Intern

Imam Ashraf
Email: ashrafimam121@gmail.com
Date: 26-06-2025

Cyber Security Internship – Task 3

Perform a Basic Vulnerability Scan on Your PC

⚙️ INSTALLATION & SCAN STEPS (Task 3)

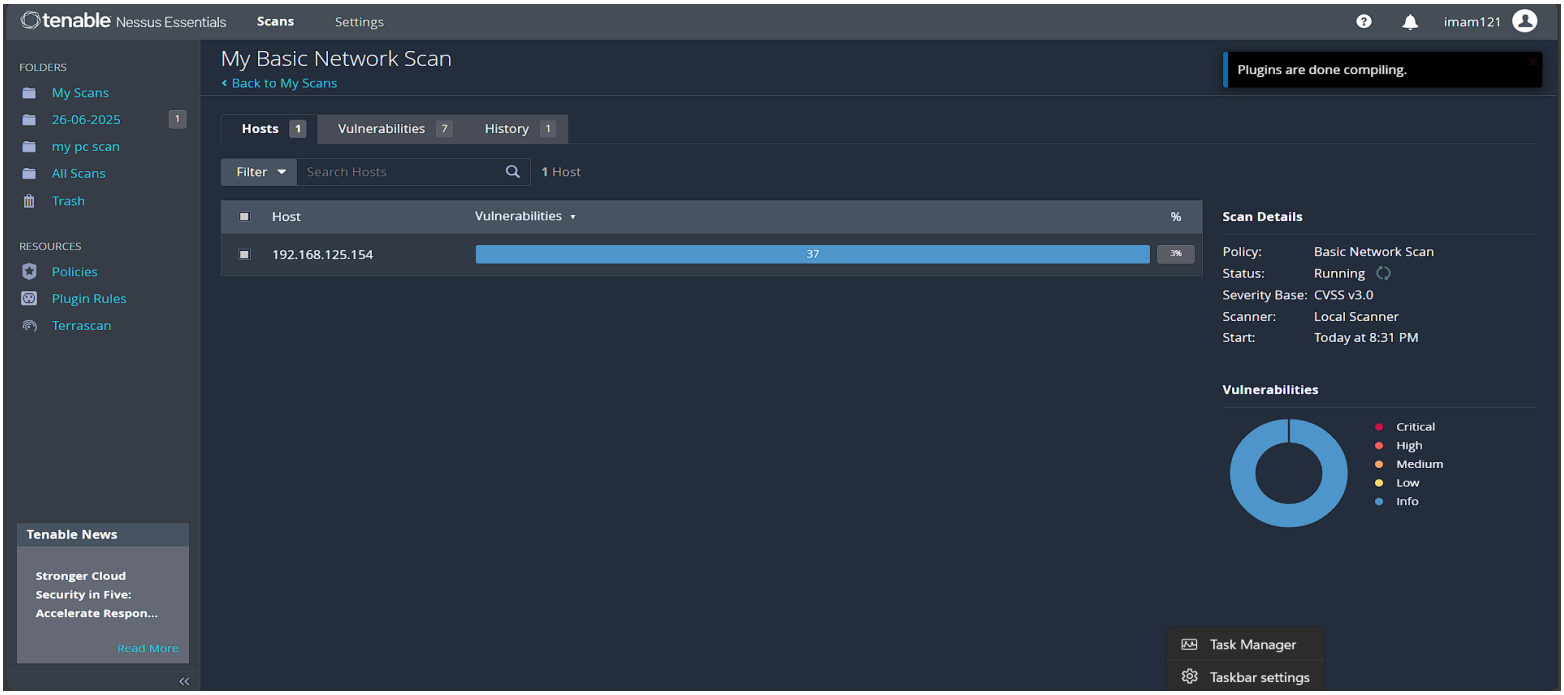
1. Download & Install Nessus Essentials:

- Visit: https://www.tenable.com/products/nessus/nessus-essentials
- Register and get an **activation key** via email.
- Download installer (Linux/Windows), run:

