VAPT Internship Task – CyArt

PART 1: THEORETICAL KNOWLEDGE

1. Understanding Security Assessment

Objective

Learn how to evaluate systems without using paid tools.

Explanation

Security Assessment is the process of identifying weaknesses in systems, networks, or applications using established frameworks.

Frameworks such as **NIST guidelines** help in systematically evaluating security posture.

Types of Security Testing

Vulnerability Assessment
Identifies known vulnerabilities using scanners like **OpenVAS** (open-source).

Penetration Testing
Simulates real-world attacks using tools such as **Metasploit** and **Nmap** on Kali Linux.

Compliance Testing
Validates systems against standards using checklists like **CIS Benchmarks**.

2. VAPT Methodology

Objective

Follow a structured Vulnerability Assessment and Penetration Testing approach.

Explanation

VAPT follows defined phases to ensure proper testing.

Phases

Planning
Define scope and objectives using tools like **Dradis CE**.

Discovery
Identify hosts and vulnerabilities using **Nmap** and **OWASP ZAP**.

Attack
Exploit vulnerabilities using **Metasploit Framework**.

Reporting
Document findings using templates from **Pentest-Tools**.

How to Learn

Practice using the **OWASP Web Security Testing Framework (WSTG)**.

3. Security Standards & Compliance

Objective

Align security practices with regulatory standards.

Explanation

Organizations follow standards to protect sensitive data.

Standards

GDPR
HIPAA
ISO 27001

How to Learn

Use **OWASP Top 10** to prioritize common web vulnerabilities.

4. Risk Assessment Basics

Objective

Prioritize vulnerabilities using scoring systems.

Explanation

CVSS Calculator
Used to assign severity scores (via NVD CVSS Calculator).

Risk Matrix
Categorizes risks as **High / Medium / Low** using spreadsheets (Excel or Google Sheets).

5. Common Vulnerabilities

Objective

Identify common flaws in systems and applications.

Explanation

Network Vulnerabilities
Misconfigurations and open ports identified using **Nmap**.

Web Vulnerabilities
SQL Injection (SQLi) and Cross-Site Scripting (XSS) practiced on **OWASP Juice Shop**.

How to Learn

Metasploitable VM
VulnHub machines

6. Documentation Fundamentals

Objective

Create structured vulnerability reports.

Explanation

Tools

Dradis CE – Collaborative reporting
CherryTree – Technical note-taking
Any standard reporting too

How to Learn

Use free reporting templates available on **GitHub**.

