

Task 2: Network Security & Scanning Report

Cybersecurity & Ethical Hacking Internship

Company: ApexPlanet Software Pvt. Ltd.

Task Duration: Days 13–24

Task Name: Network Scanning, Vulnerability Assessment & Traffic Analysis

1. Objective:

The objective of this task is to perform network reconnaissance, port scanning, service enumeration, vulnerability assessment, and network traffic analysis using professional cybersecurity tools. This task demonstrates the process of identifying active hosts, detecting open ports, identifying vulnerabilities, and analysing packet-level network communication in a controlled lab environment.

2. Lab Environment Setup:

The lab environment was created using virtualization technology to simulate a real-world attack and target environment.

Attacker Machine: Kali Linux.

Toolset: Nmap, Nessus Essentials, Wireshark.

Target Machine: Metasploitable2 and DVWA vulnerable system.

Virtualization Platform: Oracle VirtualBox.

Network Configuration: Host-Only Adapter Network, Ensures isolated and secure testing environment.

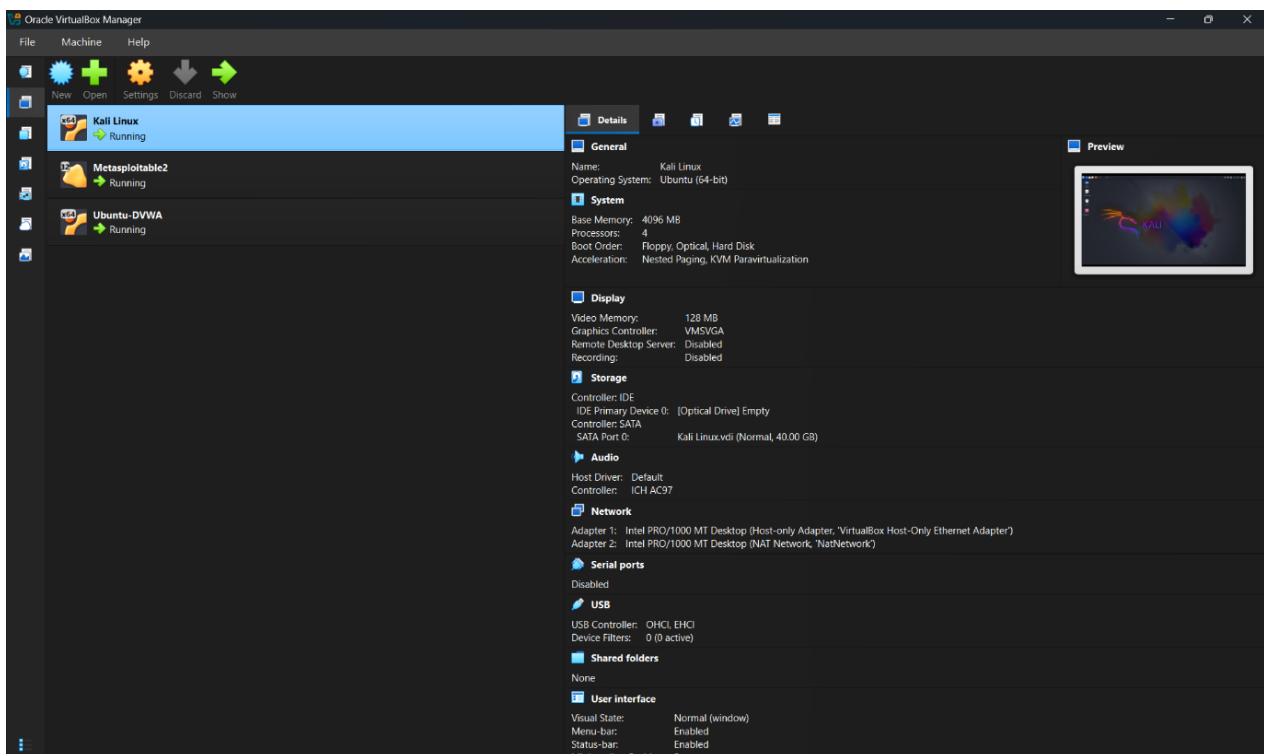


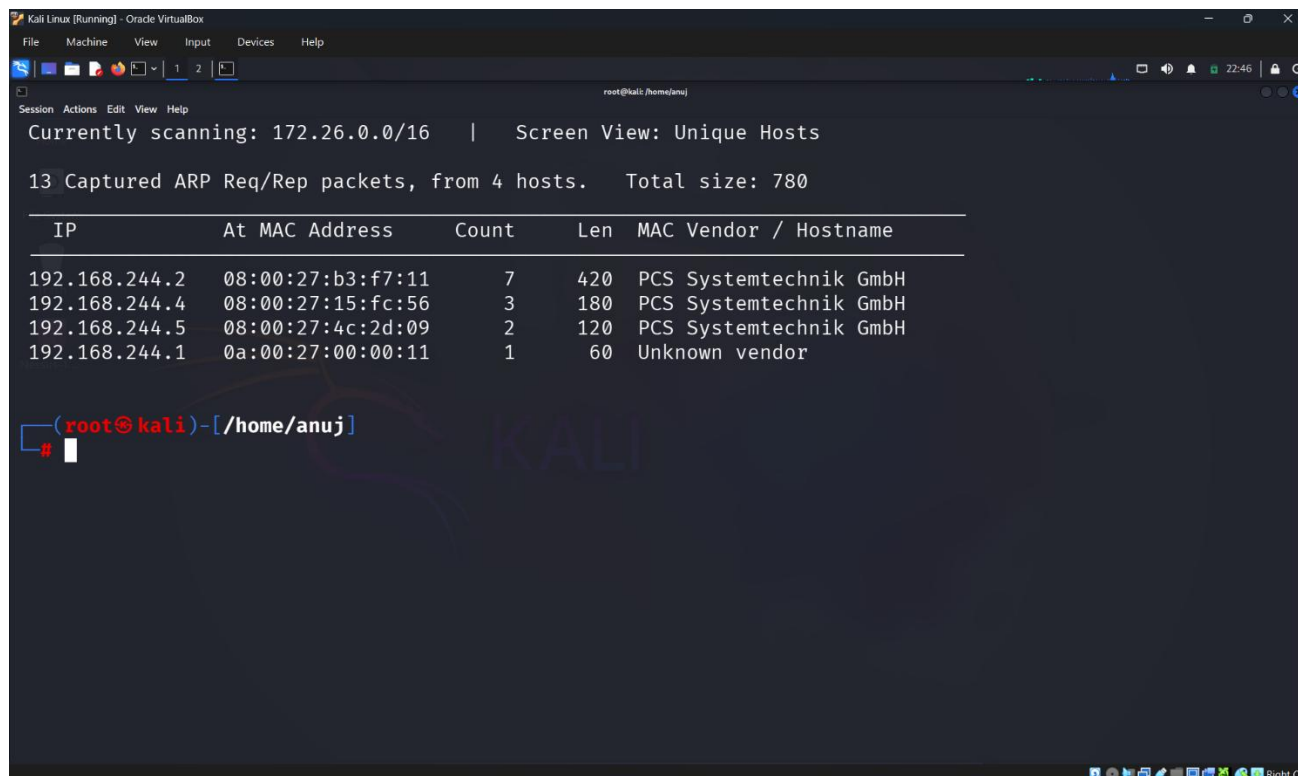
Figure 1: Virtual Lab Environment Setup in VirtualBox

3. Network Reconnaissance:

Network reconnaissance was performed to identify active hosts in the network.

Tool used: netdiscover

This tool scans the network and displays all active devices along with their IP addresses and MAC addresses.



```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@kali:/home/anuj

Currently scanning: 172.26.0.0/16 | Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 4 hosts. Total size: 780

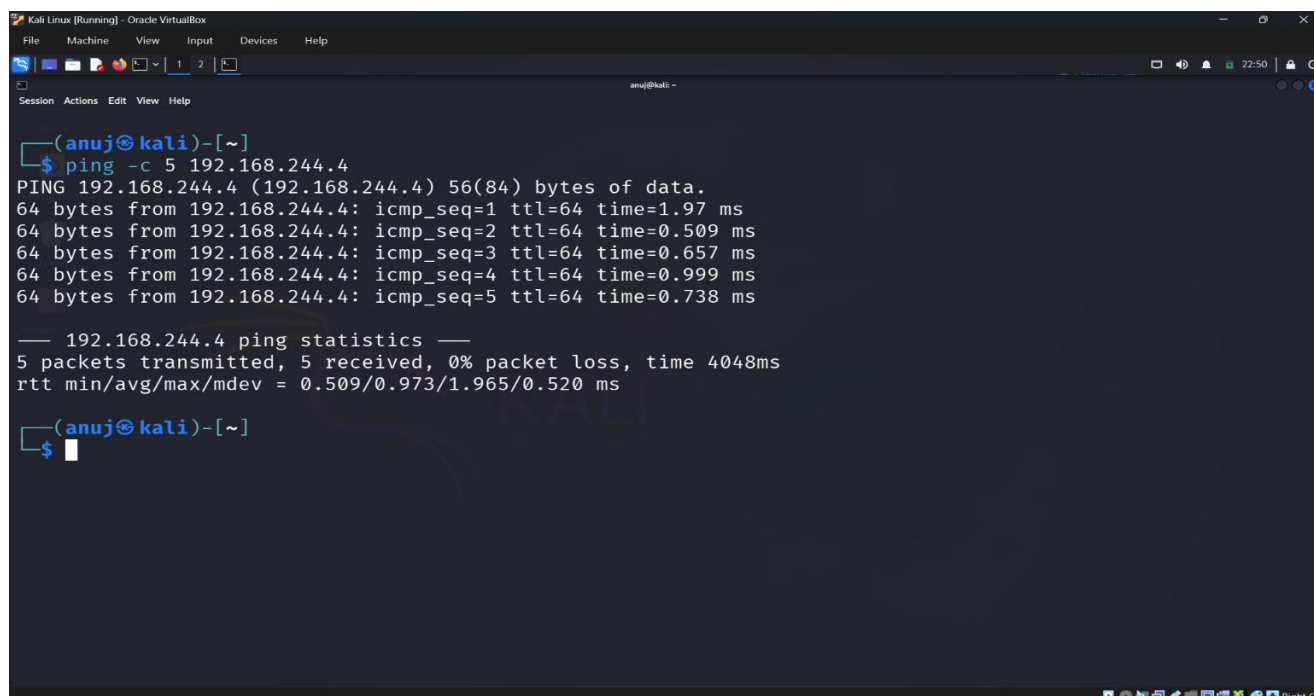
+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.244.2 | 08:00:27:b3:f7:11 | 7     | 420 | PCS Systemtechnik GmbH |
| 192.168.244.4 | 08:00:27:15:fc:56 | 3     | 180 | PCS Systemtechnik GmbH |
| 192.168.244.5 | 08:00:27:4c:2d:09 | 2     | 120 | PCS Systemtechnik GmbH |
| 192.168.244.1 | 0a:00:27:00:00:11 | 1     | 60  | Unknown vendor         |
+-----+-----+-----+-----+-----+

(anuj@kali)-[/home/anuj]
#
```

