Name: Moaz Aboelwafa Abozied

Techniques for Hardening System

1- Disabling Unnecessary Services

Definition:

This technique involves turning off any services, applications, or features on a system that are not essential for its operation.

Contribution to Security:

- **Reduces Attack Surface:** Minimizing the number of running services decreases potential vulnerabilities that attackers can exploit.
- **Prevents Unauthorized Access:** Disabling unnecessary services limits potential entry points for attackers.
- **Improves Performance:** Fewer active services can lead to enhanced system performance, making it easier to monitor and manage security.

2- Implementing Least Privilege Access

Definition:

This principle restricts users' access rights to only those necessary for them to perform their job functions.

Contribution to Security:

- **Limits Damage from Compromised Accounts:** If a user account is compromised, the damage is contained because the attacker has access only to a limited set of resources.
- **Reduces Insider Threats:** Ensuring users have only the permissions they need decreases the risk of malicious actions by insiders.
- **Enhances Accountability:** Distinct roles and permissions make it easier to track actions and hold individuals accountable.

3- Patch Management

Definition:

This technique involves regularly updating software and systems to fix vulnerabilities and improve performance.

Contribution to Security:

- **Closes Security Gaps:** Applying patches promptly protects systems from known vulnerabilities.
- **Enhances System Stability:** Regular updates improve security and ensure systems run smoothly.
- **Maintains Compliance:** Effective patch management helps meet regulatory requirements.

4- Configuration Baselines

Definition:

A configuration baseline is a set of security standards and configurations that a system should adhere to, based on best practices and organizational policies.

Contribution to Security:

- **Establishes a Secure State:** Defining a secure configuration minimizes vulnerabilities.
- **Facilitates Compliance Audits:** Documented baselines make it easier to demonstrate compliance with security standards.
- **Enables Consistency:** Ensures that all systems are configured consistently, reducing the risk of misconfigurations.

5- Network Segmentation

Definition:

This technique involves dividing a network into smaller segments to control traffic and limit access.

Contribution to Security:

- **Limits Lateral Movement:** If an attacker gains access to one segment, segmentation can prevent them from moving to others.
- **Enhances Performance:** Separating different types of traffic improves performance and reduces congestion.
- **Facilitates Compliance:** Isolation of sensitive data and systems makes it easier to comply with data protection regulations.