□ Introduction

This project demonstrates a practical system hacking scenario in a controlled lab environment using **Kali Linux** (attacker) and **Metasploitable2** (target). The exercise focuses on exploiting a common vulnerability — **Telnet service misconfiguration** — to gain unauthorized root access using default credentials.

This project aligns with key stages of the **Cyber Kill Chain**, including Reconnaissance, Exploitation, Privilege Escalation, and Post-Exploitation, and concludes with security **mitigation strategies**.

□ Tools & Environment

- **Attacker Machine**: Kali Linux (2024.1)
- **Target Machine**: Metasploitable2
- **Target IP**: 172.20.10.5
- **Tools Used**:
    - nmap (for scanning)
    - telnet (for direct access)

□ Step 1: Reconnaissance

Cyber Kill Chain Stage: Reconnaissance

✓Objective:

Identify if the Telnet port (23) is open on the target.

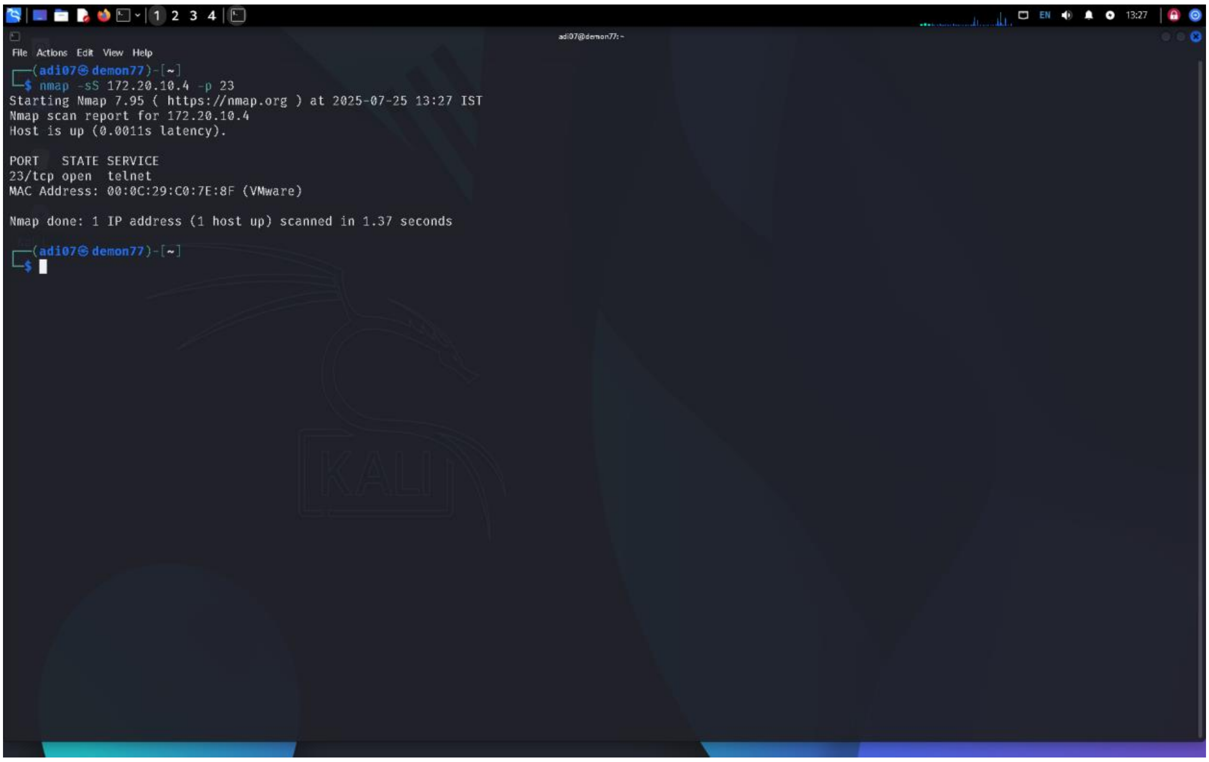
□ Command Used:

