Experiment No. 10
Use the NESSUS/ISO Kaali Linux tool to scan the network for vulnerabilities
Date of Performance:
Date of Submission:

Experiment No:10

Use the NESSUS/ISO Kaali Linux tool to scan the network for vulnerabilities

Course Outcome [CSL602.6]: Apply security basics for different attacks on network.

Aim: Use the NESSUS/ISO Kaali Linux tool to scan the network for vulnerabilities

Theory:

1. OpenVAS:

OpenVAS is a free and open-source vulnerability scanner built into Kali. It offers a comprehensive solution similar to Nessus, but requires some configuration. Here's how to use OpenVAS:

Start the service: Use the command openvas-start to initiate the OpenVAS scanner.

Web Interface: Access the OpenVAS web interface at https://localhost:9392 in your web browser. You'll need to set up an admin user and password for initial configuration.

Scans and Reports: The OpenVAS web interface allows you to configure scan targets (IP addresses, ranges), select vulnerability databases, and launch scans. It also generates reports on identified vulnerabilities.

2. Nmap with NSE Scripts:

Nmap, a versatile network mapper, can be used for vulnerability scanning when combined with NSE scripts. Here's how it works:

Basic Scan: Use the nmap command with flags to scan your network. For example, nmap -sT -A 192.168.1.0/24 performs a TCP SYN scan with additional information gathering on the subnet 192.168.1.0/24.

NSE Scripts: Nmap Scripting Engine (NSE) offers various scripts for vulnerability detection. Use the --script flag with the desired script name. For example, nmap --script vuln 192.168.1.10 runs vulnerability scripts against the IP 192.168.1.10. Explore the available NSE scripts with nmap --script-list.

Choosing the Right Tool:

OpenVAS: Offers a user-friendly web interface and a comprehensive vulnerability database. Good for detailed scans and reports. Requires some configuration.

Nmap with NSE Scripts: More lightweight and quicker for basic vulnerability checks. Requires knowledge of specific NSE scripts for desired vulnerabilities.

Resources:

Learning Resources: There are many online resources and tutorials dedicated to using OpenVAS and Nmap with NSE scripts for vulnerability scanning in Kali Linux.

Practice Environment: It's recommended to practice using these tools in a controlled environment (e.g., a personal network) before using them on a production network.

Ethical Hacking: Always obtain permission before scanning any network that you don't have ownership or control over.

Implementation:

Option 1: OpenVAS

OpenVAS is a free and open-source vulnerability scanner pre-installed on Kali Linux. Here's how to use it:

Start the OpenVAS service: Open a terminal window and type:

sudo openvas-start

Access the Web Interface: Open a web browser and navigate to https://localhost:9392. You'll need to set up an administrator user and password for initial configuration.

The first time you access the interface, you'll likely encounter a security certificate error. You can proceed by adding an exception for the self-signed certificate if you're in a controlled environment (your personal network).

Configure a Scan: Once logged in, navigate to the "Scans" tab. Here you can configure a scan by:

Defining Targets: Specify the IP addresses or network ranges you want to scan.

Selecting a Scanner Profile: Choose a pre-configured profile or create a custom one.

Launching the Scan: Click the "Start Scan" button to initiate the vulnerability assessment.

View Reports: After the scan is complete, navigate to the "Reports" tab. Here you'll find detailed reports on identified vulnerabilities, including:

Severity level (critical, high, medium, low)

Description of the vulnerability

Potential impact

Recommendations for remediation

Option 2: Nmap with NSE Scripts

Nmap is a powerful network mapper that can be extended with NSE (Nmap Scripting Engine) scripts for vulnerability detection. Here's how to use it:

Basic Network Scan: Use the nmap command with flags to scan your network. For example:

nmap -sT -A 192.168.1.0/24

This performs a TCP SYN scan with additional information gathering on the subnet 192.168.1.0/24.

Identify NSE Scripts: Explore the available NSE scripts with the command:

nmap --script-list

This will list a vast library of scripts categorized by functionality.

Run Vulnerability Scan: Use the --script flag with the desired script name. For example:

nmap --script vuln 192.168.1.10

This will run vulnerability detection scripts against the IP address 192.168.1.10. You can specify multiple scripts separated by commas.

Conclusion:

Kali Linux is a popular and powerful Linux-based operating system specifically designed for penetration testing, digital forensics, and network security assessments. Its extensive collection of tools and utilities enables cybersecurity professionals, security researchers, and hackers to test the security of computer systems, networks, and applications. However, the misuse of Kali Linux can pose a significant security risk, and the use of its tools can be subject to legal restrictions and regulations in some jurisdictions. Kali Linux is a valuable tool in the fight against cyber threats, but it requires careful use and management to avoid potential problems and ensure that it is used effectively and ethically. Its comprehensive toolkit, regular updates, active community, and flexibility are its advantages, while its complexity, legal risks, security risks, compatibility issues, and limited mainstream support are its disadvantages. Its applications include network scanning and mapping, vulnerability assessment, password cracking, and network sniffing, among others