PART 2: PRACTICAL APPLICATION

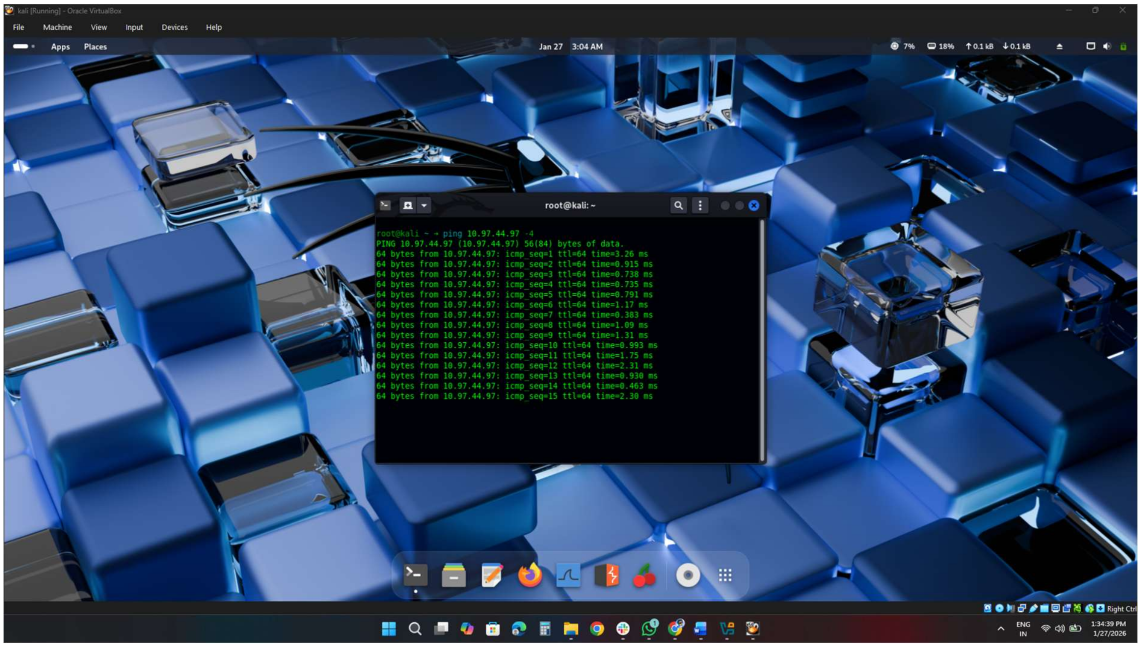
1. Setup Testing Environment

Objective

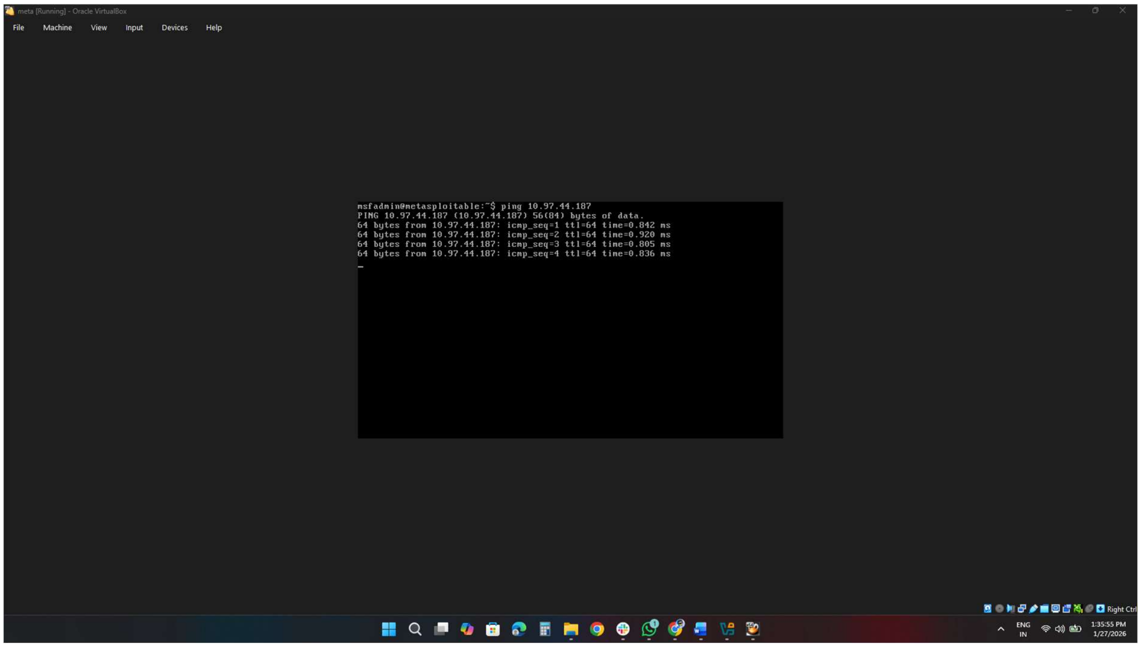
To prepare a controlled lab environment for vulnerability assessment and penetration testing.