Bash
CopyEdit

```
nmap -p 23 -sV 172.20.10.5
```

□ Output:

arduino
CopyEdit
23/tcp open telnet Linux telnetd



```
┌──(adi07㉿demon77)-[~]
└─$ nmap -sS 172.20.10.4 -p 23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-25 13:27 IST
Nmap scan report for 172.20.10.4
Host is up (0.0011s latency).

PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0C:29:C0:7E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds

┌──(adi07㉿demon77)-[~]
└─$ 
```

□ Observation:

The result confirms that **Telnet is open** and active on the target, and the system is running a **Linux telnetd** service, which can be exploited.

□ Step 2: Exploitation

Cyber Kill Chain Stage: Exploitation

✓Objective:

Exploit the exposed Telnet service to gain shell access.

□ Command Used:

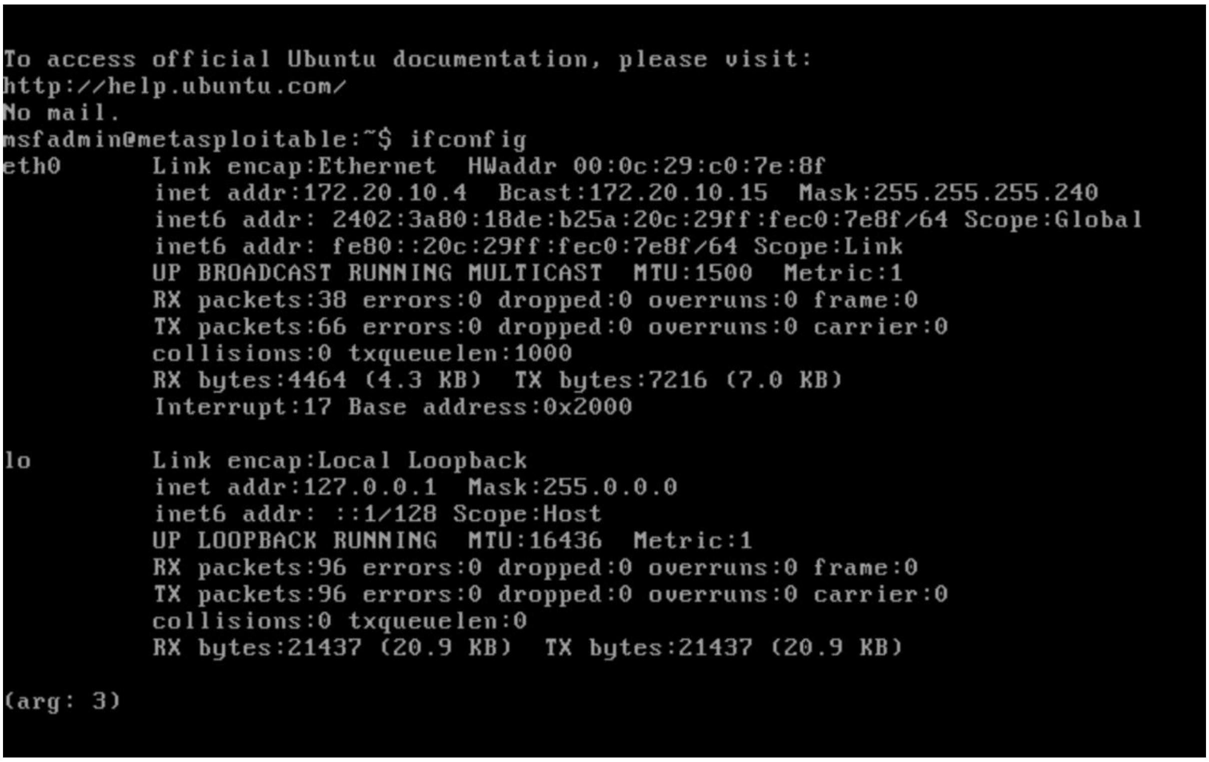
bash
CopyEdit

```
telnet 172.20.10.5
```

