Task 3: Perform a Basic Vulnerability Scan

Objective

To use a free vulnerability scanning tool (OpenVAS or Nessus Essentials) to identify common vulnerabilities on the local machine and document findings, learn about mitigations, and gain hands-on experience in vulnerability assessment.

Tools Used

- **OS:** Kali Linux (or any other Linux distro)
- **Tool:**
  - **Option 1:** OpenVAS (GVM)
  - **Option 2:** Nessus Essentials

Steps to Perform

1. Install Vulnerability Scanner

Option A: OpenVAS (GVM)

```
sudo apt update
sudo apt install openvas
sudo gvm-setup
```

Fix any issues shown by 'sudo gvm-check-setup' until it says "installation is OK".

Option B: Nessus Essentials

1. Download .deb file:

```
wget
https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.7.3-debian10_amd64.deb
```

2. Install Nessus:

```
sudo dpkg -i Nessus-*.deb
sudo systemctl start nessusd
```

3. Access Web GUI:

```
https://localhost:8834
```

2. Setup the Scan

- Open the scanner dashboard (OpenVAS GUI or Nessus Web GUI).
- Create a new scan.
- Set target to:

```
127.0.0.1 or your local machine IP (e.g., 192.168.1.x)
```

- Select Full/System scan or Basic Network Scan.

3. Run the Scan

- Start the scan and let it run completely (may take 30–60 mins).
- Do not interrupt until it finishes.

4. Review Results

- After scan completion, open the report.
- Check vulnerabilities by severity:
  - Critical

- High
- Medium
- Low
- Info

5. Analyze & Document
- Open the most critical vulnerabilities.
- For each:
  - Note Vulnerability Name
  - CVSS Score
  - Affected Services
  - Suggested Fix

6. Research Mitigations
- Use CVE or Nessus plugin ID to research:
  - Software patches
  - Configuration changes
  - Best practices

7. Take Screenshots
- Screenshot of:
  - Dashboard
  - Vulnerabilities summary
  - Details of one critical vulnerability
  - CVSS chart or pie chart (if available)

8. Save/Export Report
- Export the full report in:
  - PDF / HTML format (from Nessus or OpenVAS GUI)

Final Deliverables
- Screenshots of scan setup, results
- PDF/HTML report of vulnerabilities
- Summary table of top issues
- Short note on 1–2 fixes you would apply

Example: Summary Table

Vulnerability Title	Severity	CVSS	Fix/Mitigation
SSH Server CBC Mode Ciphers	Medium	5.3	Disable CBC ciphers in SSH config
SSL Self-Signed Certificate	High	7.4	Replace with valid, trusted certificate
Apache Outdated Version	Critical	9.8	Update to the latest stable version

Outcome
Understood how to use a vulnerability scanner
Identified real issues in system setup
Learned about patching and secure configurations
Gained beginner-level experience in vulnerability management