Tools Used

- Kali Linux
- Metasploitable (Vulnerable VM)
- VirtualBox



```
root@kali ~ → ping 10.97.44.97 -4
PING 10.97.44.97 (10.97.44.97) 56(84) bytes of data.
64 bytes from 10.97.44.97: icmp_seq=1 ttl=64 time=3.26 ms
64 bytes from 10.97.44.97: icmp_seq=2 ttl=64 time=0.915 ms
64 bytes from 10.97.44.97: icmp_seq=3 ttl=64 time=0.738 ms
64 bytes from 10.97.44.97: icmp_seq=4 ttl=64 time=0.735 ms
64 bytes from 10.97.44.97: icmp_seq=5 ttl=64 time=0.791 ms
64 bytes from 10.97.44.97: icmp_seq=6 ttl=64 time=1.17 ms
64 bytes from 10.97.44.97: icmp_seq=7 ttl=64 time=0.383 ms
64 bytes from 10.97.44.97: icmp_seq=8 ttl=64 time=1.09 ms
64 bytes from 10.97.44.97: icmp_seq=9 ttl=64 time=1.31 ms
64 bytes from 10.97.44.97: icmp_seq=10 ttl=64 time=0.993 ms
64 bytes from 10.97.44.97: icmp_seq=11 ttl=64 time=1.75 ms
64 bytes from 10.97.44.97: icmp_seq=12 ttl=64 time=2.31 ms
64 bytes from 10.97.44.97: icmp_seq=13 ttl=64 time=0.930 ms
64 bytes from 10.97.44.97: icmp_seq=14 ttl=64 time=0.463 ms
64 bytes from 10.97.44.97: icmp_seq=15 ttl=64 time=2.30 ms
```



```
msfadmin@metasploitable:~$ ping 10.97.44.187
PING 10.97.44.187 (10.97.44.187) 56(84) bytes of data.
64 bytes from 10.97.44.187: icmp_seq=1 ttl=64 time=0.842 ms
64 bytes from 10.97.44.187: icmp_seq=2 ttl=64 time=0.920 ms
64 bytes from 10.97.44.187: icmp_seq=3 ttl=64 time=0.805 ms
64 bytes from 10.97.44.187: icmp_seq=4 ttl=64 time=0.836 ms
_
```

2. Vulnerability Scanning

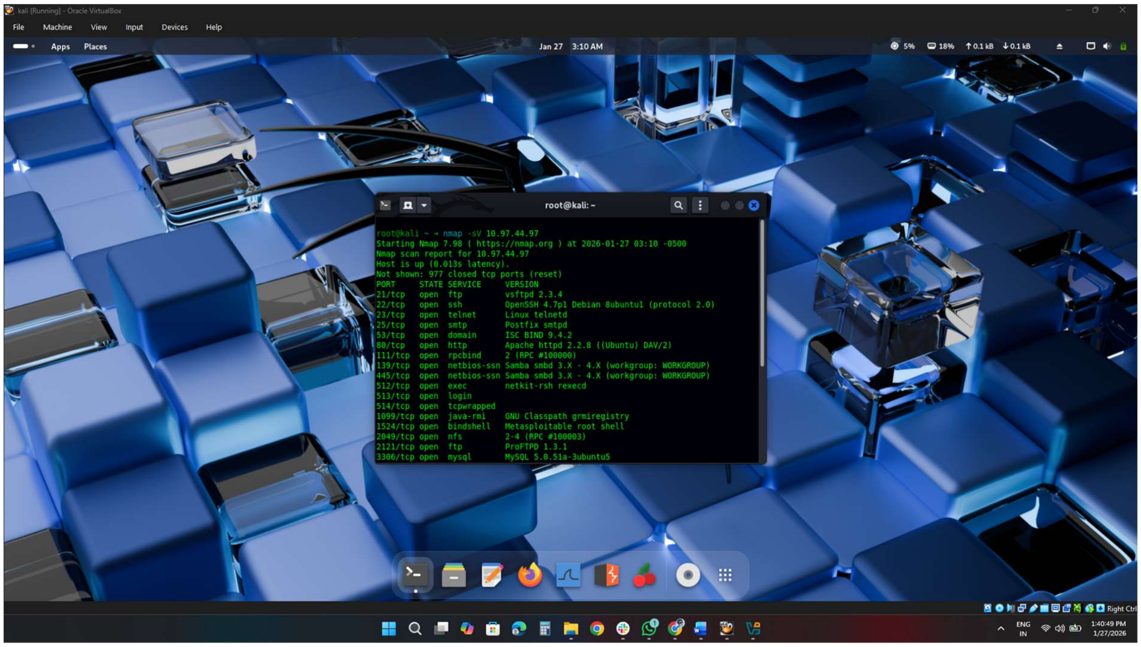
Objective

To identify vulnerabilities using open-source scanning tools.