Figure 2: Network reconnaissance using netdiscover

4. Connectivity Verification:

Connectivity between the attacker and target system was verified using ICMP ping. Successful ping replies confirmed network communication between systems.



```
Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help

anuj@kali: ~

(anuj@kali)-[~]
$ ping -c 5 192.168.244.4
PING 192.168.244.4 (192.168.244.4) 56(84) bytes of data.
64 bytes from 192.168.244.4: icmp_seq=1 ttl=64 time=1.97 ms
64 bytes from 192.168.244.4: icmp_seq=2 ttl=64 time=0.509 ms
64 bytes from 192.168.244.4: icmp_seq=3 ttl=64 time=0.657 ms
64 bytes from 192.168.244.4: icmp_seq=4 ttl=64 time=0.999 ms
64 bytes from 192.168.244.4: icmp_seq=5 ttl=64 time=0.738 ms

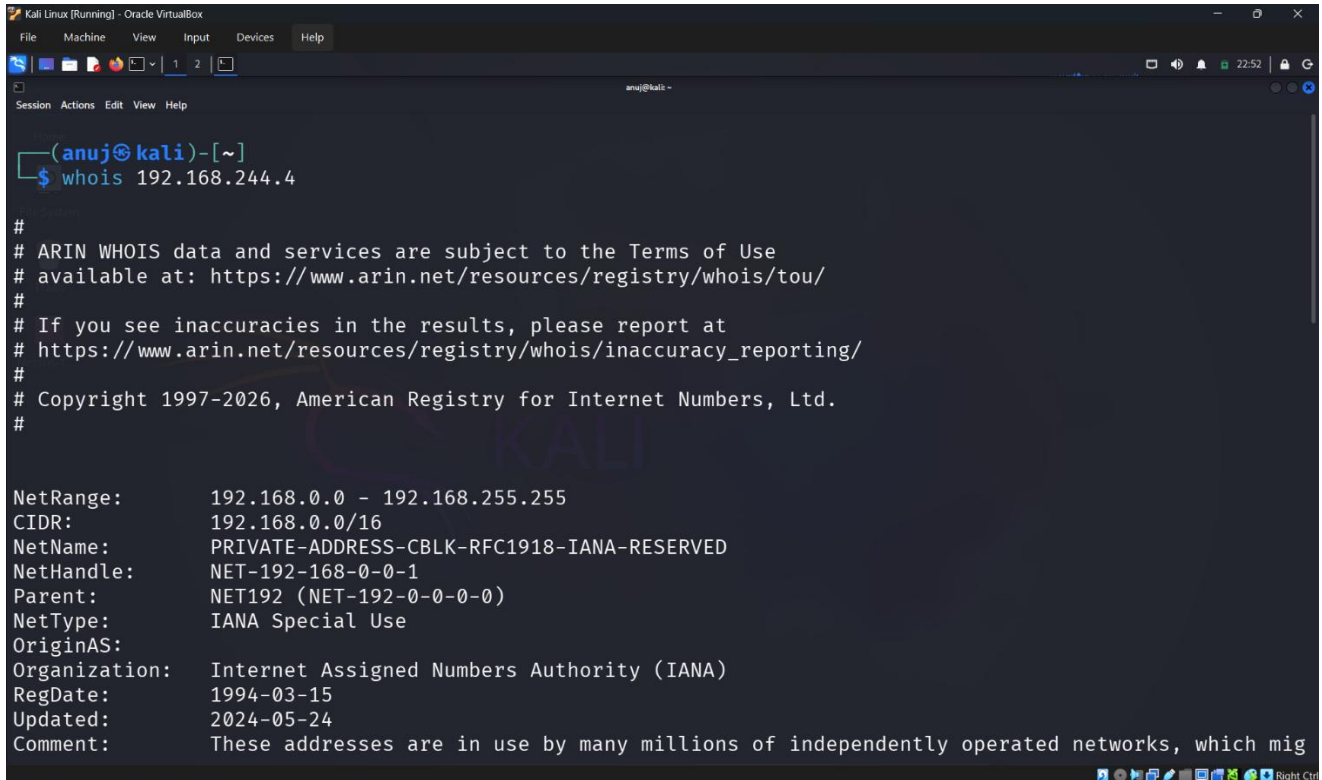
— 192.168.244.4 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4048ms
rtt min/avg/max/mdev = 0.509/0.973/1.965/0.520 ms

(anuj@kali)-[~]
$
```

