CompTIA

CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 19

Recommending Remediation

Objectives

- Explain common attacks and vulnerabilities against specialized systems.
- Given a scenario, analyze the findings and recommend the appropriate remediation within a report.

Lesson 19

Topic 19A

Employ Technical Controls

Hardening the System

- System hardening is the process of securing a device or application
- Techniques can include:
  - Install any available patches and updates
  - Ensure systems are incorporating firewall and anti-malware solutions
  - Disable specific ports or services that are not needed
  - Uninstall any unnecessary software
  - Ensure hosts are properly segmented from other hosts on the network

Sanitizing User Input

- Strips user-supplied input of unwanted or untrusted data
  - Used so the application can safely process that input, and mitigate the effects of code injection, particularly XSS and SQL injection.
- Tactics for input sanitization include:
  - **Escaping** converts text into bytes.
  - **Null byte sanitization** removes the null byte entirely
  - **Parameterized query** incorporates placeholders in a SQL query.

Implementing Multifactor Authentication (MFA)

- Generally, authentication uses one of the following methods:
  - Something you know
  - Something you have
  - Something you are
- MFA requires, at a minimum, a *second* method of authentication:
  - A password and a security code sent to the user's smartphone
  - A smart card and biometric fingerprint

Encrypting Passwords

- Passwords should always be stored in a secure format that prevents an attacker from easily reusing them
  - Unsalted hashes are vulnerable to a rainbow attack
- It is recommended to store passwords in an encrypted format.
- In cases where credentials are being stored for a particular service:
  - A password manager or similar solution can be used as they commonly implement encrypted databases to store passwords.

Process-Level Remediation

- An insecure process can lead to social engineering, Denial of Service, physical attacks, and insider threats.
- Process-level remediation changes how a process is used or implemented with the goal of reducing security vulnerabilities.
- For example, if a process is done through a non-secure channel
  - It can be migrated to use an encrypted channel of similar functionality.

Patch Management

- Identifying, testing, and deploying OS and application updates.
  - Keep track of services that require patches, test the updates, and document which ones have been applied
  - Note when the technology did not allow patching, but a mitigation strategy was implemented instead.
- Testing new patches and keeping track of mitigation strategies are the key portions of the patch management process
  - They allow for business continuity while remaining secure from potential malicious actors.

Rotating Keys

- Periodically generating and implementing new access keys to a server/service.
- Like password rotation, certain services use key files or strings to grant access.
  - Such as a server accessing a repository and should be scheduled for periodic updates.
- Many of the recommendations for passwords apply here, such as using a minimum length and setting up expiry periods for keys.

Certificate Management

- The process of properly administering digital security certificates.
  - Includes managing proper storage and transmission of the certificate as well as the suspension and revocation done in response to certain cases.
- If a certificate is stolen or otherwise negatively affected
  - A new certificate should be generated and implemented, and the old one should be removed and revoked.
- **Certificate pinning** is the process of assigning a specific certificate to a particular element to avoid man-in-the-middle-attacks.

Providing Secret Management Solution

- A platform that controls passwords, key pairs, and other sensitive information that should be stored securely.
- These solutions are usually paid software or services that include the security measures to keep secrets securely stored
- Commonly have support for different types of dynamic and static credentials.

Network Segmentation

- Logically separates system infrastructure using subnets, VLANs and/or firewalls to prevent communicating with one another.
- A common method is to determine:
  - Which services need to be internet-facing
  - Which services need to be both internet-facing and internally accessible
  - Which services should be kept internal only.
- A physically separate network or host (with no cabling or wireless links to other networks) is referred to as air-gapped.

Review Activity: Employ Technical Controls

- List some techniques used when hardening a system
- Discuss reasons for sanitizing user input
- Describe how Multifactor Authentication improves security
- Explain why its recommended to encrypt passwords
- Review when it may be necessary to remediate at the process-level

Review Activity: Employ Technical Controls

- Explain the significance of Patch Management
- Describe what's involved when employing Key Rotation
- Outline why it's essential to secure digital certificates
- Review what's involved in a secret management solution
- Describe the importance of segmenting a network

Lesson 19

Topic 19B

Administrative and Operational Controls

Implementing Policies and Procedures

- Policies and procedures enable an organization to operate normally while minimizing cybersecurity incidents.
- After the PenTest, the team will analyze the risk of identified issues and recommend mitigation strategies on the policies, such as:
  - Implement technical controls where needed
  - Review policies and procedures
  - Put key performance indicators (KPIs) in place
  - Update policies and procedures when needed