Tools Used

OpenVAS
Nikto
Nmap

2.1 Network Scanning using Nmap



```
root@kali ~ → nmap -sV 10.97.44.97
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-27 03:10 -0500
Nmap scan report for 10.97.44.97
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

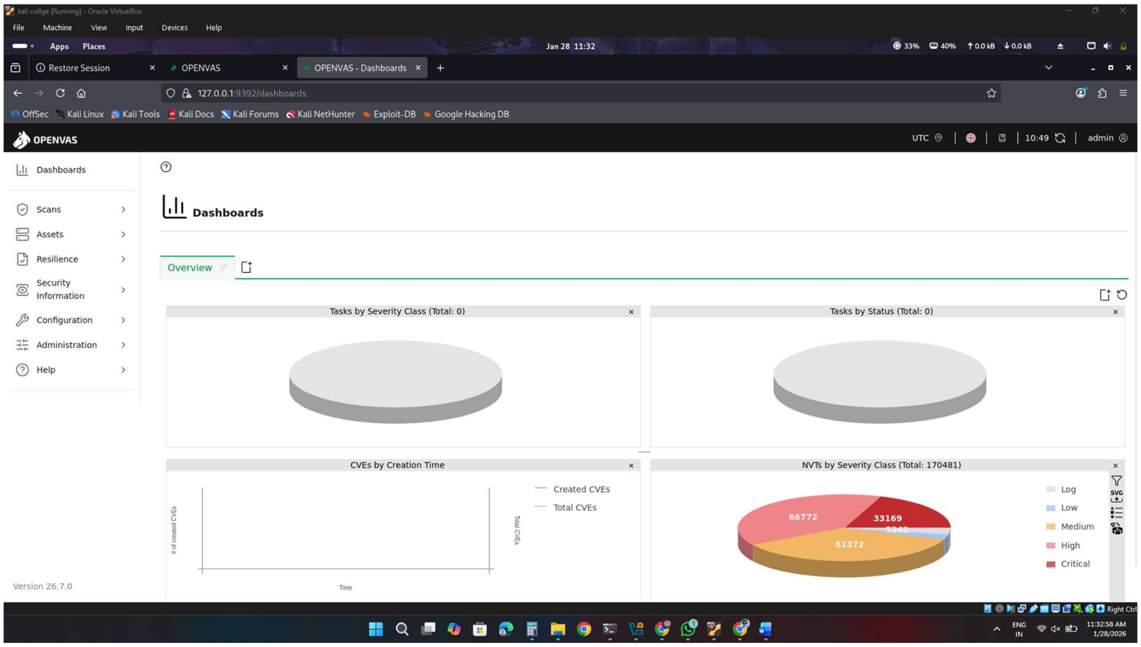
2.2 Vulnerability Scanning using OpenVAS

Objective

To identify known vulnerabilities using an open-source vulnerability scanner.

Tool Used

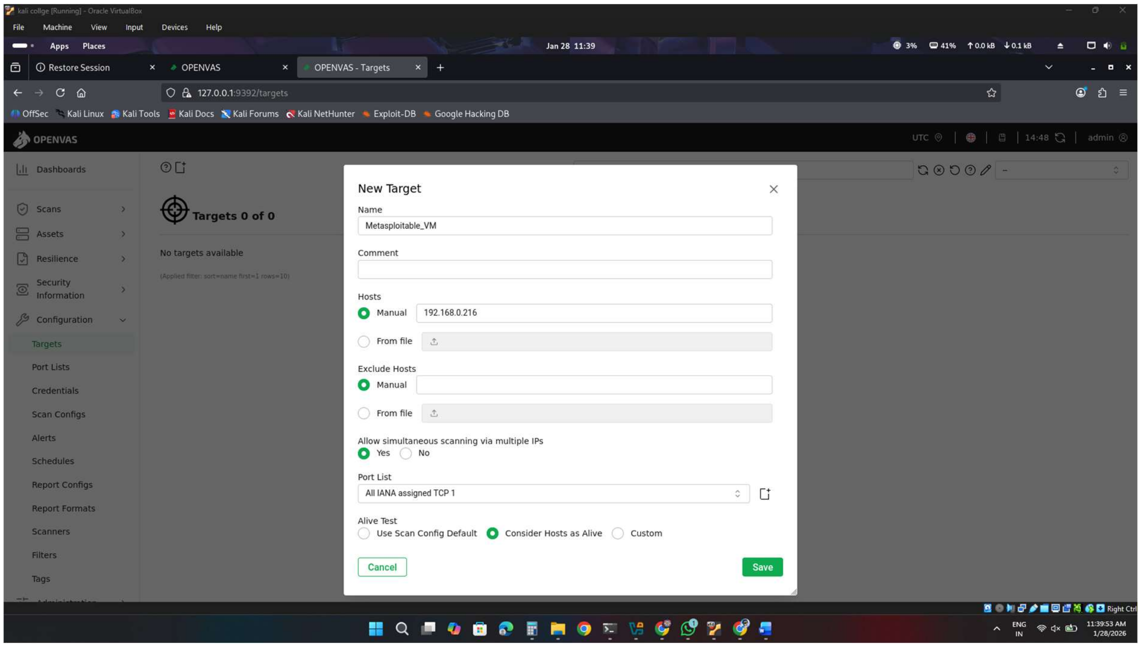
OpenVAS (Greenbone GVM)



2.3 Target Configuration

Objective

