CYBER SECURITY INTERNSHIP

Task 3 : Perform a Basic Vulnerability Scan on Your PC.

Objective: Use free tools to identify common vulnerabilities on your computer.

Tools: Nessus Essentials.

Deliverables: Vulnerability scan report with identified issues.

- **Introduction:**

The purpose of this task is to perform a **vulnerability assessment** on my local Kali Linux system using **Tenable Nessus Essentials**, a widely used vulnerability scanner.
The goal is to identify potential system weaknesses, understand severity levels, and learn how security scanners detect risks based on CVEs (Common Vulnerabilities and Exposures) and CVSS scores.

- **Tools Used:** Nessus Essentials

Nessus Essentials is a free vulnerability scanner that performs:

- ✓ Host discovery
- ✓ Port scanning
- ✓ Service enumeration
- ✓ Vulnerability detection
- ✓ Risk scoring (Critical, High, Medium, Low)

It uses a large plugin database to match system findings with known vulnerabilities.

- **Machine Scanned:**

- ✓ **Operating System:** Kali Linux (VMware Workstation)
- ✓ **IP Address:** 192.XXX.XXX.XXX
- ✓ **Network Type:** NAT (VMware virtual network)

I performed the scan on my own virtual machine to identify security issues related to services, ports, and outdated configurations.

- **Steps Performed:**

Step1: Installed Nessus Essentials

Downloaded the Debian package from the official Tenable website and installed it using:

Command:

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

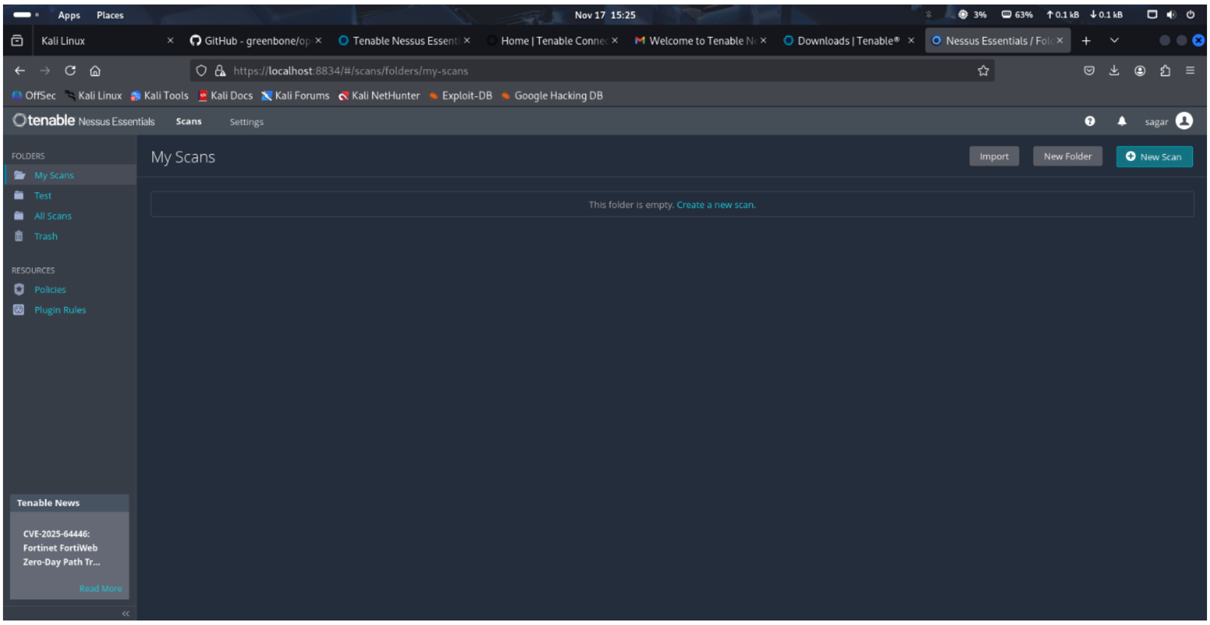
Accessed the Nessus web interface through:
Command: https://localhost:8834/

Step 2: Waited for Plugin Compilation

Nessus downloaded and compiled all vulnerability plugins.
This process takes 20–40 minutes.

