Basic vulnerability scan

1. Install OpenVAS or Nessus Essentials

- **Instructions**:

  - **Option 1: OpenVAS (Free, Open-Source)**:

    - **Linux (Recommended)**:

      - Install on a Linux distro like Ubuntu or Kali Linux for best compatibility.

      - Run: `sudo apt update && sudo apt install openvas` (Ubuntu/Debian) or use Kali's pre-installed OpenVAS.

      - Initialize OpenVAS: `sudo gvm-setup`. This sets up the Greenbone Vulnerability Management (GVM) suite.

      - Start services: `sudo gvm-start`. Access the web interface at `https://127.0.0.1:9392` (use the credentials generated during setup).

      - Update vulnerability feeds: `sudo gvm-feed-update`.

  - **Option 2: Nessus Essentials (Free for Non-Commercial Use)**:

    - Visit https://www.tenable.com/products/nessus/nessus-essentials.

    - Register with your email to get an activation code.

    - Download the installer for your OS (Windows, macOS, or Linux).

    - Install Nessus Essentials:

      - **Windows**: Run the `.exe` file, follow prompts, and enter the activation code.

      - **Linux/macOS**: Use `dpkg` (Debian) or `rpm` (Red Hat) for Linux, or the `.dmg` for macOS.

    - Access the web interface at `https://localhost:8834` and complete the setup (create an account, enter the activation code).

    - Update plugins: Allow Nessus to download the latest vulnerability plugins during setup.

  - **Verification**: Ensure the web interface is accessible and plugins/feeds are updated.

- **Note**: Choose OpenVAS for open-source flexibility or Nessus Essentials for a user-friendly interface (limited to 16 IPs for scanning). Install only on a system you own or are authorized to use.

---

2. Set Up Scan Target as Your Local Machine IP or Localhost

- **Instructions**:

  - **Find Your Local Machine IP**:

    - **Windows**: Open Command Prompt, run `ipconfig`, and note the “IPv4 Address” (e.g., 192.168.1.100).

    - **Linux/macOS**: Open a terminal, run `ifconfig` or `ip addr`, and note the IP (e.g., `inet 192.168.1.100`).

    - Alternatively, use `127.0.0.1` (localhost) if scanning the machine hosting the scanner.

  - **OpenVAS**:

    - Log in to the Greenbone Security Assistant (web interface).

    - Navigate to **Configuration > Targets**.

    - Create a new target:

      - Name: “Local Machine”.

      - Host: Enter your IP (e.g., `192.168.1.100`) or `127.0.0.1`.

      - Port List: Select “All TCP and UDP” for a full scan.

      - Save the target.

  - **Nessus Essentials**:

    - Log in to the Nessus web interface.

    - Go to **Scans > New Scan > Basic Network Scan**.

    - In the “Targets” field, enter your IP (e.g., `192.168.1.100`) or `localhost`.

    - Save the configuration.

- **Note**: Ensure you have permission to scan the target (in this case, your own machine). Scanning unauthorized systems is illegal.

---

3. Start a Full Vulnerability Scan

- **Instructions**:

  - **OpenVAS**:

    - Go to **Scans > Tasks** and create a new task.

    - Name: “Local Machine Full Scan”.

    - Target: Select the “Local Machine” target created in step 2.

    - Scan Config: Choose “Full and Fast” for a thorough scan with optimized performance.

    - Save and start the scan by clicking the “Play” button.

  - **Nessus Essentials**:

    - In the **Scans** section, select the scan created in step 2.

    - Configure scan settings:

      - Use the “Basic Network Scan” template.

      - Enable “Scan for all ports” under **Settings > Discovery**.

      - Enable credentialed scanning (optional, for deeper inspection):

        - Under **Credentials**, add your local machine’s admin/root credentials (Windows: username/password, Linux: SSH credentials).

    - Launch the scan by clicking **Run Scan**.

  - **Note**: A full scan includes port scanning, service detection, and vulnerability checks. Ensure your machine is online and not in sleep mode during the scan.

---

4. Wait for Scan to Complete (May Take 30-60 Minutes)

- **Instructions**:

  - **OpenVAS**: Check the scan status in the **Scans > Tasks** section. Progress is displayed as a percentage. A full scan on a single machine typically takes 30-60 minutes, depending on the number of open ports and system performance.

  - **Nessus Essentials**: Monitor the scan status in the **Scans** section. A progress bar indicates completion percentage.

  - **Troubleshooting**:

    - If the scan stalls, check network connectivity and ensure the target is responsive.

    - Verify the scanner service is running (e.g., `sudo gvm-check-setup` for OpenVAS or check Nessus service status).

  - **Note**: Avoid running resource-intensive applications during the scan to prevent performance issues.

---

5. Review the Report for Vulnerabilities and Severity.

- **Instructions**:

  - **OpenVAS**:

    - Go to **Scans > Reports** and select the completed scan.

    - Review the report, which categorizes vulnerabilities by severity:

      - **High**: Critical issues (e.g., exploitable services like outdated SMBv1).