To define the target host for vulnerability scanning.



New Target

Name: Metasploitable_VM

Comment:

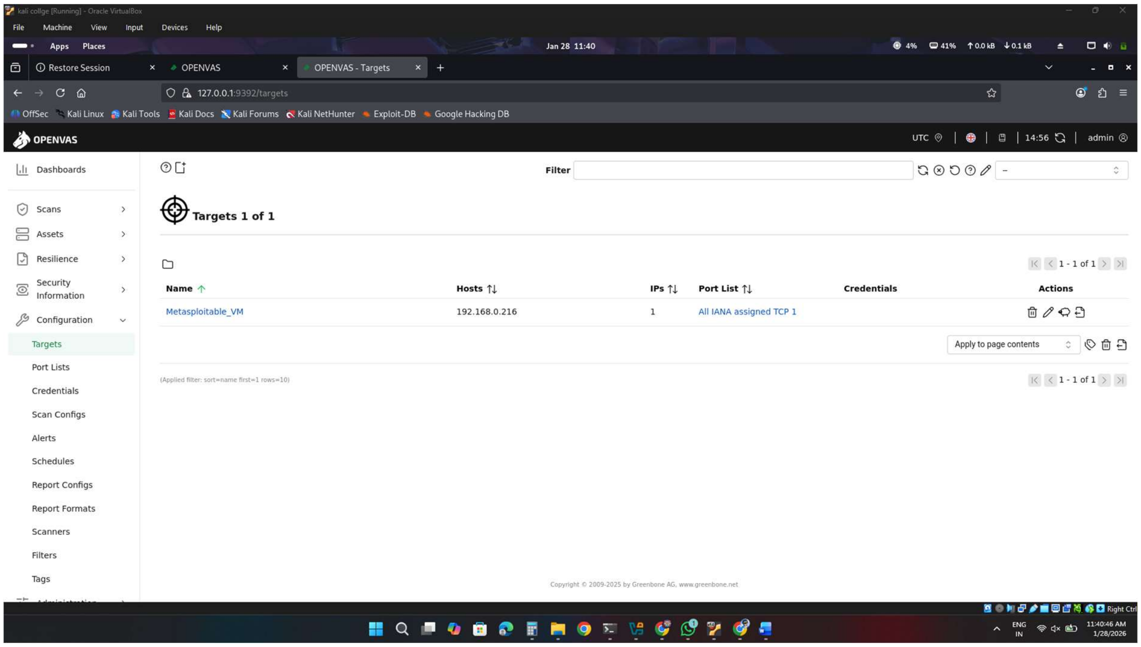
Hosts
● Manual 192.168.0.216
○ From file

Exclude Hosts
● Manual
○ From file

Allow simultaneous scanning via multiple IPs
● Yes ○ No

Port List: All IANA assigned TCP 1

Alive Test
○ Use Scan Config Default ● Consider Hosts as Alive ○ Custom



Targets 1 of 1

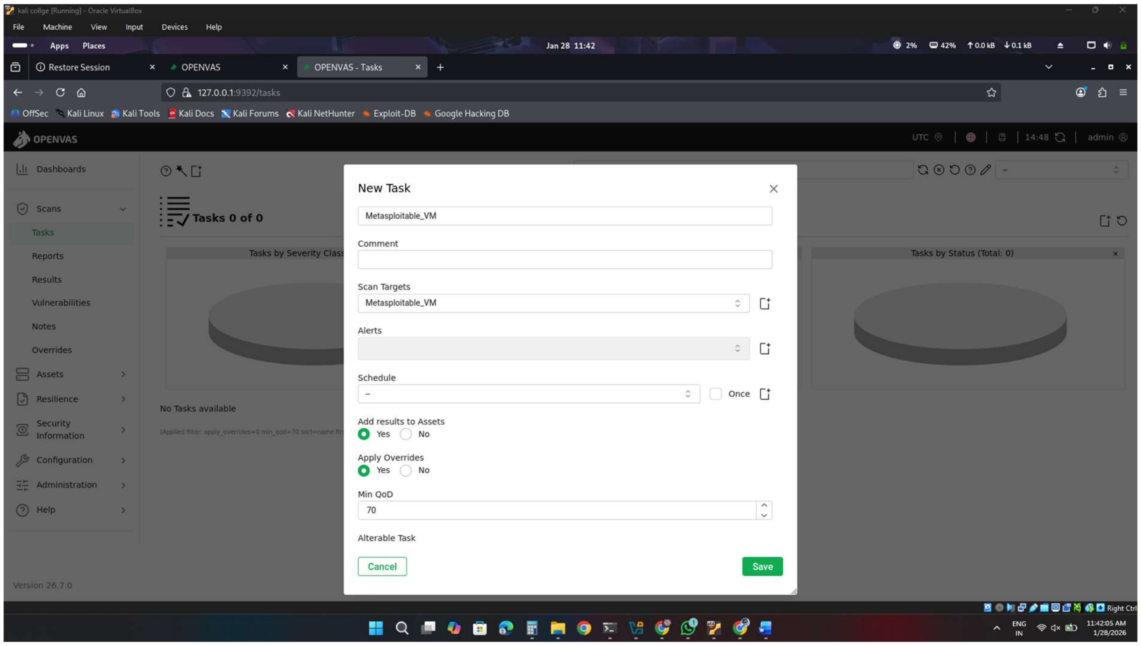
Name	Hosts	IPs	Port List	Credentials	Actions
Metasploitable_VM	192.168.0.216	1	All IANA assigned TCP 1		

