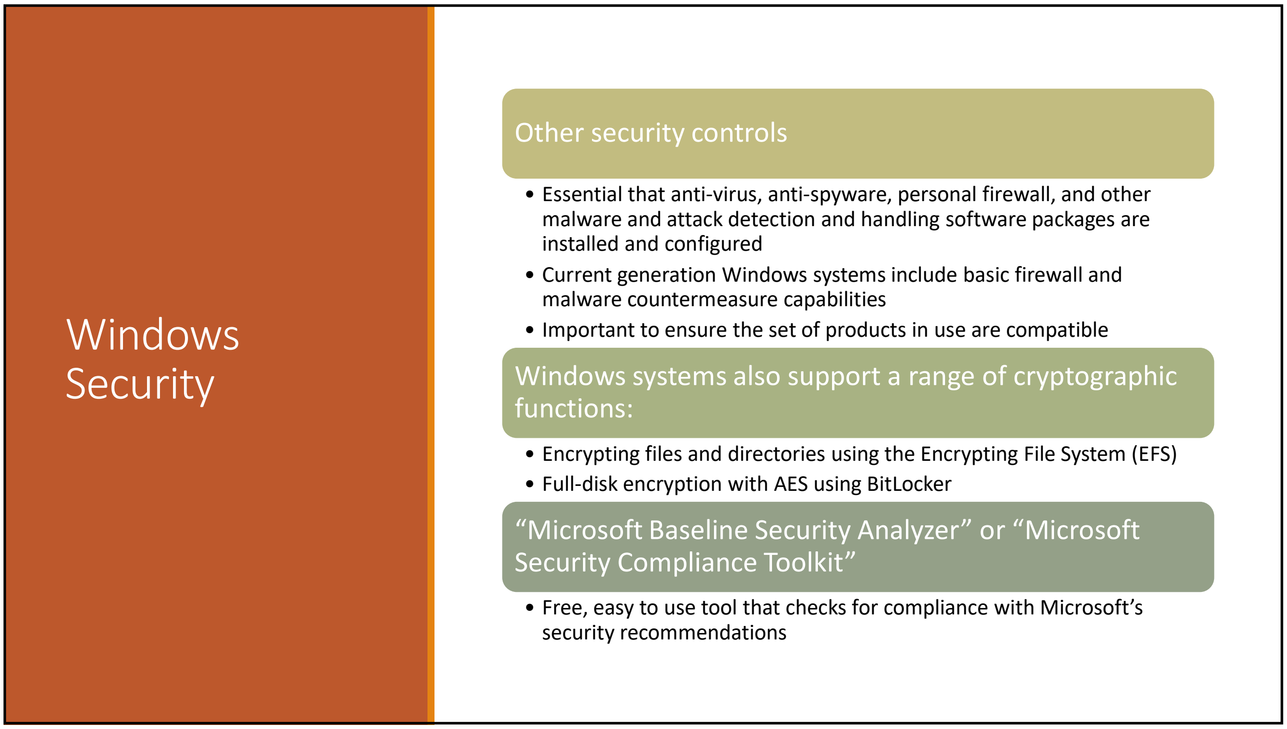


Windows Security

Application and service configuration

- Much of the configuration information is centralized in the Registry
  - Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
  - More useful for making bulk changes

30



Windows Security

Other security controls

- Essential that anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured
- Current generation Windows systems include basic firewall and malware countermeasure capabilities
- Important to ensure the set of products in use are compatible

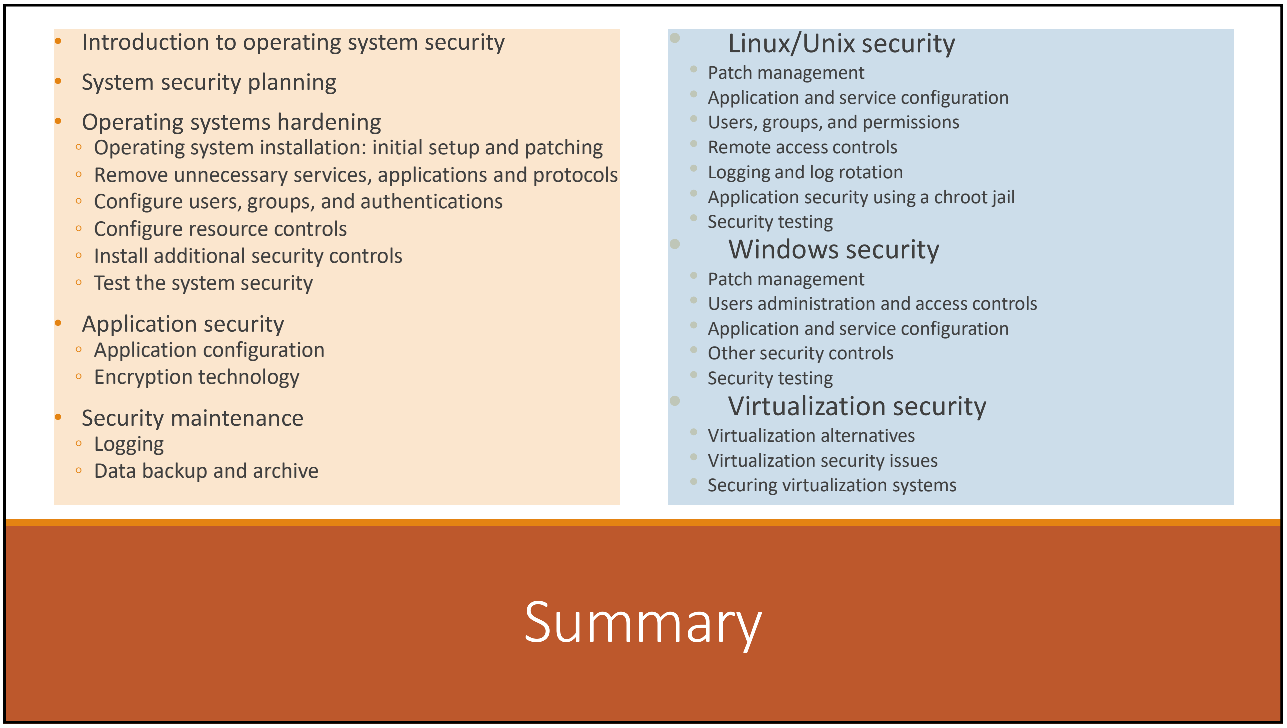
Windows systems also support a range of cryptographic functions:

- Encrypting files and directories using the Encrypting File System (EFS)
- Full-disk encryption with AES using BitLocker

"Microsoft Baseline Security Analyzer" or "Microsoft Security Compliance Toolkit"

- Free, easy to use tool that checks for compliance with Microsoft's security recommendations

31

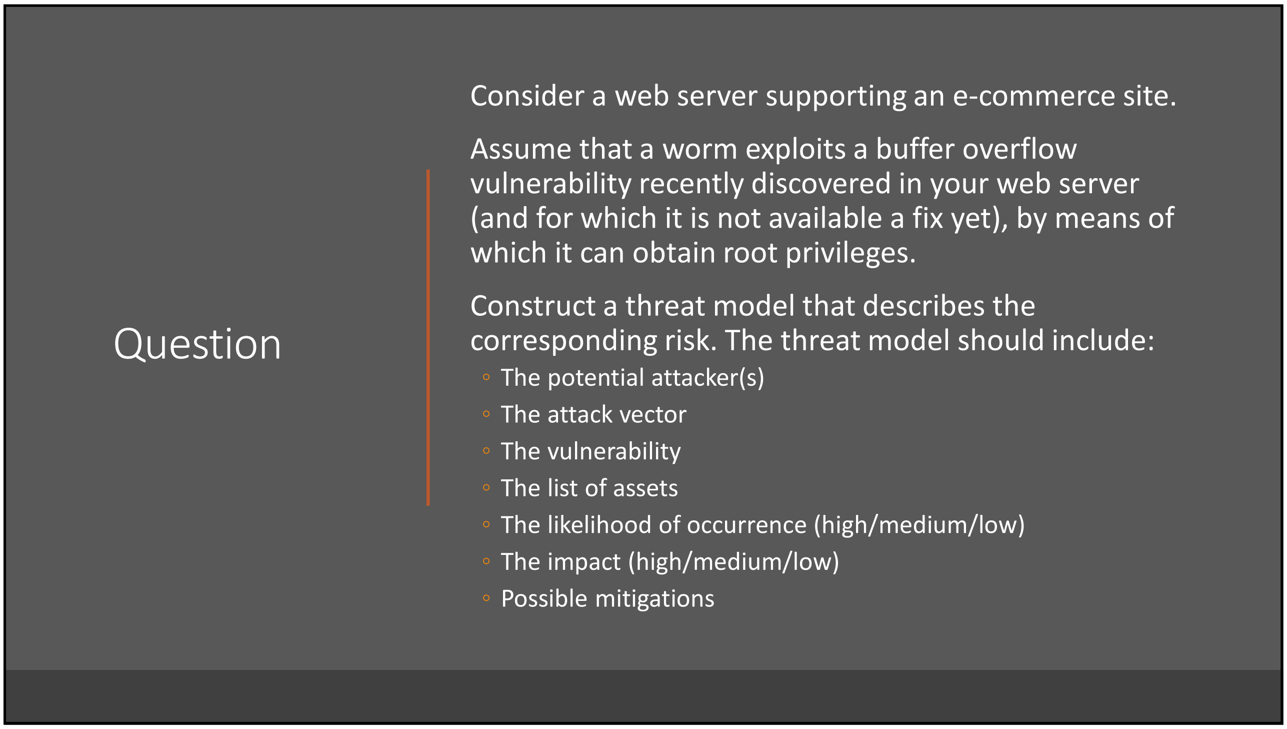


- Introduction to operating system security
- System security planning
- Operating systems hardening
  - Operating system installation: initial setup and patching
  - Remove unnecessary services, applications and protocols
  - Configure users, groups, and authentications
  - Configure resource controls
  - Install additional security controls
  - Test the system security
- Application security
  - Application configuration
  - Encryption technology
- Security maintenance
  - Logging
  - Data backup and archive

- Linux/Unix security
  - Patch management
  - Application and service configuration
  - Users, groups, and permissions
  - Remote access controls
  - Logging and log rotation
  - Application security using a chroot jail
  - Security testing
- Windows security
  - Patch management
  - Users administration and access controls
  - Application and service configuration
  - Other security controls
  - Security testing
- Virtualization security
  - Virtualization alternatives
  - Virtualization security issues
  - Securing virtualization systems

Summary

32



Question

Consider a web server supporting an e-commerce site.

Assume that a worm exploits a buffer overflow vulnerability recently discovered in your web server (and for which it is not available a fix yet), by means of which it can obtain root privileges.

Construct a threat model that describes the corresponding risk. The threat model should include:

- The potential attacker(s)
- The attack vector
- The vulnerability
- The list of assets
- The likelihood of occurrence (high/medium/low)
- The impact (high/medium/low)
- Possible mitigations