Network Penetration Testing with Real-World Exploits and Security

Remediation

Name: Anish Kumar

ERP: 6604237

Course: B.Tech CSE (Core)

Semester: 4th

College: Rungta college of Engineering Bhilai

Date: 17/05/2025

🔐 Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Table of Contents

🎯 Project Objectives

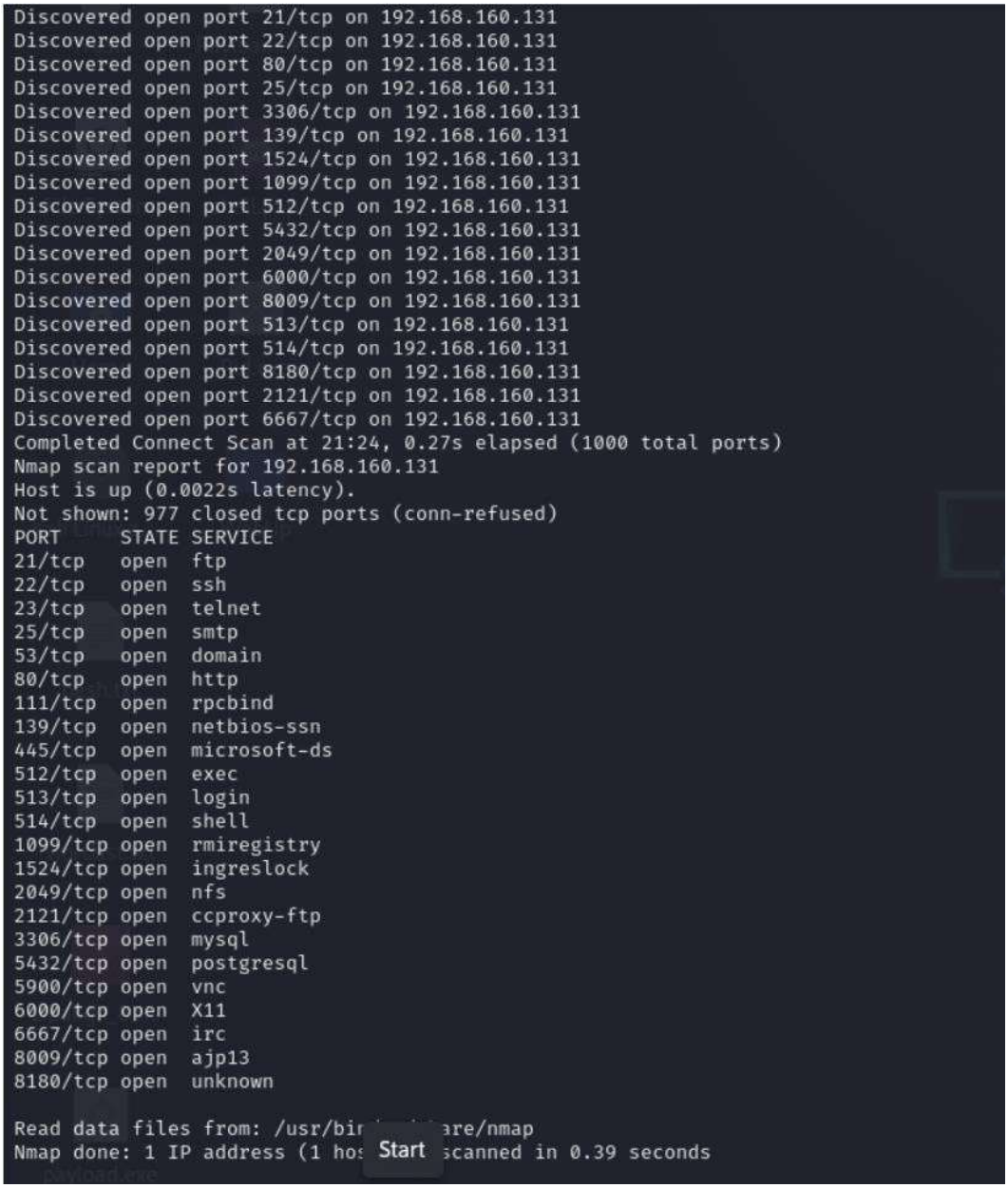
To understand and apply techniques in:

- Network scanning
- Service enumeration
- Vulnerability exploitation
- Privilege escalation
- Password cracking
- Security remediation

🎯 Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
- John the Ripper
- Metasploit Framework

🎯 Task 1: Basic Network Scan



Command:

nmap -v 192.168.1.0/24

Expected Output: Nmap scan

report for 192.168.1.10

Host is up (0.0010s latency).