(Applied filter: sort=name first=1 rows=10)

2.4 Running Vulnerability Scan

Objective

To execute a vulnerability scan against the configured target.



New Task

Metasploitable_VM

Comment

Scan Targets: Metasploitable_VM

Alerts

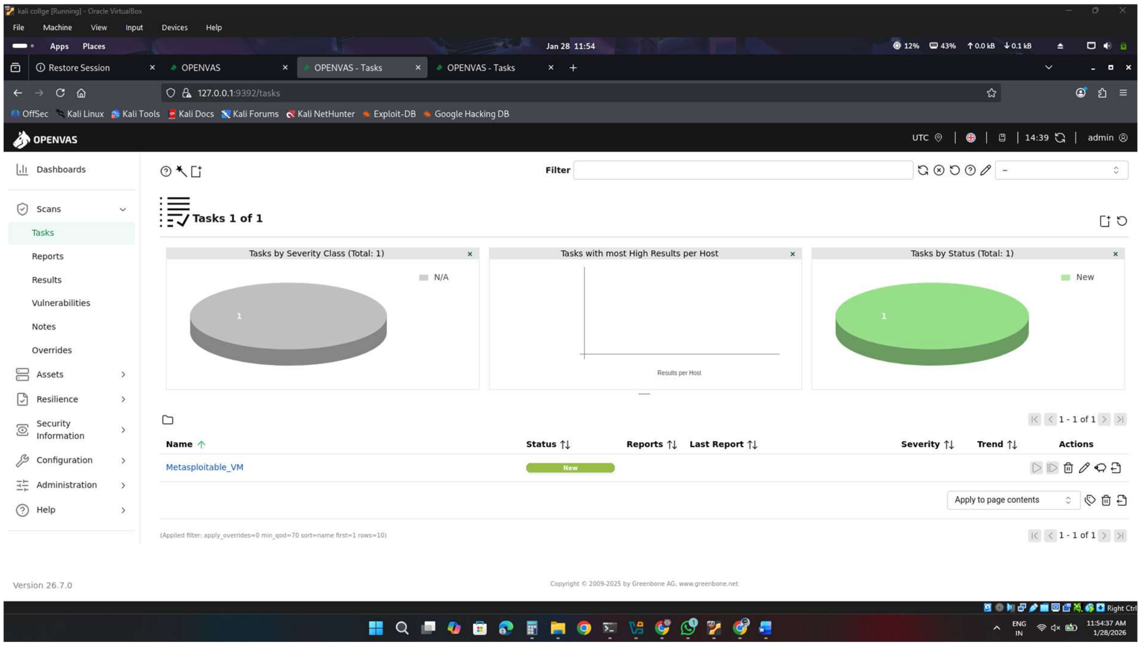
Schedule: -- □ Once

Add results to Assets: ● Yes ○ No

Apply Overrides: ● Yes ○ No

Min QoD: 70

Alterable Task



Name	Status	Reports	Last Report	Severity	Trend	Actions
Metasploitable_VM	New					

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

OpenVAS Scan Attempt