      - **Medium**: Moderate risks (e.g., misconfigured HTTPS settings).

      - **Low**: Minor issues (e.g., unnecessary open ports).

    - Note the number of vulnerabilities, affected services/ports, and CVE references.

  - **Nessus Essentials**:

    - Go to **Scans**, click the completed scan, and view the **Vulnerabilities** tab.

- Sort by severity (Critical, High, Medium, Low, Info).

- Review details for each vulnerability, including description, affected component, and CVSS score.

- **Key Metrics to Note**:

- Total vulnerabilities.

- Severity distribution (e.g., 2 Critical, 5 High, 10 Medium).

- Common issues (e.g., outdated software, weak configurations).

- **Example Findings**:

- Outdated Windows version (e.g., unpatched Windows 10).

- Open ports with vulnerable services (e.g., RDP on 3389 with weak credentials).

- Missing security patches for software like Adobe Reader or Java.

---

6. Research Simple Fixes or Mitigations for Found Vulnerabilities

- **Instructions**:

- For each high/critical vulnerability, research mitigations using resources like the National Vulnerability Database (https://nvd.nist.gov/) or vendor documentation.

- **Common Vulnerabilities and Fixes**:

- **Outdated Software (e.g., Windows, Apache)**:

- **Fix**: Update to the latest version (e.g., Windows Update, `sudo apt upgrade` for Linux).

- **Source**: Check vendor sites (e.g., Microsoft, Apache) for patch notes.

- **Unnecessary Open Ports (e.g., 445/SMB)**:

- **Fix**: Disable unused services (e.g., disable SMBv1 via PowerShell: `Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`).

- **Source**: Microsoft documentation or Linux man pages.

- **Weak Credentials (e.g., RDP)**:

- **Fix**: Enforce strong passwords or use SSH keys. Disable remote access if unneeded (e.g., `netsh advfirewall firewall set rule name="Remote Desktop" new enable=no`).

- **Source**: NIST guidelines (https://csrc.nist.gov/).

- **Unencrypted Protocols (e.g., HTTP on port 80)**:

- **Fix**: Enable HTTPS with a valid SSL/TLS certificate or close the port.

- **Source**: Let's Encrypt (https://letsencrypt.org/) for free certificates.

- **General Mitigations**:

- Enable a host-based firewall (e.g., Windows Defender Firewall, `ufw` on Linux).

- Install and update antivirus software (e.g., Windows Defender, ClamAV).

- Regularly update all software to patch known vulnerabilities.

- **Note**: Test fixes in a controlled environment to avoid disrupting system functionality.

---

7. Document the Most Critical Vulnerabilities

- **Scenario**: You're preparing a report for your records or to share with a supervisor to demonstrate your findings.

- **Instructions**:

- Create a document (e.g., Word, Google Docs, or text file) with the following:

- **Scan Details**: Date, time, tool used (OpenVAS/Nessus), and target (e.g., 192.168.1.100).

- **Critical/High-Severity Vulnerabilities**:

- List each vulnerability (e.g., "CVE-2023-1234: Outdated SMBv1").

- Include details: Affected port/service, severity, CVSS score, and potential impact (e.g., remote code execution).

- **Recommendations**: Summarize mitigations from step 6 for each vulnerability.

- **Example**:

```
```

Vulnerability Assessment Report

Date: May 29, 2025

Tool: Nessus Essentials

Target: 192.168.1.100 (Local Machine)

Critical Vulnerabilities:

1. CVE-2023-1234: SMBv1 Enabled (Port 445)

- Severity: Critical (CVSS 9.8)

- Impact: Remote code execution via EternalBlue exploit.

- Recommendation: Disable SMBv1, apply latest Windows patches.

2. CVE-2022-5678: Outdated Apache 2.4.10 (Port 80)

- Severity: High (CVSS 7.5)

- Impact: Denial-of-service attack possible.

- Recommendation: Update Apache to 2.4.57 or later.

Total Vulnerabilities: 15 (2 Critical, 5 High, 8 Medium/Low)

,,,

Outcome: Introductory Vulnerability Assessment Experience and Understanding of Common PC Risks

- **Key Learnings**:

- **Hands-On Experience**: You've installed and configured a professional vulnerability scanner (OpenVAS or Nessus Essentials), conducted a full scan, and interpreted results.

- **Common PC Risks Identified**:

- Outdated software (e.g., unpatched OS or applications) is a frequent source of vulnerabilities.

- Open ports with insecure services (e.g., SMB, RDP) expose systems to exploits.

- Weak configurations (e.g., default credentials, unencrypted protocols) increase attack surfaces.

- **Practical Skills Gained**:

  - Setting up and running vulnerability scans.

  - Analyzing reports to prioritize critical issues.

  - Researching and applying basic mitigations to improve security.

  - Documenting findings for professional reporting.

- **Real-World Application**: This exercise mirrors tasks performed by cybersecurity analysts in vulnerability management, preparing you to identify and mitigate risks in personal or organizational environments.