Figure 3: Connectivity verification using ICMP ping

5. Information Gathering using “WHOIS”:

WHOIS lookup was performed to gather additional information about the target system. This provides ownership and registration information when available.



```
(anuj@kali)-[~]
$ whois 192.168.244.4

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2026, American Registry for Internet Numbers, Ltd.
#

NetRange:      192.168.0.0 - 192.168.255.255
CIDR:          192.168.0.0/16
NetName:       PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:     NET-192-168-0-0-1
Parent:        NET192 (NET-192-0-0-0-0)
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:       1994-03-15
Updated:       2024-05-24
Comment:       These addresses are in use by many millions of independently operated networks, which mig
```

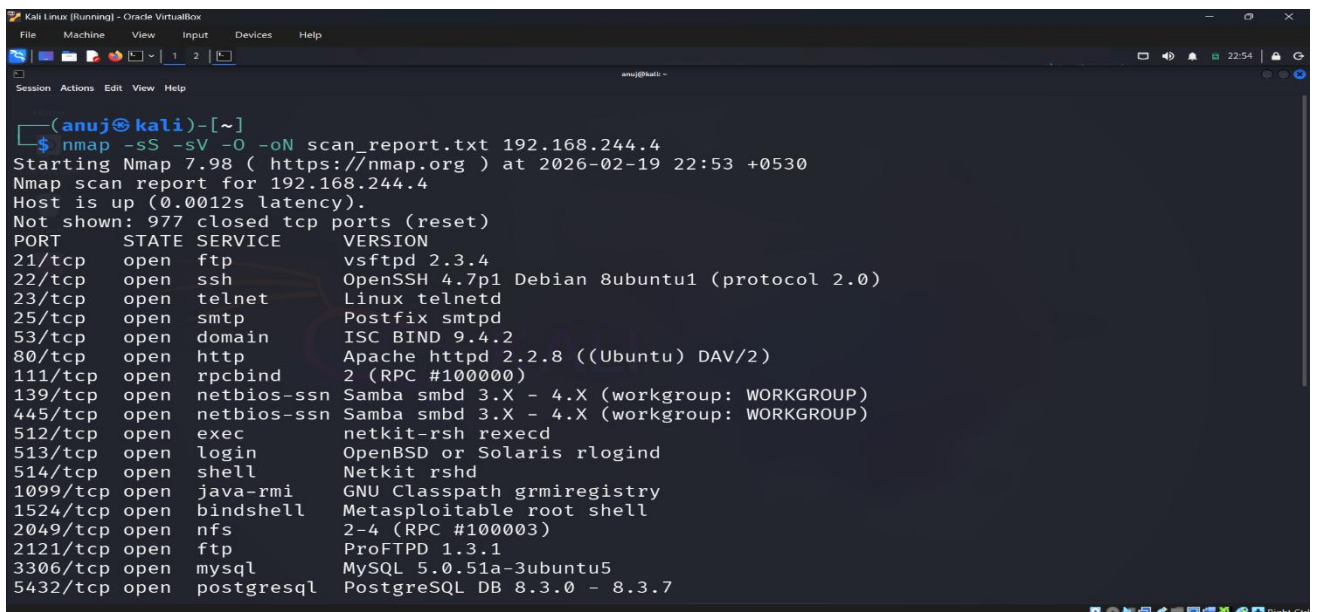
Figure 4: WHOIS information gathering

6. Network Scanning using Nmap:

Nmap was used to identify open ports, running services, and operating system information.