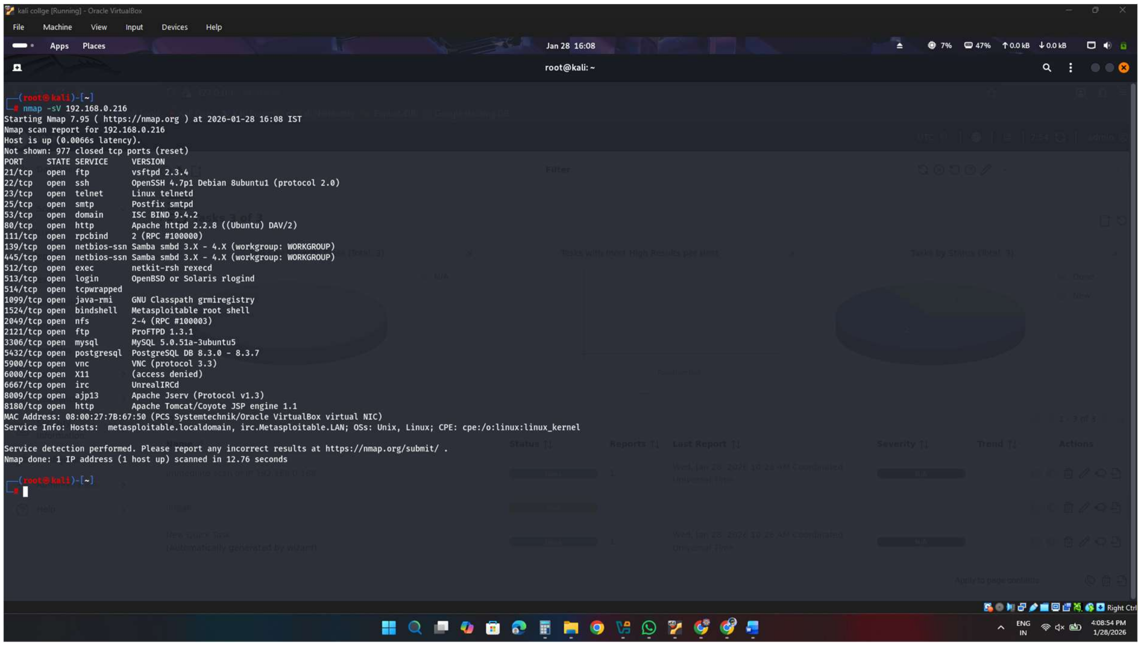
OpenVAS (Greenbone Community Edition) was successfully installed and accessed via the web interface at https://127.0.0.1:9392.

GVM services were started successfully; however, vulnerability scans could not be executed due to repeated service and database synchronization issues in the lab environment, despite multiple attempts.

Justification

Due to time constraints and persistent tool execution errors, further vulnerability assessment was completed using Nmap and manual analysis techniques.

2.3 Network Scanning using Nmap