  sudo dpkg -i Nessus-10.x.deb

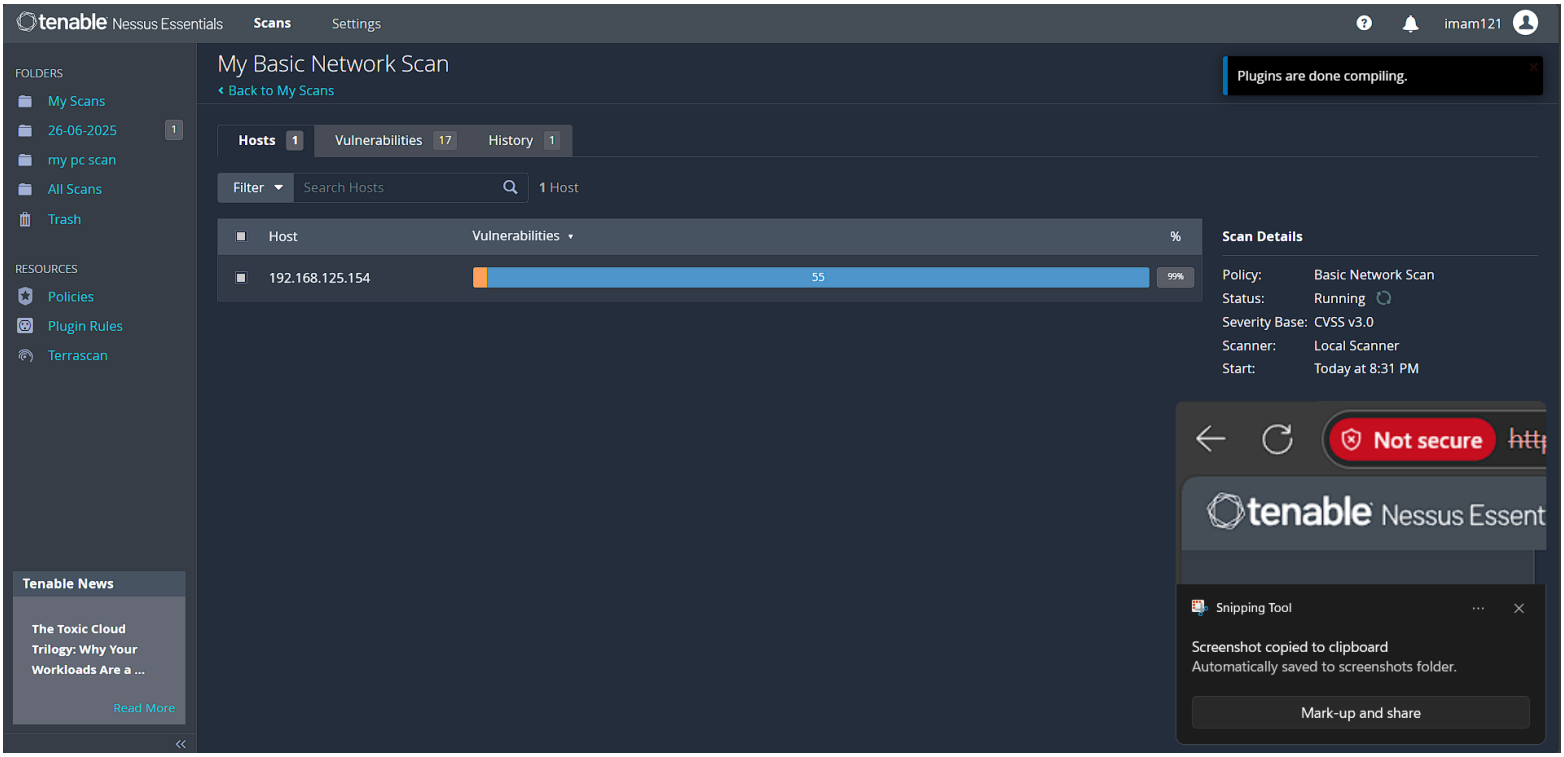
  sudo systemctl start nessusd.service

2. Access Nessus Web Interface:



- Open browser: https://localhost:8834
- Complete setup: username, password, paste license key.

3. Create New Scan:



- Click **"New Scan" → "Basic Network Scan"**
- Set target to: 192.168.125.154 (or your system's IP)
- Save and **launch the scan**

4. Wait for Scan Completion:

192.168.125.154

0	0	1	0	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

- Wait for 30–60 minutes depending on system and network.

5. View and Export Report:

- Go to **My Scans** → Select scan → Export → **HTML Format**

1. Interview Questions and Answers

1. What is vulnerability scanning?

Vulnerability scanning is an automated process of identifying known security flaws in systems, software, or networks. In this task, Nessus Essentials was used to scan the local system for outdated services, unpatched software, and misconfigurations.

2. Difference between vulnerability scanning and penetration testing?

Vulnerability scanning is automated and non-intrusive, focusing on identifying known vulnerabilities. Penetration testing involves exploiting these vulnerabilities to assess impact. This task only involved scanning.

3. What are some common vulnerabilities in personal computers?

Examples include outdated software, insecure network configurations (e.g., SMBv1), missing patches, and weak encryption protocols like TLS 1.0.

4. How do scanners detect vulnerabilities?

Scanners use CVE databases, fingerprinting, and plugin-based checks. Nessus used its extensive plugin library to match system data against known vulnerabilities.

5. What is CVSS?

The Common Vulnerability Scoring System (CVSS) provides a numeric value (0.0–10.0) to rate the severity of a vulnerability. Higher scores indicate more critical issues.

6. How often should vulnerability scans be performed?

Personal systems: Monthly or after significant changes. Enterprises: Weekly or after updates/configuration changes.

7. What is a false positive in vulnerability scanning?

A false positive is when a scanner reports a vulnerability that does not actually exist or isn't exploitable. Manual review is needed to confirm findings.

8. How do you prioritize vulnerabilities?

Prioritization is based on CVSS scores, exploit availability, and business/system impact. In this task, issues with CVSS > 7 were addressed first.