Vulnerability Scanning

Task:

Perform regular vulnerability scans on network devices and software.

What is Vulnerability Scanning?

Vulnerability scanning involves identifying security weaknesses in network devices, applications, and operating systems. Regular scans help prevent exploitation by attackers by allowing organizations to patch vulnerabilities before they can be leveraged for attacks.

Steps to Perform a Vulnerability Scan

1. Choose a Vulnerability Scanning Tool

Use tools like OpenVAS, Nessus, or Qualys to automate the scanning process.

2. Define the Scope of the Scan

Identify the network devices, applications, and systems that need to be scanned.

3. Configure Scan Settings

Adjust scan parameters to focus on critical assets, authentication settings, and scan intensity.

4. Run the Vulnerability Scan

Launch the scan and allow it to identify potential security weaknesses.

5. Analyze the Scan Results

Review the detected vulnerabilities and assess their severity.

6. Patch and Mitigate Vulnerabilities

Apply security patches, update software, or implement mitigation strategies based on the scan results.

7. Schedule Regular Scans

Set up automated scans to continuously monitor for new vulnerabilities and improve security posture.

Vulnerability Scanning Tools:

- OpenVAS: https://www.openvas.org/

- Nessus: https://www.tenable.com/products/nessus
- Qualys: https://www.qualys.com/