Suhaila Adel Ali Abd El-Naby

21063119

Session 2 Assignment

1.Define hardening systems

- **Define Systems Hardening:**

Definition: Systems hardening refers to the comprehensive process of securing a computer system by reducing its vulnerability footprint. This includes implementing best practices such as configuring robust security settings, removing unnecessary services, and applying software patches to prevent exploitation.

Importance in Maintaining Cybersecurity: Systems hardening is essential to minimize potential entry points that cybercriminals can exploit. By reducing the system's exposure to threats, organizations can better safeguard sensitive data, maintain service availability, and ensure compliance with security standards. Moreover, a well-hardened system is more resistant to malware, data breaches, and unauthorized access.

- **Systems That Can Benefit from Hardening:**

1. **Servers:**
    - **Importance**: Servers are often the backbone of an organization's IT infrastructure, hosting critical applications and databases.
    - **Hardening Techniques**:
        - Disable unnecessary network services and protocols.
        - Use intrusion detection systems (IDS) and firewalls.
        - Enforce strict permissions and regularly update server software.
    - **Example**: A web server with hardening measures can be protected from vulnerabilities like SQL injection or cross-site scripting (XSS).
2. **Workstations:**
    - **Importance**: Workstations are frequently used by employees and can be a weak point if not secured properly.
    - **Hardening Techniques**:
        - Install antivirus and endpoint protection.
        - Implement regular operating system updates.
        - Configure strong password policies and use multi-factor authentication (MFA).

- **Example**: A corporate laptop used by employees could be hardened by encrypting the hard drive and restricting the installation of unauthorized software.

3. **Network Devices:**
    - **Importance**: Devices like routers, switches, and firewalls control the flow of data within and outside a network, making them critical for overall network security.
    - **Hardening Techniques**:
        - Change default admin credentials and disable remote access.
        - Update firmware regularly to patch vulnerabilities.
        - Use secure communication protocols (e.g., SSH instead of Telnet).
    - **Example**: Hardening a router might include setting up a VPN to ensure secure remote access.

2.Techniques for hardening systems

1. **Disabling Unnecessary Services:**
    - **Description**: This technique involves turning off services, applications, or processes that are not needed for the system to function properly.
    - **Contribution to Security**: By reducing the number of active services, the attack surface is minimized, lowering the chances for hackers to exploit vulnerabilities. This also helps prevent unauthorized access or execution of malware through less-monitored pathways.
2. **Implementing Least Privilege Access:**
    - **Description**: The principle of least privilege restricts user and application permissions to only what is necessary for them to perform their tasks.
    - **Contribution to Security**: Limiting access reduces the risk of internal and external threats. If an account is compromised, the potential damage is minimized as the attacker has restricted access to critical system areas.
3. **Patch Management:**
    - **Description**: Patch management involves regularly updating and applying patches to fix vulnerabilities in software and hardware.
    - **Contribution to Security**: Keeping systems up to date ensures that known security vulnerabilities are patched, preventing attackers from exploiting these weaknesses. This technique is crucial for protecting against zero-day attacks and emerging threats.
4. **Configuration Baselines:**
    - **Description**: Establishing a configuration baseline refers to setting and maintaining a standard security configuration for systems and regularly auditing to ensure compliance.
    - **Contribution to Security**: A consistent and secure configuration helps protect against unauthorized changes, misconfigurations, and security gaps. Automated tools can compare current settings to the baseline, alerting administrators to any discrepancies.
5. **Network Segmentation:**
    - **Description**: Network segmentation divides a network into smaller, isolated segments or zones, each with its security controls.
    - **Contribution to Security**: By isolating sensitive data and systems, segmentation limits an attacker's ability to move laterally within the network. It ensures that even if one segment is compromised, the threat cannot easily spread to other parts of the network.

3.Security standards and guidelines

1. CIS (Center for Internet Security) Benchmarks:

- **Summary**: CIS Benchmarks are a set of best practices and guidelines designed to help organizations secure their systems, networks, and software. These benchmarks are developed through a global community consensus process and are frequently updated to address emerging threats.
- **Implementation**: CIS Benchmarks provide step-by-step configuration recommendations to harden various systems, such as operating systems, cloud environments, and applications. Organizations can use CIS-CAT, an assessment tool provided by CIS, to ensure compliance.
- **Contribution to Hardening Strategies**: By following CIS Benchmarks, organizations can standardize their security practices and reduce vulnerabilities, making it easier to protect against unauthorized access and cyberattacks.