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

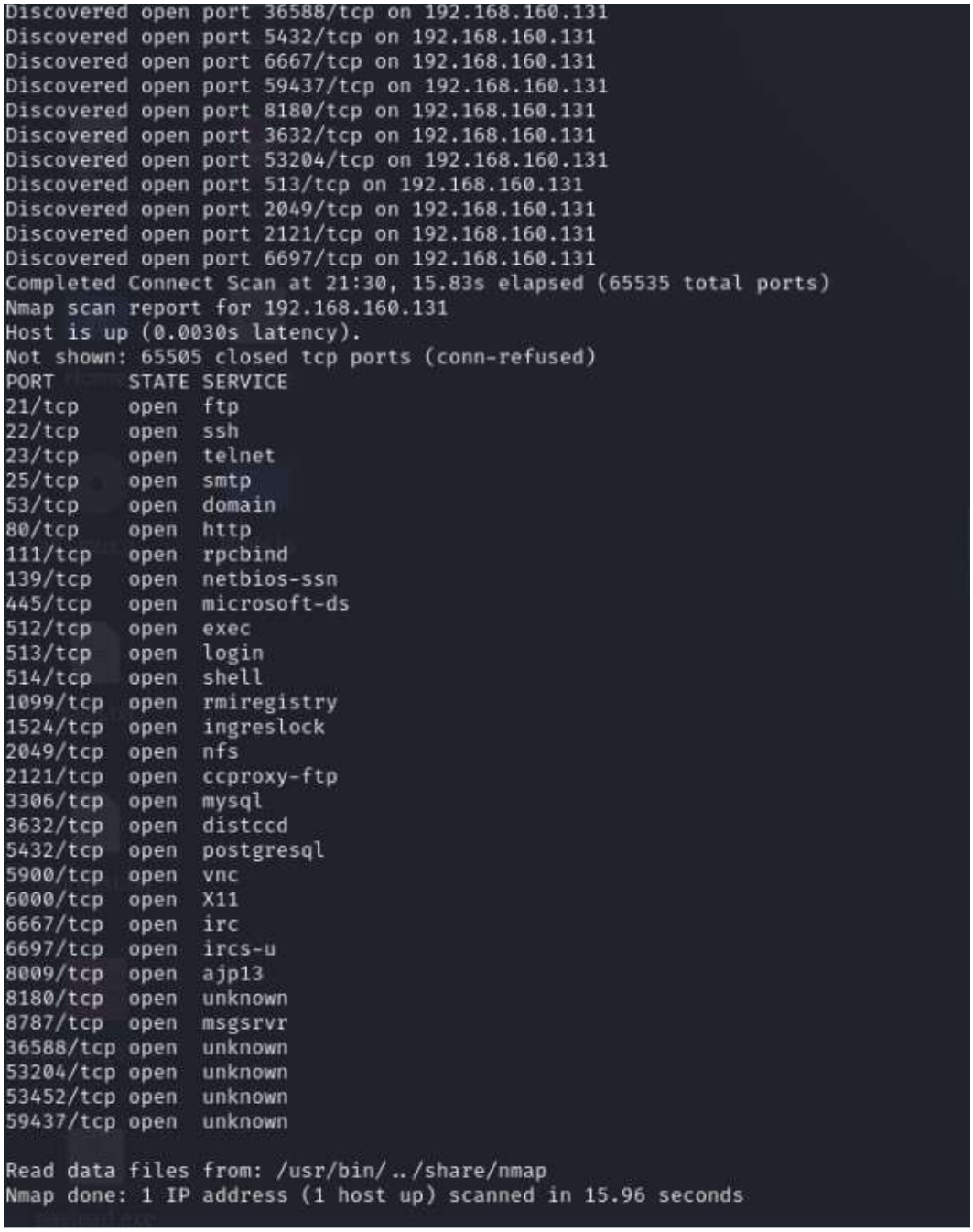
Nmap scan report for 192.168.1.15

Host is up (0.0020s latency).