```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.0.216
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-28 16:08 IST
Nmap scan report for 192.168.0.216
Host is up (0.0066s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7B:67:50 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.76 seconds

┌──(root㉿kali)-[~]
└─# 
```

2.3 Analysis of Nmap Scan Results

Observed Open Ports (Example)

- 21/tcp – FTP (vsftpd 2.3.4)
- 22/tcp – SSH
- 23/tcp – Telnet
- 80/tcp – HTTP (Apache 2.2.8)
- 445/tcp – SMB (Samba 3.x)
- 3306/tcp – MySQL
- 8180/tcp – Apache Tomcat

2.5 Manual Vulnerability Identification

Manual Vulnerability Mapping Table

Port	**Service**	**Sambhavit Vulnerability**
21	FTP	Anonymous login / outdated FTP
23	Telnet	Plain-text communication
80	HTTP	SQL Injection / XSS
445	SMB	SMB misconfiguration
3306	MySQL	Weak database credentials
8180	Tomcat	Default credentials

2.6 Risk Assessment

Vulnerabilities ko classify kiya:

- **High Risk:** FTP, Telnet, SMB, Tomcat
- **Medium Risk:** SSH, MySQL
- **Low Risk:** Informational services

Vulnerability Scan Summary

In this practical task, vulnerability scanning was performed on the target system using the Nmap tool. The main objective of the scan was to identify open ports, running services, and potential security weaknesses. The Nmap scan was executed successfully and revealed multiple exposed services that may pose security risks.

Tools Used

The following free and open-source tools were used to complete this task:

- Kali Linux
- Nmap
- OpenVAS (Greenbone Community Edition – scan attempt)

Nmap Scan Execution

After identifying the target system's IP address, a service version detection scan was performed using Nmap. This scan provided detailed information about open ports and the services running on them, which was later used for vulnerability analysis.

Command used:

```
Nmap -sV 192.168.0.216
```

Observed Open Ports and Services

The Nmap scan results confirmed that multiple high-risk services such as FTP, Telnet, HTTP, and SMB were enabled on the target system. These exposed services increase the attack surface and may allow unauthorized access if not properly secured.

Vulnerability Identification (Manual Analysis)

Based on the Nmap scan results, vulnerabilities were manually identified by analyzing the exposed services and their known security weaknesses.

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	FTP (Outdated / Anonymous Access)	7.5	High	Target IP
002	Telnet Service Enabled	8.0	High	Target IP
003	SMB Misconfiguration	6.5	Medium	Target IP
004	Apache HTTP Outdated Version	6.0	Medium	Target IP

Risk Assessment and Prioritization

The identified vulnerabilities were prioritized based on their severity, exposure, and potential impact. CVSS concepts were applied to classify vulnerabilities into High and Medium risk categories.

Vulnerabilities were prioritized using CVSS concepts based on service exposure, impact, and ease of exploitation.

OpenVAS Scan Attempt

An automated vulnerability scanning attempt was made using OpenVAS (Greenbone Community Edition). The OpenVAS services started successfully and the web interface was accessible. However, due to backend technical and synchronization issues, the vulnerability scan could not be executed successfully.

OpenVAS scan was attempted, but due to technical issues, the scan could not be completed. Therefore, manual vulnerability assessment was perform ed based on Nmap scan results.

Remediation Suggestions

The following remediation steps are recommended to mitigate the identified vulnerabilities:

- Disable unused services such as Telnet
- Restrict access to FTP and SMB services
- Update outdated software and services to the latest versions
- Implement strong authentication mechanisms

Conclusion

In this task, vulnerability scanning was successfully performed using the Nmap tool. Multiple insecure services and potential vulnerabilities were identified on the target system. Although the OpenVAS scan could not be completed due to technical limitations, the scan attempt was properly documented and manual analysis was used to perform risk assessment and prioritization.