Write-Up: Basic Vulnerability Scan Using Nessus and OpenVAS

[NAVNEET BIJALWAN]

1. Introduction

- The objective of this exercise is to perform a basic vulnerability scan on your personal computer using free tools. This will help identify common vulnerabilities that may exist on your system, allowing for timely remediation and improved security posture.

2. Tools Used

- OpenVAS Community Edition: A free and open-source vulnerability scanner that provides comprehensive scanning capabilities.

- Nessus Essentials: A free version of the Nessus vulnerability scanner, which is widely used for identifying vulnerabilities in systems.

3. Procedure

- The following steps outline the process of conducting a vulnerability scan on your PC:

Step 1: Installation

- OpenVAS Installation:

  - Download the OpenVAS Community Edition from the official website.

  - Follow the installation instructions specific to your operating system (Windows, Linux, etc.).

  - Ensure that all dependencies are installed and configured correctly.

- Nessus Essentials Installation:
  - Download Nessus Essentials from the Tenable website.
  - Install the software by following the provided installation guide.
  - Create a free account to obtain an activation code for Nessus Essentials.

Step 2: Setting Up the Scan Target

- Determine your local machine's IP address:
  - On Windows, open Command Prompt and type `ipconfig`.
  - On Linux or macOS, open Terminal and type `ifconfig` or `ip a`.
- Set the scan target in OpenVAS or Nessus Essentials:
  - For OpenVAS, navigate to the "Targets" section and add your local IP address or use "localhost" as the target.
  - For Nessus Essentials, create a new scan and specify the target as your local machine's IP address or "localhost".

Step 3: Starting the Vulnerability Scan

- Initiate a full vulnerability scan:
  - In OpenVAS, select the scan configuration (e.g., Full and Fast) and start the scan.
  - In Nessus Essentials, choose the scan type and click on "Launch" to begin the scanning process.
- Monitor the progress of the scan through the respective user interface.

4. Deliverables

- After the scan is complete, generate a vulnerability scan report. This report will include:
  - A summary of identified vulnerabilities.
  - Risk levels associated with each vulnerability (Critical, High, Medium, Low).
  - Recommendations for remediation or mitigation of the identified issues.

5. Example of Identified Issues

- The scan report may highlight various vulnerabilities, such as:

  - Outdated software versions with known vulnerabilities.
  - Open ports that may expose the system to attacks.
  - Weak passwords or misconfigurations in services.
  - Unpatched operating system vulnerabilities.

Report Findings:

Report on Vulnerabilities Detected in Host **192.168.174.129**

1. Introduction

- This report summarizes the vulnerabilities detected on the host with IP address 192.168.174.129, as identified by the Nessus Essentials scan conducted on May 29, 2025. The host is identified as "METASPLOITABLE" and runs on Ubuntu 8.04 with various services exposed.

2. Scan Overview

- Scan Information:
  - Start Time: Thu May 29 11:10:23 2025
  - End Time: Thu May 29 11:30:59 2025
  - Operating System: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
  - MAC Address: 00:0C:29:FA:DD:2A

3. Vulnerability Summary

- The scan identified a total of 11 critical, 7 high, 26 medium, 9 low, and 114 informational vulnerabilities.

4. Critical Vulnerabilities

- 4.1 Apache Tomcat A JP Connector Request Injection (Ghostcat)
  - Risk Factor: High
  - CVSS Score: 9.8
  - Description: Vulnerable A JP connector allows file read/inclusion, potentially leading to remote code execution.
  - Solution: Update A JP configuration to require authorization or upgrade Tomcat to version 7.0.100 or later.
- **4.2 Apache Tomcat** SEoL (<= 5.5.x)
  - Risk Factor: Critical
  - CVSS Score: 10.0
  - Description: Unsupported version of Apache Tomcat installed, no security patches available.
  - Solution: Upgrade to a supported version of Apache Tomcat.
- **4.3 Bind Shell Backdoor Detection**
  - Risk Factor: Critical
  - CVSS Score: 9.8
  - Description: A shell is listening on a remote port without authentication, indicating potential compromise.
  - Solution: Verify if the host has been compromised and consider system reinstallation.
- **4.4 Canonical Ubuntu Linux SEoL (8.04.x)**
  - Risk Factor: Critical
  - CVSS Score: 10.0
  - Description: Unsupported version of Ubuntu Linux, no security patches available.
  - Solution: Upgrade to a currently supported version of Ubuntu.

5. High Vulnerabilities

- **5.1 Debian OpenSSH**/OpenSSL Package Random Number Generator Weakness
  - Risk Factor: Critical
  - CVSS Score: 10.0
  - Description: Weak SSH host keys due to a bug in OpenSSL's random number generator.
  - Solution: Regenerate all cryptographic material generated on the host.
- **5.2 SSL Version 2 and 3 Protocol Detection**
  - Risk Factor: Critical
  - CVSS Score: 9.8
  - Description: Support for SSL 2.0 and 3.0, which are known to have vulnerabilities.
  - Solution: Disable SSL 2.0 and 3.0; use TLS 1.2 or higher.

6. Medium Vulnerabilities

- 6.1 NFS Shares World Readable
  - Risk Factor: Medium
  - CVSS Score: 7.5
  - Description: NFS server exports world-readable shares without access restrictions.
  - Solution: Implement access restrictions on NFS shares.
- 6.2 SSL Medium Strength Cipher Suites Supported (SWEET32)
  - Risk Factor: Medium
  - CVSS Score: 7.5
  - Description: Support for medium strength SSL ciphers, which are easier to exploit.
  - Solution: Reconfigure the application to avoid medium strength ciphers.

7. Recommendations

- Immediate Actions:
  - Upgrade all outdated software and services to their latest supported versions.
  - Disable any unnecessary services, especially those with known vulnerabilities.
  - Implement strong password policies and secure configurations for all services.
- **Long-term Actions:**
  - Regularly update and patch all software and services.
  - Conduct periodic vulnerability assessments to identify and mitigate new risks.
  - Educate staff on security best practices and the importance of maintaining secure configurations.

- The vulnerabilities identified in this report pose significant risks to the security of the host 192.168.174.129. Immediate action is required to mitigate these risks and ensure the integrity and security of the system.

6. Conclusion

Conducting a basic vulnerability scan on your PC is an essential step in maintaining cybersecurity. By utilizing tools like OpenVAS or Nessus Essentials, users can identify and address vulnerabilities proactively, thereby enhancing the overall security of their systems.

7. Recommendations

- Regularly perform vulnerability scans to keep your system secure.
- Stay updated with the latest security patches and software updates.
- Implement strong password policies and secure configurations for all services.