**REPORT FILE FOR TASK 3**

# ELEVATELABS-CYBERSECURITY-INTERNSHIP-TASK-3-vulnerability Scan

**TASK 3:- PERFORM A BASIC VULNERABILITY SCAN ON YOUR PC.**

**⚙️ Objective:**

Use free tools available in Kali Linux to identify common vulnerabilities on your computer.

**🖥️ Scan Target:**

127.0.0.1 (Localhost)

**🧰 Tools Used:**

**nmap –** for port and vulnerability scanning.

**nikto –** for scanning web servers.

**lynis –** for full system security auditing.

**✅Step 1:** Update Kali Linux

Open the terminal and run:

sudo apt update && sudo apt upgrade -y

**✅ Step 2:** Scan with Nmap for Open Ports & Vulnerabilities

Nmap is pre-installed in Kali. Run:

sudo nmap --script vuln 127.0.0.1

This uses nmap's built-in vulnerability detection scripts.

**✅ Step 3**: Scan Web Server with Nikto (if running a local web server)

sudo nikto -h http://127.0.0.1

This will test for common vulnerabilities like outdated software, default files, etc.

**✅ Step 4:** Perform System Security Audit with Lynis

Install if not available:

sudo apt install lynis -y

Run audit:

sudo lynis audit system

Lynis will give a detailed security audit with suggestions.

**✅ Step 5:** Analyze Results

Nmap: Look at open ports and detected vulnerabilities.

Nikto: Note insecure configurations or outdated software.

Lynis: Check the score and review suggested actions.

🔍SHORT SUMMARY ...........................................................................

✅ 1. Updated Kali Linux

sudo apt update && sudo apt upgrade -y

✅ 2. Nmap Scan for Open Ports and Services

sudo nmap -sS -sV -T4 -O -v 127.0.0.1

✅ 3. Nmap Vulnerability Scan

sudo nmap --script vuln 127.0.0.1

✅ 4. Web Server Scan Using Nikto

sudo nikto -h http://127.0.0.1

✅ 5. System Audit Using Lynis

sudo apt install lynis -y

sudo lynis audit system

**📊 Summary of VULNURABILITIES FINDINGS** ..............-----------------------------------------------------

Tool Result Summary

Nmap Detected open ports: [e.g., 22, 80]. Services: SSH, HTTP

Nikto Found potential issues: outdated Apache version, directory listing enabled

Lynis Audit Score: 68/100. Suggestions: update firewall rules, disable unused services

⚠️ Critical Vulnerabilities Identified:

Open SSH port (22) – Exposed to brute force attacks.

Directory listing enabled – Reveals sensitive file structure.

Outdated services – May contain unpatched vulnerabilities.

🛡️ Suggested Fixes/Mitigations:

Configure firewall using ufw:

sudo apt install ufw

sudo ufw enable

sudo ufw allow only required ports

Disable directory listing in web server config.

**RESULT**