Step 3: Created a New Scan

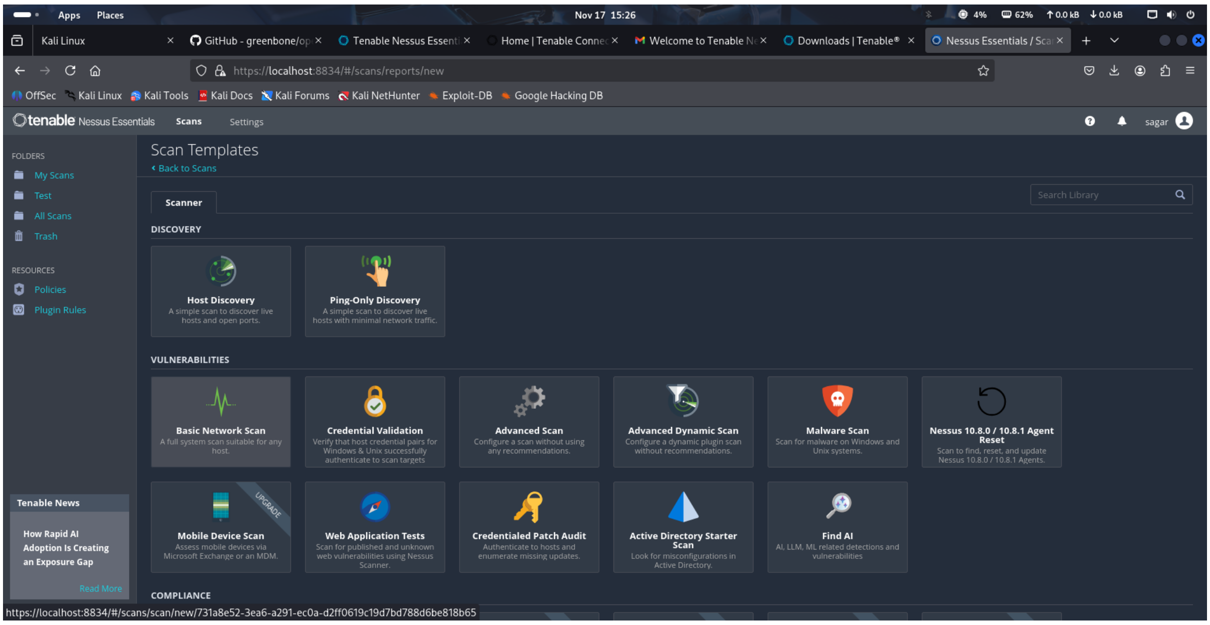
1. Clicked New Scan
2. Selected Basic Network Scan
3. Set target as: 192.XXX.XXX.XXX



My Scans

This folder is empty. Create a new scan.

CVE-2025-64446: Fortinet FortiWeb Zero-Day Path Tr...



Scan Templates

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

Ping-Only Discovery
A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Credential Validation
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Nessus 10.8.0 / 10.8.1 Agent Reset
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