2. NIST (National Institute of Standards and Technology) Guidelines:

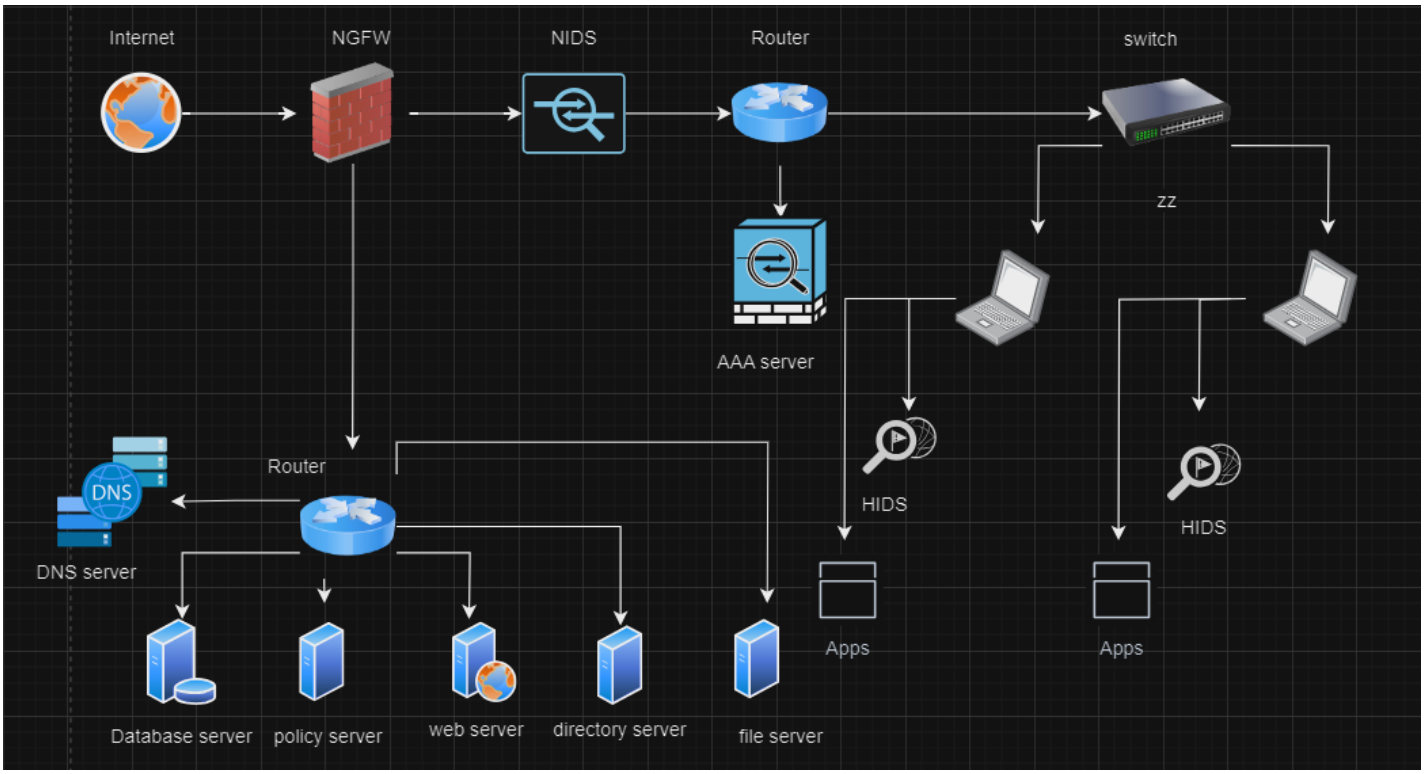
- **Summary**: NIST provides comprehensive guidelines on cybersecurity and risk management, such as the NIST Cybersecurity Framework and Special Publication 800 series. These guidelines cover topics like access control, incident response, and continuous monitoring.
- **Implementation**: NIST's frameworks help organizations assess their current security posture, identify areas for improvement, and implement effective controls. They provide a systematic approach to protecting critical assets and data.
- **Contribution to Hardening Strategies**: NIST guidelines ensure organizations establish robust security measures tailored to their risk environment. This includes strong access controls, encryption practices, and continuous monitoring for anomalies, significantly enhancing system hardening.

3. ISO/IEC 27001:

- **Summary**: ISO/IEC 27001 is an international standard that specifies the requirements for an information security management system (ISMS). It focuses on systematically managing sensitive company information to remain secure.
- **Implementation**: Organizations seeking ISO/IEC 27001 certification must undergo rigorous audits and demonstrate adherence to a structured approach to risk management and data protection. This involves implementing policies, procedures, and controls that mitigate risks effectively.
- **Contribution to Hardening Strategies**: ISO/IEC 27001 provides a framework for identifying, managing, and reducing risks to information security. The standard requires continuous evaluation and improvement of security measures, which aligns with system hardening goals, such as protecting against data breaches and ensuring business continuity.

4.Design a secure network architecture and define the usage of each device

- **Router:** Connects networks and directs traffic (data packets) based on IP addresses.
- **Switches:** Connects devices within a network segment, forwarding traffic based on MAC addresses.
- **NIDS (Network Intrusion Detection System):** Monitors network traffic for malicious activity.
- **Firewall:** Filters network traffic, blocking unauthorized access.
- **Database Servers:** Store and manage data.
- **Policy Servers:** Enforce security policies and access controls.
- **Web Server:** Delivers web content.
- **Directory Servers:** Manage user accounts and authentication.
- **HIDS (Host-based Intrusion Detection System):** Monitors individual hosts for security threats.
- **DNS (Domain Name System):** Translates domain names into IP addresses.
- **NGFW (Next-Generation Firewall):** Advanced firewall that can inspect application-level traffic.
- **File Servers:** Store and share files.
- **Authentication Services:** Verify user identities.
- **DHCP (Dynamic Host Configuration Protocol) Directory Services:** Assign IP addresses to devices.
- **Web Servers Hosting:** Host websites.
- **Internally Used Apps:** Applications used within the organization.



5.TryHackMe challenges

First challenge

Second challenge