This scan performs:

- SYN scan for open ports (-sS).
- Service version detection (-sV).
- Operating system detection(-O).



```
(anuj@kali)-[~]
$ nmap -sS -sV -O -oN scan_report.txt 192.168.244.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-19 22:53 +0530
Nmap scan report for 192.168.244.4
Host is up (0.0012s 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 rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
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
```

Figure 5: Nmap scan showing open ports and services

7. Vulnerability Assessment using Nessus Essentials:

Vulnerability scanning was performed using Nessus Essentials, developed by Tenable. Nessus identifies vulnerabilities, misconfigurations, and security risks in the target system.

Steps performed:

- Configured target IP.
- Launched vulnerability scan.
- Analysed vulnerability results.

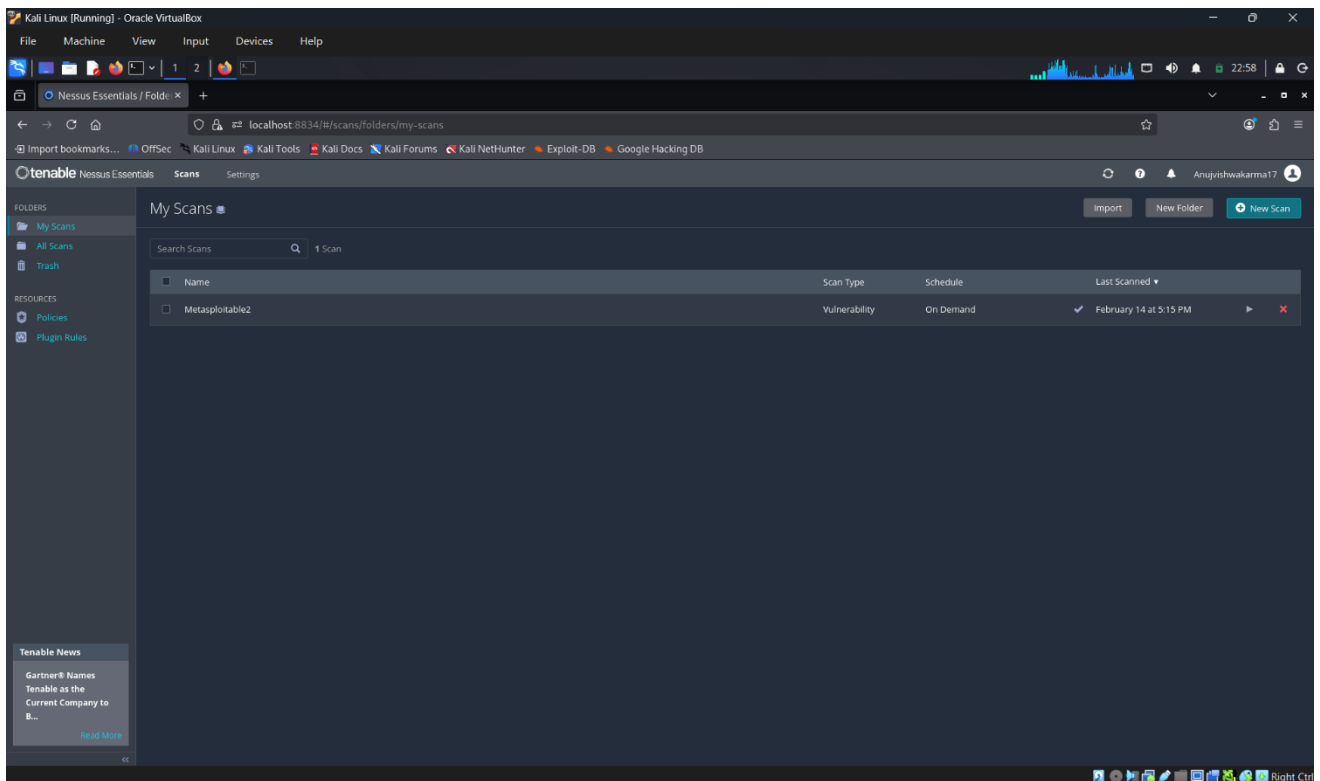


Figure 6: Nessus vulnerability scanner dashboard

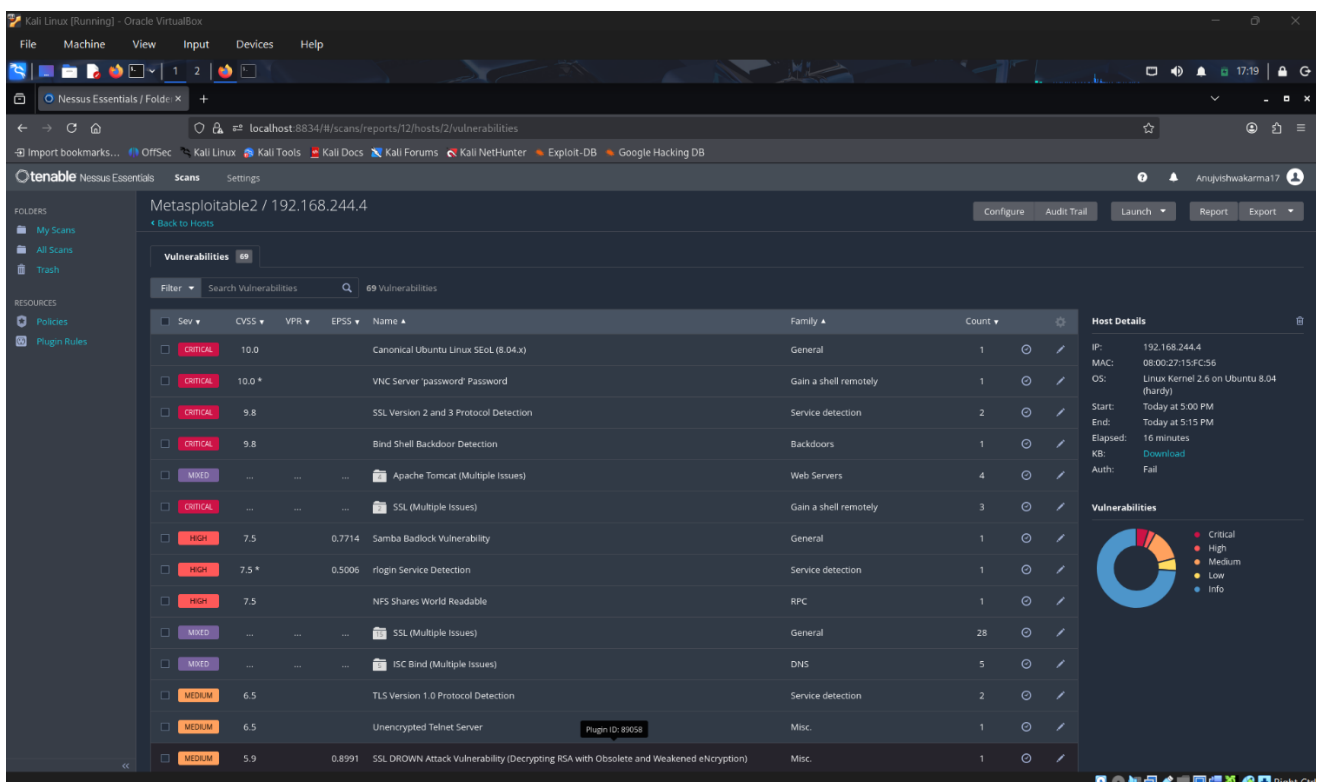


Figure 7: Vulnerability scan results

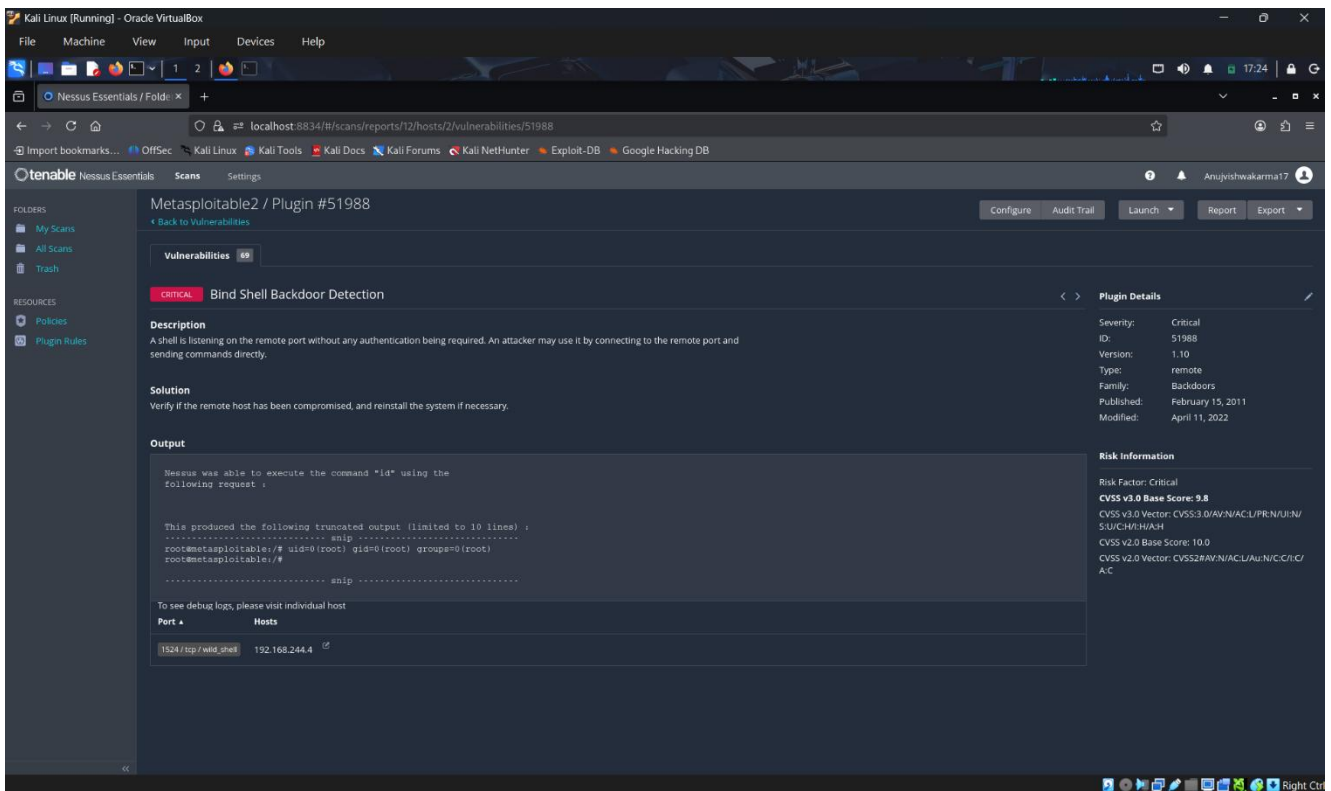


Figure 8: Critical vulnerability detected in target system

8. Network Traffic Analysis using Wireshark:

Wireshark was used to capture and analyse network traffic between attacker and target.

Steps performed:

- Started packet capture on eth0 interface.
- Accessed DVWA login page.
- Captured HTTP traffic.
- Applied HTTP filter.

This allowed analysis of login.php HTTP request packets.

