**Experiment 3: Vulnerability Scanning using OpenVAS**

**Aim:**

Identifying and manage security vulnerabilities in your system.

**A vulnerability scanner (openvas)will scan and evaluate hosts Detects vulnerabilities on your network and systems. It does this by looking for misconfigurations or vulnerabilities, then compiling a report with what it found.**

**OpenVAS:**

**OpenVAS (Open Vulnerability Assessment System)** is a powerful, vulnerability scanner that helps identify security vulnerabilities in computer systems, networks, and web applications. It is part of the **Greenbone Vulnerability Management (GVM)** suite, which provides tools for scanning, reporting, and managing vulnerabilities.

**Prerequisites for Using OpenVAS**

1. A Linux-based server or VM with kali linux
2. Root or sudo access for installation and setup.
3. Stable internet connection for updates.

### Why OpenVAS?

1. **Open Source**: Being open-source means that OpenVAS is freely available
2. **Comprehensive Vulnerability Detection**: OpenVAS boasts a vast database of known vulnerabilities
3. **Regular Updates**: The OpenVAS community actively maintains and updates the tool

**Openvas installation procedure:**

## **Prepare Kali Linux for the installation of OpenVAS**

*sudo apt update* ***—***or use *sudo apt-get update*

## **Installing OpenVAS on Kali Linux**

sudo apt install openvas

1. start the setup process
2. Verify the Installation

## Starting OpenVAS

1. First time you want to open this URL you will get a security warning. Click on **Advanced** and **Accept the Risk and Continue**.
2. The **Greenbone Security Assistant**login page is displayed.
3. Type the credentials in the Username and Password text box and click Login. use the automatically generated admin credentials
4. Configuration for a new target
5. Creating a Task. On **Task,**click in the **Reports**field.

**Key Features of OpenVAS**

1. Comprehensive Vulnerability Scanning:
   * Supports multiple network protocols Detects a wide range of vulnerabilities
2. Regular Updates:
3. Customizable Scans:
   * Allows users to create custom scan configurations and tailor scanning to specific needs.
4. Scalability:
   * Suitable for small-scale networks as well as large enterprise environments.

5. Customizable Scan Configurations

6. Detailed Reporting

7. Credentialed Scanning

8. Uncredentialed Scanning

9. Integration With Other Tools

10.Scalability

11.Open Source

**Experiment 4 :**

**Internal Penetration Testing**

**a. Mapping b. Scanning**

**Aim:**

Internal penetration testing simulates an attack from within the network to identify vulnerabilities that could be exploited by an insider or an attacker who has breached the perimeter. This type of testing involves **mapping** and **scanning** as critical steps in understanding the network structure and identifying potential vulnerabilities.

**a. Mapping**

**Network Mapping with nmap tool**

1. $ Nmap -PR -sn Host/n
2. $ Nmap -PE -sn Host
3. $ Nmap -PA80 -sn Host
4. $ nmap -O -V host
5. $ nmap -sL Host
6. $ Nmap -iL iplist.txt
7. $ Nmap -P 22 -iL iplist.txt
8. $ Sudo nmap -sA -iL iplist.txt
9. $ Sudo nmap -sV -iL iplist.txt
10. $ Sudo nmap -O -iL iplist.txt
11. $ sudo nmap host -f
12. $ sudo nmap host –spoof-mac o
13. $ nmap -iL iplist.txt –script vuln
14. $ sudo nmap -sV -P21-8080 –script vulners Host
15. $ nmap –script vulscan
16. $ nmap -vulners -sV host

**b. Scanning**

Scanning focuses on identifying weaknesses or vulnerabilities in the discovered systems and services.

Types of Scanning

1. Port Scanning:
   * Detect open ports on discovered hosts to identify services in use.

nmap -p- 192.168.1.0/24

nmap -sT- 192.168.1.0

nmap -sS- 192.168.1.0

nmap -sA- 192.168.1.0

1. Service Version Detection:
   * Determine the software version running on open ports.

nmap -sV 192.168.1.10

* + - * .

1. Operating System Fingerprinting:
   * Identify the OS of devices for targeting vulnerabilities specific to them.

nmap -O 192.168.1.10

**Tools for Mapping and Scanning**

1. Mapping:
   * Nmap,
2. Scanning:
   * Nmap