Step 1: Install OpenVAS or Nessus Essentials

- OpenVAS (Open Vulnerability Assessment System) and Nessus Essentials are both popular vulnerability scanning tools.

- You can install OpenVAS on Linux systems, while Nessus Essentials can be installed on Windows, Linux, or macOS.

- Follow the installation instructions for your chosen tool.

Step 2: Set up scan target

- Identify your local machine's IP address or use localhost (127.0.0.1) as the scan target.

- Ensure the target machine is accessible and configured to allow the scan.

Step 3: Start a full vulnerability scan

- Launch OpenVAS or Nessus Essentials and create a new scan task.

- Select the scan target (your local machine IP or localhost) and choose a full vulnerability scan template.

- Configure any additional settings as needed (e.g., scan scope, credentials).

Step 4: Wait for scan to complete

- The scan may take 30-60 minutes to complete, depending on the system's complexity and the number of vulnerabilities.

- Monitor the scan's progress and wait for it to finish.

Step 5: Review the report

- Once the scan is complete, review the report to identify vulnerabilities and their severity levels.

- Look for critical, high, medium, and low-severity vulnerabilities.

Step 6: Research simple fixes or mitigations

- Research each vulnerability and identify potential fixes or mitigations.

- Prioritize critical and high-severity vulnerabilities.

Step 7: Document critical vulnerabilities

- Document the most critical vulnerabilities, including their severity levels and potential impact.

- Include recommendations for remediation or mitigation.

Step 8: Take screenshots of scan results

- Take screenshots of the scan results, including the vulnerability list and details.

- Use these screenshots for documentation or reporting purposes.

Example of vulnerability report:

- Vulnerability: Outdated software (e.g., Adobe Reader)

- Severity: High

- Description: The software is outdated and vulnerable to exploits.

- Recommendation: Update the software to the latest version.

