MIT World Peace University

Information and Cybersecurity
Second Year B. Tech, Semester 1

Learning to Work with NESSUS tool for Vulnerability Assessment

Lab Assignment 11

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 20

May 13, 2023

Contents

1 Aim

Configuration and demonstration of NESSUS tool for vulnerability assessment

2 Objectives

To learn authentication technique for access control

3 Theory

3.1 Vulnerability Assessment

Vulnerability assessment is the process of identifying and evaluating potential security vulnerabilities in a computer system or network. This assessment helps organizations to identify and prioritize potential risks and develop strategies to mitigate them. One of the popular vulnerability assessment tools is Nessus.

Nessus is a widely used vulnerability assessment tool that is designed to scan and detect vulnerabilities in networks, systems, and applications. Here are some of the features of Nessus:

1. Multiple scanning options: Nessus offers various scanning options, including network, web application, and database scanning. It supports multiple protocols, such as TCP/IP, SNMP, SSH, and HTTP/HTTPS.
2. Comprehensive vulnerability database: Nessus maintains a comprehensive database of known vulnerabilities and exploits, which it uses to identify potential vulnerabilities in the target system.
3. Customizable policies: Nessus allows users to customize scan policies based on their specific needs. Users can create policies to scan specific IP addresses, ports, or protocols.
4. Real-time alerts: Nessus provides real-time alerts on critical vulnerabilities, enabling organizations to quickly remediate potential threats.
5. Compliance reporting: Nessus generates compliance reports based on industry standards such as PCI DSS, HIPAA, and CIS.
6. Integration with other tools: Nessus can integrate with other security tools such as SIEMs and incident response platforms.

3.2 How Nessus Works

1. Discovery: Nessus starts by discovering devices on the network, including servers, workstations, routers, and switches.
2. Scan configuration: The user configures the scan policy based on their needs, such as IP range, scanning ports, protocols, and vulnerabilities to scan for.
3. Scan execution: Nessus then scans the target system for vulnerabilities based on the configured policy. The scanning process may take some time, depending on the size of the network and the complexity of the scan policy.

4. Vulnerability assessment: Nessus then analyzes the scan results and reports potential vulnerabilities. It provides detailed information on the type of vulnerability, the level of severity, and possible remediation actions.

5. Reporting: Nessus generates a report that summarizes the vulnerabilities found during the scan. The report includes detailed information on each vulnerability, including its severity level and recommended remediation actions.

4 Platform

Operating System: Arch Linux x86-64
IDEs or Text Editors Used: Visual Studio Code
Compilers or Interpreters : Python 3.10.1

5 Input and Output

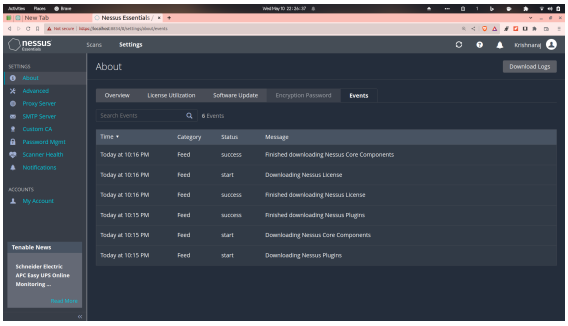

Figure 1: Nessus Home Page

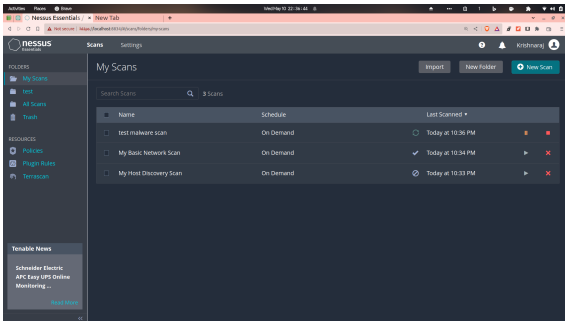

Figure 2: Nessus Scans

6 Conclusion

Thus, we have learnt about the authentication technique for access control, and implemented it using NESSUS tool for vulnerability assessment.Thus, we have seen how to implement digital signatures

using DSA algorithm.

7 FAQ

1. **What vulnerabilities can Nessus detect?**

   Nessus is a vulnerability scanner that can detect a wide range of vulnerabilities in an IT environment, including:

   (a) Operating system vulnerabilities: Nessus can identify vulnerabilities in the operating systems of network devices, servers, and workstations, including Windows, Linux, Unix, and macOS.

   (b) Application vulnerabilities: Nessus can detect vulnerabilities in popular applications such as web browsers, email clients, and office productivity software.

   (c) Network vulnerabilities: Nessus can identify network vulnerabilities, including weak passwords, open ports, and misconfigured network devices.

   (d) Malware and botnets: Nessus can detect signs of malware and botnets on network devices and workstations.

   (e) Web application vulnerabilities: Nessus can identify vulnerabilities in web applications, including SQL injection, cross-site scripting, and directory traversal.

2. **What are the limitations of Nessus essentials?**

   Nessus Essentials is a free version of the Nessus vulnerability scanner that is limited in its capabilities compared to the paid version. Some of the limitations of Nessus Essentials include:

   - Limited scanning: Nessus Essentials is limited to scanning up to 16 IP addresses or hosts at a time, while the paid version can scan thousands of hosts.
   - No scheduling: Nessus Essentials does not allow users to schedule scans or automated reporting, which can be inconvenient for organizations with large IT environments.
   - Limited vulnerability coverage: Nessus Essentials has a smaller set of plugins for detecting vulnerabilities compared to the paid version, which can limit its effectiveness in identifying security issues.
   - No support: Nessus Essentials does not come with technical support from Tenable, the company behind Nessus.

3. **How can you identify a false positive vulnerability in Nessus?**

   A false positive vulnerability in Nessus occurs when the scanner reports a vulnerability that does not actually exist. To identify false positive vulnerabilities in Nessus, follow these steps:

   - Verify the vulnerability: Check the affected device or application to verify if the reported vulnerability actually exists.
   - Check the plugin output: Review the Nessus plugin output to identify any discrepancies or errors that may have led to the false positive.
   - Confirm with multiple sources: Check other vulnerability scanners, security advisories, and technical forums to confirm if the vulnerability is a known issue.

- Perform additional testing: Conduct additional testing or penetration testing to confirm if the vulnerability can be exploited.

4. **How many hosts can Nessus scan? What port does Nessus use?**

   The number of hosts that Nessus can scan depends on the version of the software and the license purchased. The free version of Nessus, Nessus Essentials, can scan up to 16 IP addresses or hosts at a time, while the paid versions can scan thousands of hosts.

   Nessus uses various ports to communicate with the devices being scanned. The default port used by Nessus is 8834 for web-based communication, but Nessus can also use other ports depending on the type of scan being performed. For example, Nessus may use port 22 for SSH communication or port 445 for SMB communication.