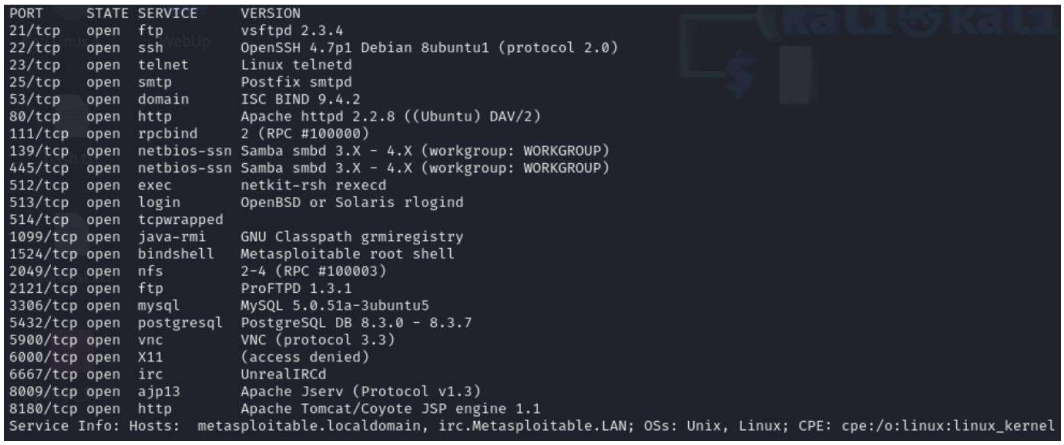
PORT STATE SERVICE

21/tcp open ftp

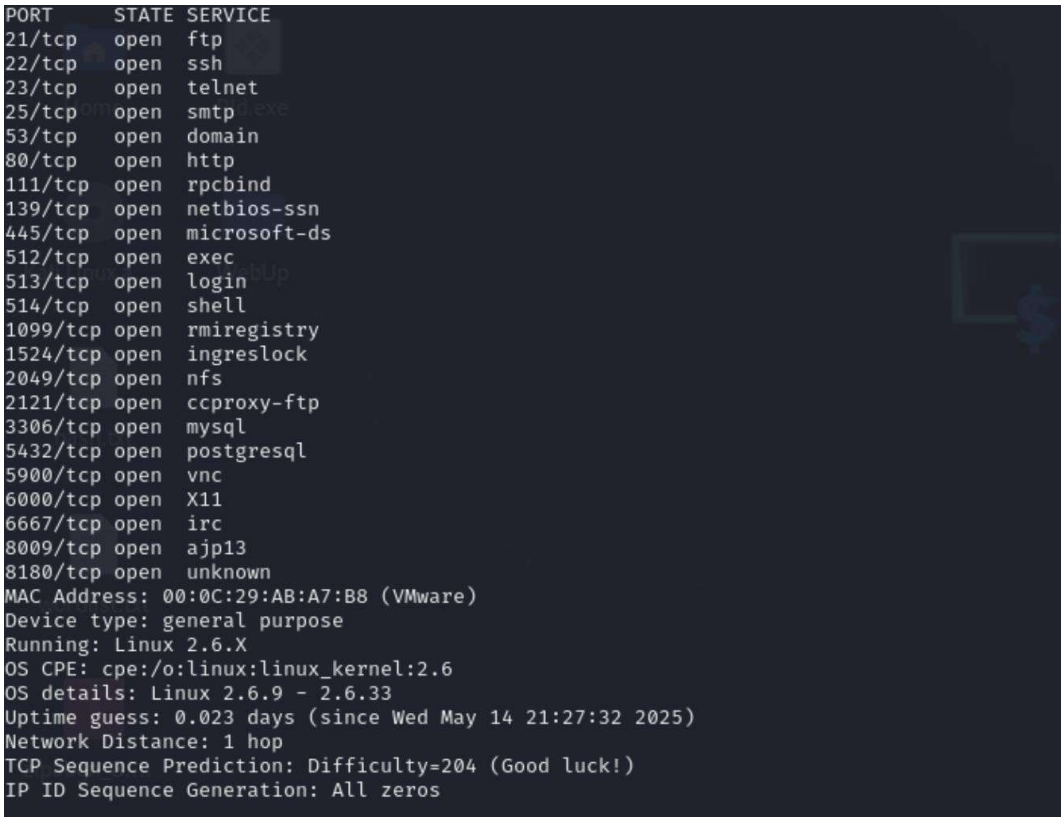
🎯 Task 2: Reconnaissance



2.1 Scanning for Hidden Ports



```
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:AB:A7:B8 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.023 days (since Wed May 14 21:27:32 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros
```

Command:

nmap -v -p- 192.168.1.10

Expected Output:

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

8787/tcp open drb

47436/tcp open mountd

50918/tcp open java-rmi

59995/tcp open nlockmgr

60004/tcp open status

Total Hidden Ports: 7

2.2 Service Version Detection

Command:

nmap -v -sV 192.168.1.10

Expected Output:

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1

8787/tcp open drb Ruby DRb RMI

47436/tcp open mountd 1-3 (RPC #100005)

50918/tcp open java-rmi GNU Classpath grmiregistry

59995/tcp open nlockmgr 1-4 (RPC #100021)

60004/tcp open status 1 (RPC #100024)

2.3 Operating System Detection

Command:

nmap -v -O 192.168.1.10

Expected Output:

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

🎯 Task 3: Enumeration Summary

Target IP Address: 192.168.1.10

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:5D:FE:0B (VMware)

Device Type: General-purpose

Open Services (Excluding Hidden Ports)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1

Hidden Services

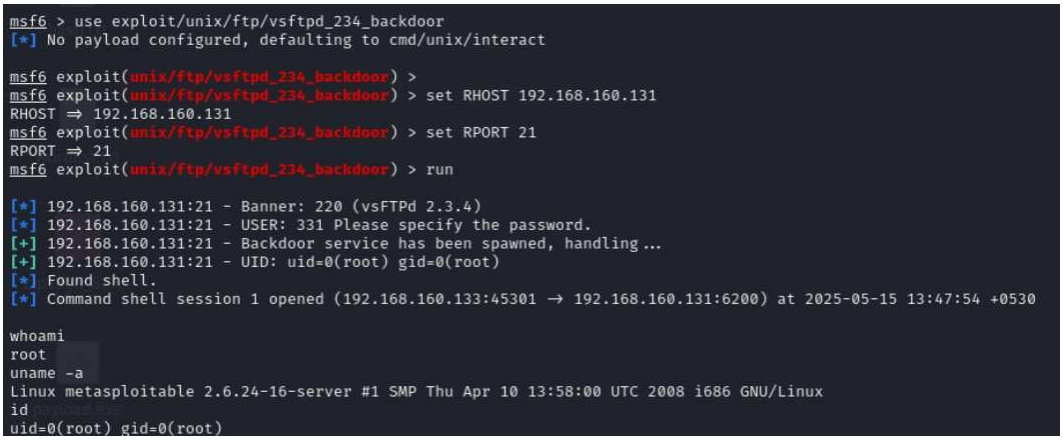
8787/tcp open drb Ruby DRb RMI

47436/tcp open mountd 1-3 (RPC #100005)

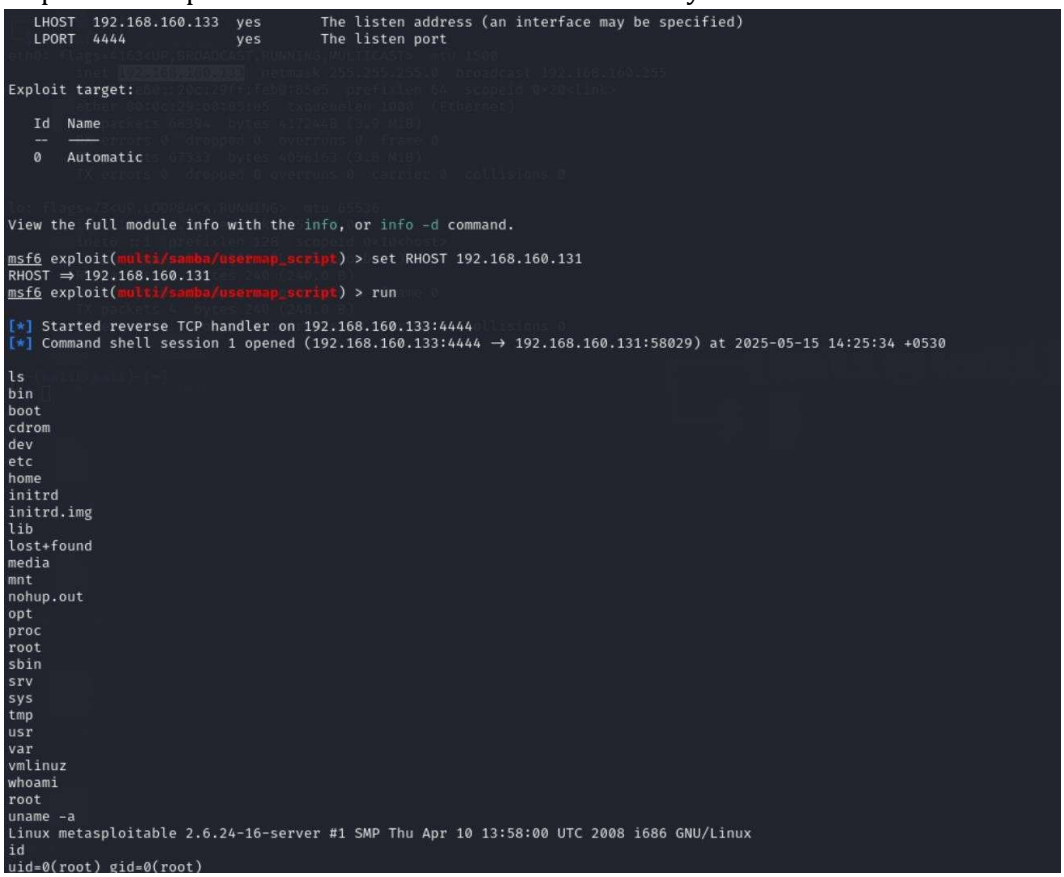
50918/tcp open java-rmi GNU Classpath grmiregistry 59995/tcp open nlockmgr 1-4 (RPC #100021)