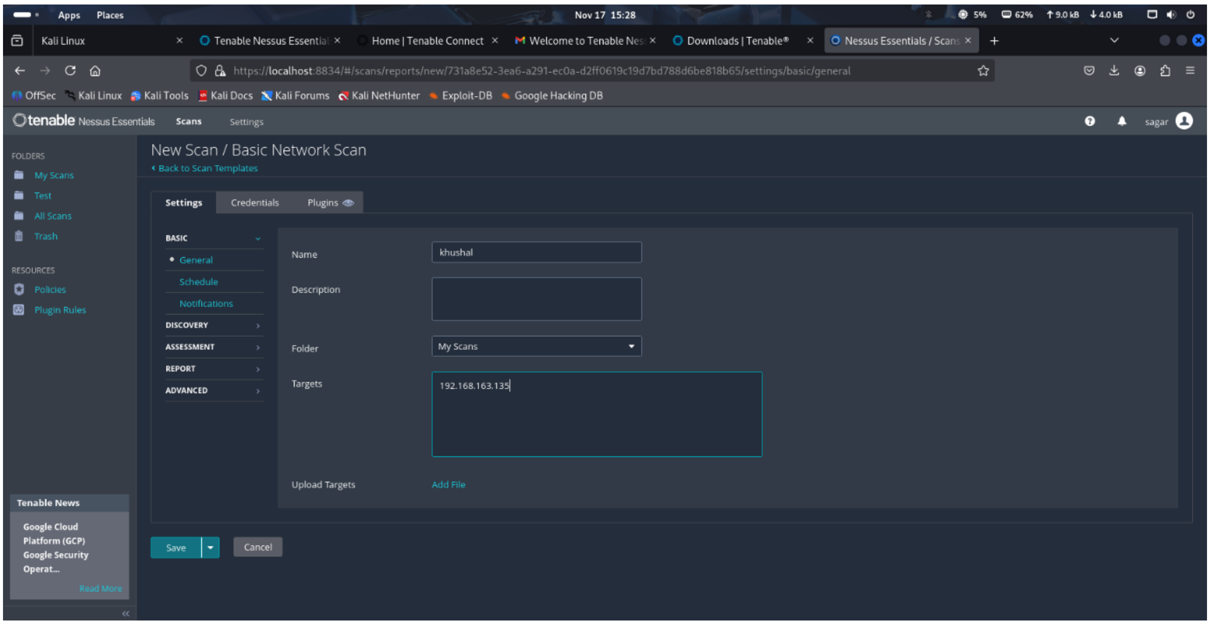
Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Find AI
AI, LLM, ML related detections and vulnerabilities

COMPLIANCE

How Rapid AI Adoption Is Creating an Exposure Gap

https://localhost:8834/#/scans/scan/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65



Name: khushal

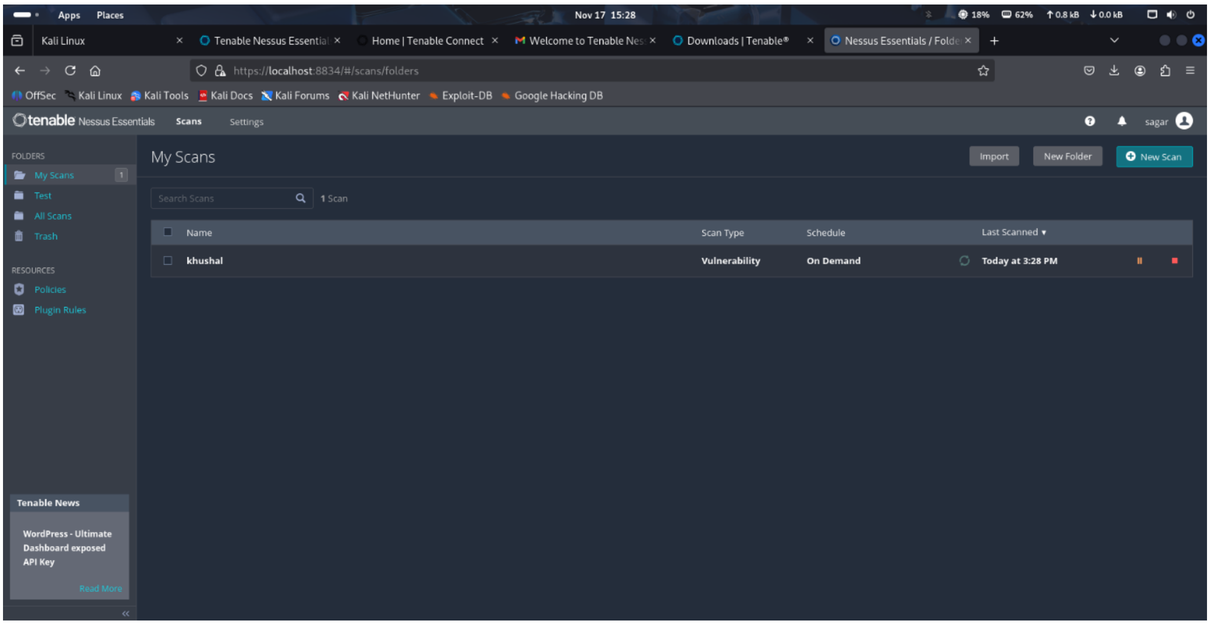
Description:

Folder: My Scans

Targets: 192.168.163.135

Step 4: Launched the Scan:
Clicked Launch, and Nessus began scanning for:

- Open ports
- Running services
- Software versions
- Known vulnerabilities
- Weak configurations



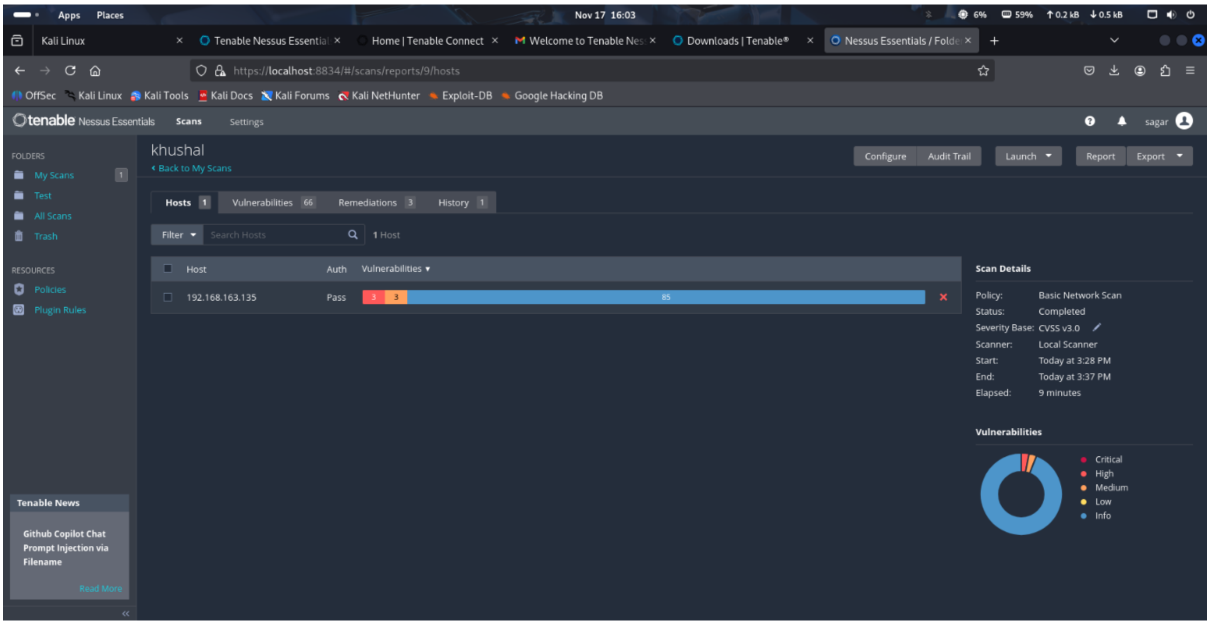
Name	Scan Type	Schedule	Last Scanned ▾
khushal	Vulnerability	On Demand	Today at 3:28 PM

Host Scanned:

192.XXX.XXX.XXX (Kali VM)

Total Vulnerabilities Found:

66 vulnerabilities



khushal

‹ Back to My Scans

Hosts 1 | Vulnerabilities 66 | Remediations 3 | History 1

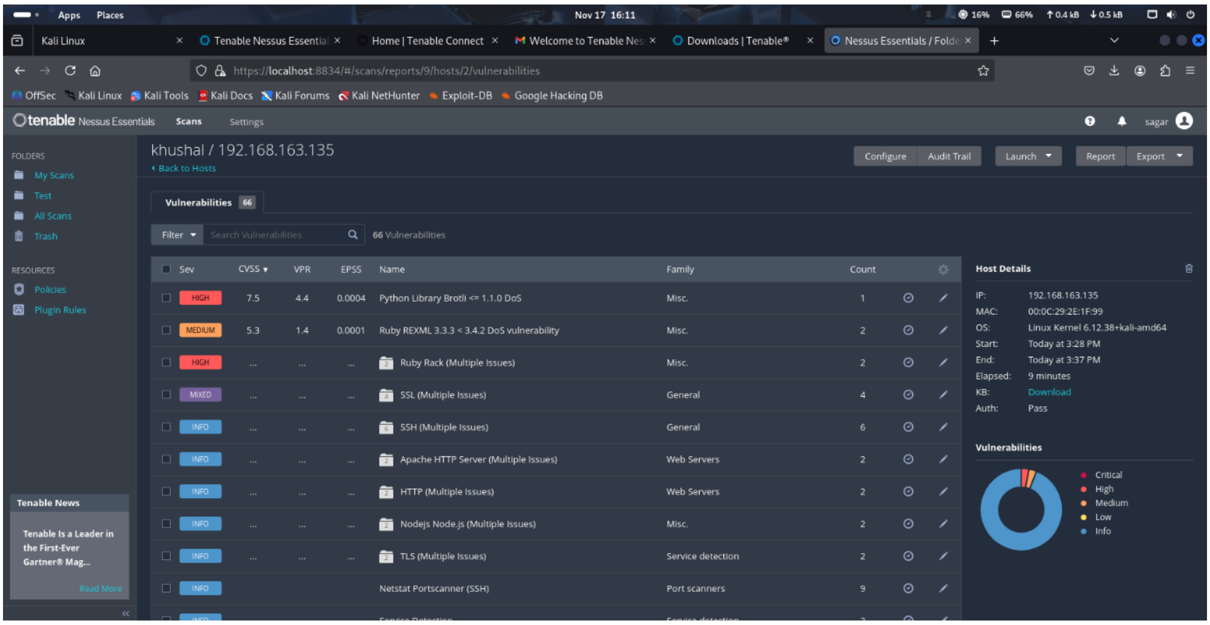
Filter ▾ Search Hosts 1 Host

☐	Host	Auth	Vulnerabilities ▾
☐	192.168.163.135	Pass	3 3 85

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:28 PM
End: Today at 3:37 PM
Elapsed: 9 minutes

Vulnerabilities



khushal / 192.168.163.135

‹ Back to Hosts

Vulnerabilities 66

Filter ▾ Search Vulnerabilities 66 Vulnerabilities

☐	Sev	CVSS ▾	VPR	EPSS	Name	Family	Count
☐	HIGH	7.5	4.4	0.0004	Python Library Brotli <= 1.1.0 DoS	Misc.	1
☐	MEDIUM	5.3	1.4	0.0001	Ruby REXML 3.3.3 < 3.4.2 DoS vulnerability	Misc.	2
☐	HIGH	...	...	...	Ruby Rack (Multiple Issues)	Misc.	2
☐	MIXED	...	...	...	SSL (Multiple Issues)	General	4
☐	INFO	...	...	...	SSH (Multiple Issues)	General	6
☐	INFO	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
☐	INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
☐	INFO	...	...	...	Nodejs Node.js (Multiple Issues)	Misc.	2
☐	INFO	...	...	...	TLS (Multiple Issues)	Service detection	2
☐	INFO				Netstat Portscanner (SSH)	Port scanners	9
☐	INFO				Service Detection	Service detection	2

Host Details

IP: 192.168.163.135
MAC: 00:0C:29:2E:1F:99
OS: Linux Kernel 6.12.38+kali-amd64
Start: Today at 3:28 PM
End: Today at 3:37 PM
Elapsed: 9 minutes
KB: Download
Auth: Pass

Vulnerabilities

High Severity Vulnerability Example:

Python Library Brotli ≤ 1.1.0 – DoS Vulnerability

Description:
The installed Brotli library version (1.1.0) is vulnerable to a Denial-of-Service (DoS) attack due to improper handling of decompression.

Impact:
An attacker may crash applications using this library by sending malicious Brotli-compressed data.

CVSS Score: 3.6 (High Severity in Nessus context)

Solution (Fix Applied):
Updated Brotli to the latest version:

```
sudo apt update

sudo apt upgrade -y

pip3 install --upgrade brotli
```