Employing Role Based Access Control

- Role Based Access Control is where resources are protected by ACLs that provide user permissions based on job functions.
- This can be done at different levels:
  - On logical resources such as a server, service, database, or file.
  - On physical resources such a building or the server room

Enforcing Minimum Password Requirements

- Password polices are used to reduce the threat of an attack
- The following are examples of password mitigation strategies:
  - Don't allow developers to hard-code credentials into apps.
  - Hash stored passwords rather than storing them in plaintext.
  - Avoid cryptographically weak hash functions, like MD5 and SHA-1.
  - Confirm network access protocols are using strong ciphers
  - Ensure security solutions like IDS and data loss prevention (DLP) can monitor and manage unencrypted traffic in the network.

Securing the Development Lifecycle

- Security should be an active component in the development process and follow a software development life cycle (SDLC).
- An SDLC focuses primarily on the design, development, and maintenance of applications and other software.
  - Development passes through several phases
  - Security is incorporated at each of those phases.
  - Includes best practices during development

Insecure Coding Practices

- The organization should also actively avoid insecure coding practices, that include:
  - Lack of input validation.
  - Hard-coded credentials.
  - Lack of error handling.
  - Verbose comments in source code.
  - Lack of code signing.

Managing Mobile Devices

- Mobile device management (MDM) is is the process of tracking, controlling, and securing the organization's mobile infrastructure.
- Enables the organization to enforce security policies and manage applications, data, and other content, on all connected devices
  - Rather than applying security controls to each device individually.
- Additional policies and procedures that are recommended for clients to implement include:
  - Perform monthly vulnerability scans.
  - Complete annual or biannual penetration tests.

Implementing People Security Controls

- When it comes to people, they always have been, and probably always will be, the weakest link in security.
- In addition to plain old human error, people are also vulnerable to the many social engineering attacks that are in use.
- Some of the mitigation strategies and techniques that you should recommend clients implement include the following:
  - Have management set the security tone, and lead by example
  - Constant reinforcement and reminders
  - Implement penalties for non-compliance

Outlining Other Operational Considerations

- **Job rotation** is the practice of cycling employees though different assigned roles.
- **Time of day restrictions** rely on normal operating hours for users and limits the access they have when it is usually not needed.
- **Mandatory Vacations** - Users are more likely to make mistakes when they are tired or stressed
- **User Training Remediation** should include requiring end-user cybersecurity training for all employees.

Review Activity: Administrative and Operational Controls

- Describe why an organization should implement policies and procedures
- Outline the importance of employing role-based access control and enforcing minimum password requirements
- Explain why it’s essential to include security in the SDLC
- Describe some insecure coding practices that should be avoided
- Review techniques for managing mobile devices
- Discuss reasons it’s important to factor in the people when designing security controls
- List operational considerations when suggesting remediation guidelines

Lesson 19

Topic 19C

Physical Controls

Controlling Access to Buildings

- Building access control manages the ability of individuals entering a facility according to their permission to enter.
- For example, a common implementation in high-rise buildings is using RFID access cards in the elevators
  - Certain floors can only be accessed when the key card is first provided.
- RFID cards may be vulnerable to cloning and replay attacks
  - Other physical access controls can be used to provide additional layers of security.

Employing Biometric Controls

- Biometric controls are enhanced forms of access control that rely on body features, such as the fingerprint or iris.
- Biological characteristics are unique enough to rely on them as access control measures
  - Technology is precise enough to be implemented in a reliable manner.
- Common everyday examples used to unlock the device include
  - Fingerprint scanners in laptops
  - Face recognition features in smartphones

Utilizing Video Surveillance

- Video surveillance monitors activity using cameras.
- Technology such as Wi-Fi or internet-connected features can introduce potential problems and attack vectors. Wi-Fi attacks can:
  - Disconnect cameras from the network and lose video feed
  - Provide an attacker with vital information on inside operations and then used to pivot to navigate the network or perform other attacks.
- Best practices involves using wired connections, network segregation, and patching of the camera firmware.

Review Activity: Physical Controls

- Describe methods to control access to buildings
- Explain how biometric controls can be used to restrict access
- Discuss best practices when using video surveillance

Lesson 19

Summary