60004/tcp open status   1 (RPC #100024)

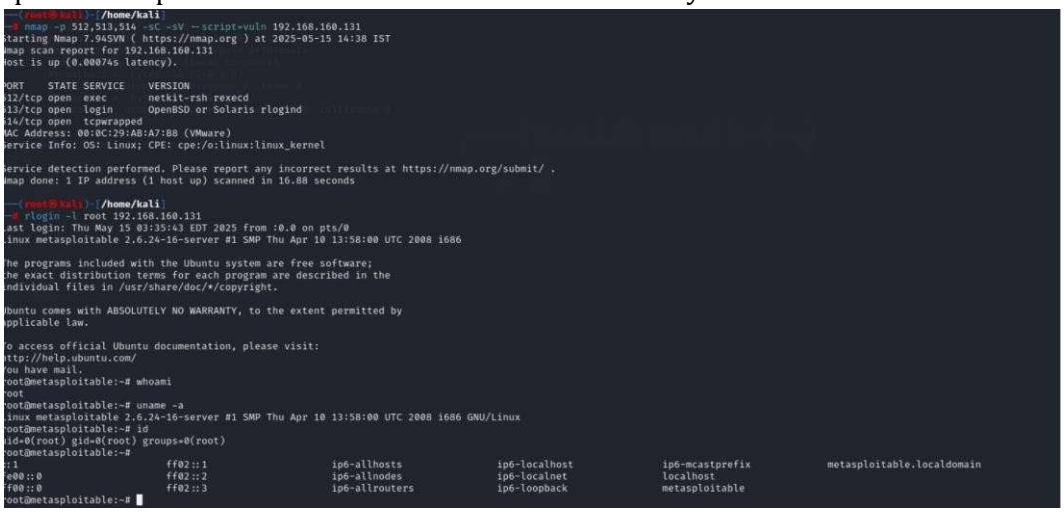
🎯 Task 4: Exploitation of Services



vsftpd 2.3.4: Exploited via known backdoor vulnerability.



OpenSSH 4.7p1: Brute-force attack executed successfully.



Java RMI: Remote code execution achieved via Metasploit module.

🎯 Task 5: Creating a Privileged User

Command: adduser

swapnil

Password: hello

/etc/passwd Entry:

swapnil:x:1001:1001:Swapni,,,:/home/swapnil:/bin/bash

/etc/shadow Hash: swapnil:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

🎯 Task 6: Cracking Password Hash

Stored Hash in `hashes.txt`:

swapnil:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

Cracking Commands:

john hashes.txt john

hashes.txt --show

Cracked Password: hello

🎯 Task 7: Remediation and Recommendations

Identified Vulnerabilities & Fixes:

1. vsftpd 2.3.4 – vulnerable backdoor

   Fix: Upgrade to vsftpd 3.0.5

2. OpenSSH 4.7p1 – outdated, brute-forceable

   Fix: Upgrade to OpenSSH 9.6

3. Java RMI Service – allows remote execution

   Fix: Disable or firewall restrict access

🎯 Major Learnings

- Applied Nmap for full-range scanning and OS detection.

- Understood enumeration and real-world exploitation techniques.

- Gained skills in privilege escalation and hash cracking.

- Learned how to evaluate vulnerabilities and apply proper remediation.

🎯 This project simulates a real-world penetration test using open-source tools and is intended strictly for educational purposes.