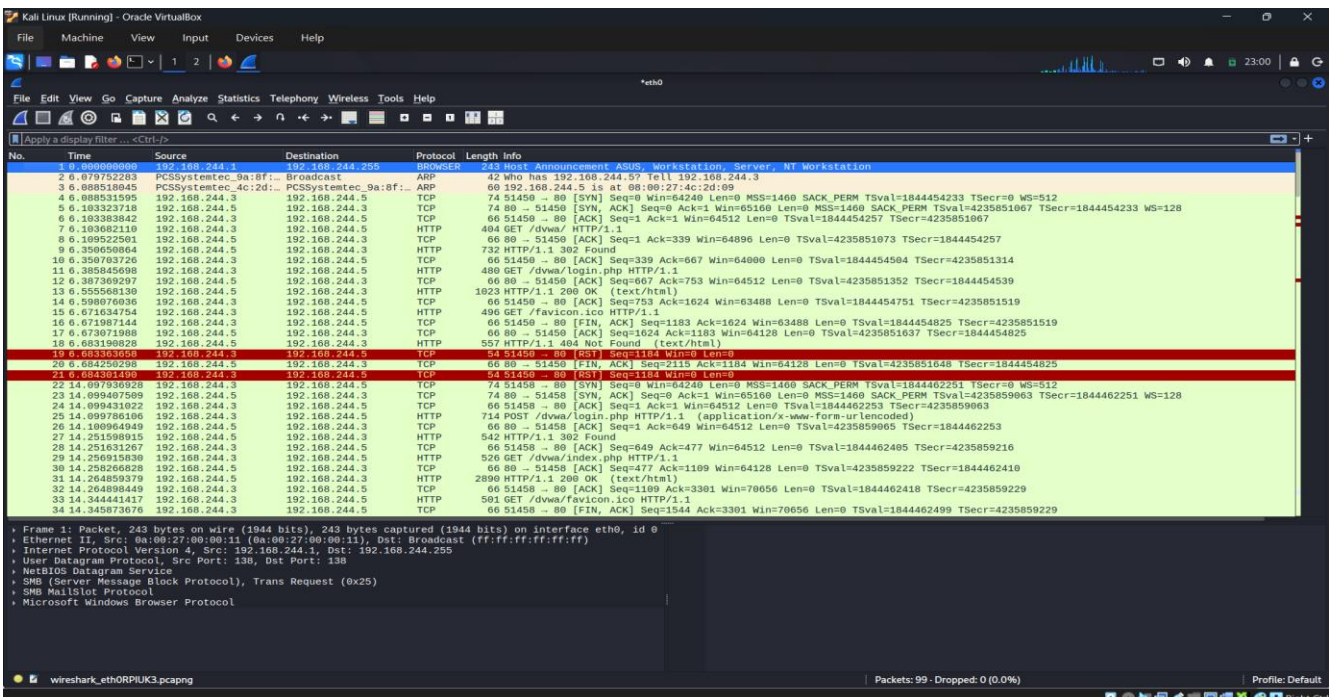


Figure 9: Wireshark capturing network traffic

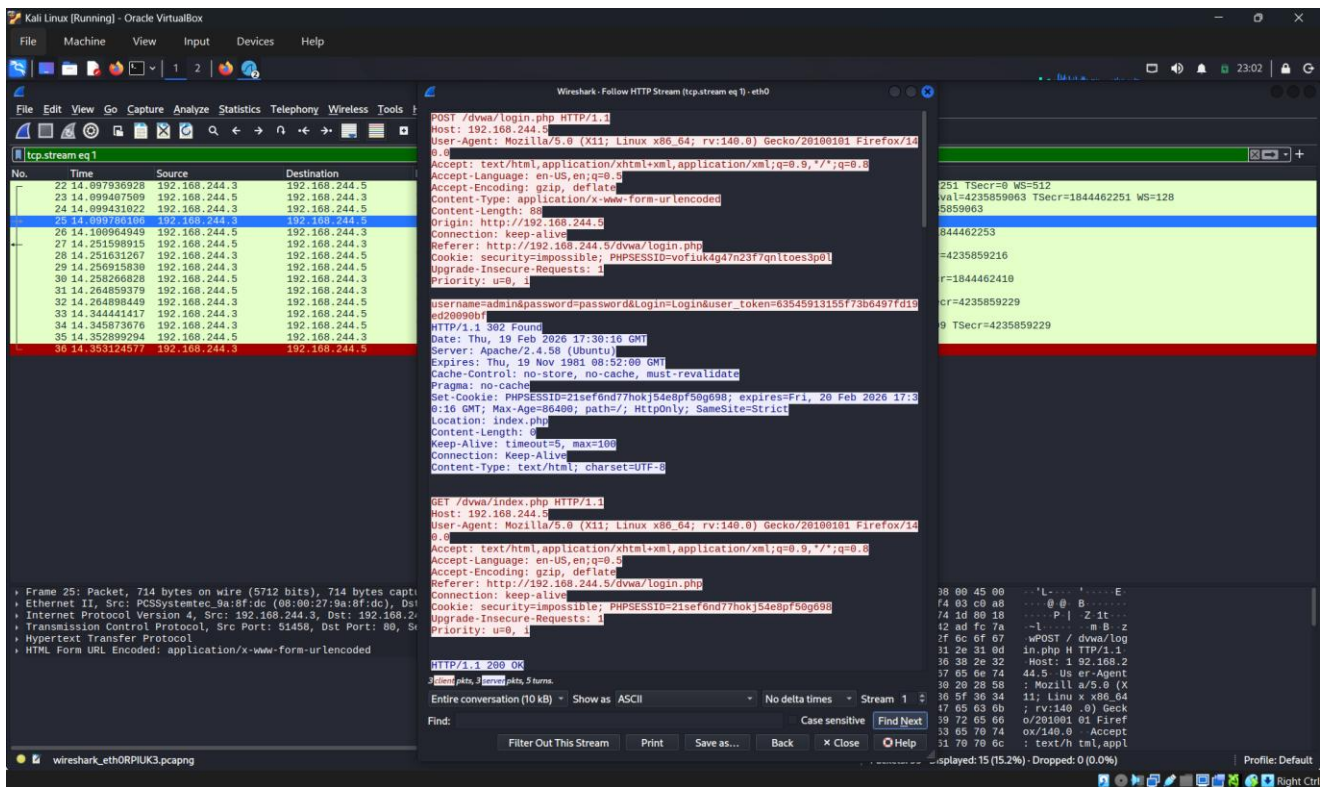


Figure 10: HTTP packet analysis showing DVWA login request

9. Key Findings:

The following findings were observed:

- Multiple open ports were detected.
- Outdated and vulnerable services were identified.
- Critical vulnerability including backdoor service was detected.
- HTTP traffic was successfully captured and analysed.
- Plain text communication was observed in HTTP packets.

10. Conclusion:

This task successfully demonstrated the process of network reconnaissance, port scanning, vulnerability assessment, and packet analysis using professional cybersecurity tools.

The use of Nmap enabled identification of open ports and services. Nessus Essentials identified critical vulnerabilities in the target system. Wireshark provided detailed packet-level traffic analysis.

This task enhanced practical knowledge of cybersecurity assessment techniques and provided hands-on experience in identifying and analysing network security vulnerabilities.

-----X-----X-----X-----