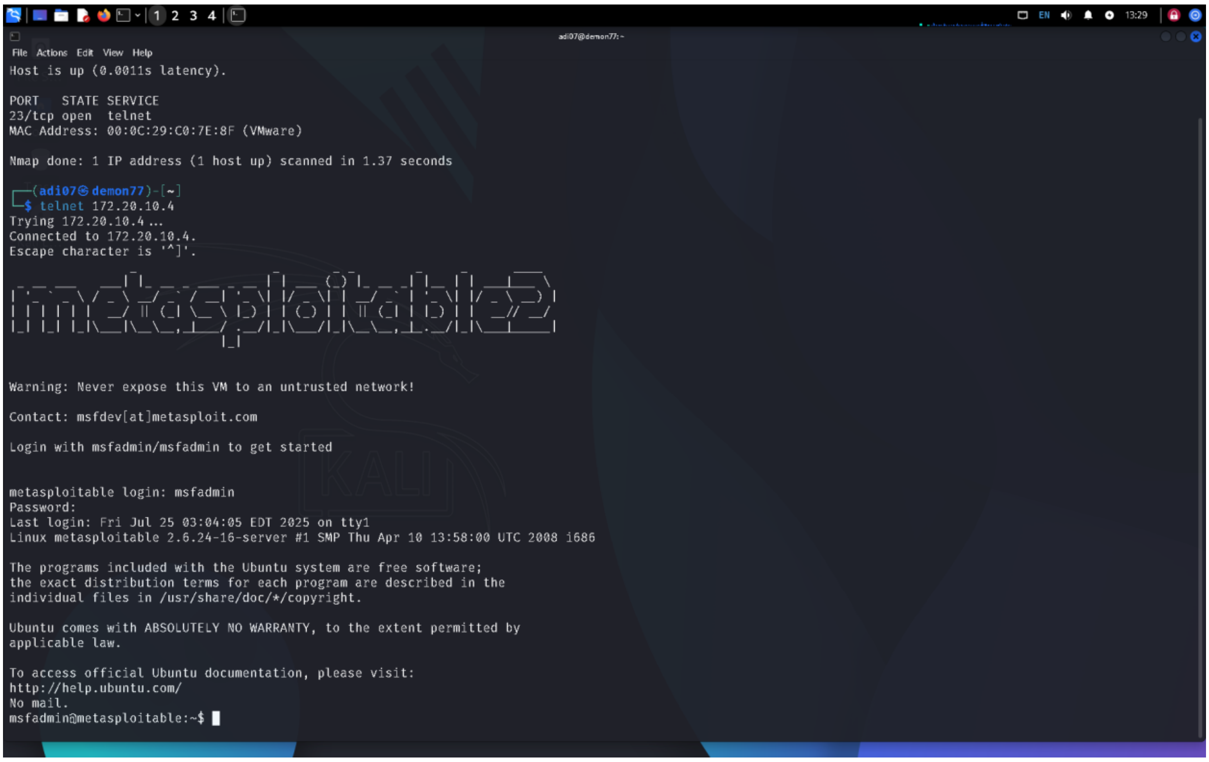
□ Output:

vbnet
CopyEdit

```
Trying 172.20.10.5...
Connected to 172.20.10.5.
Escape character is '^]'.

Ubuntu 8.04 metaploitable login: msfadmin
Password: msfadmin
```



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:7e:8f
          inet addr:172.20.10.4  Bcast:172.20.10.15  Mask:255.255.255.240
          inet6 addr: 2402:3a80:18de:b25a:20c:29ff:fec0:7e8f/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fec0:7e8f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4464 (4.3 KB)  TX bytes:7216 (7.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

(arg: 3)
```



```
Host is up (0.0011s latency).

PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0C:29:C0:7E:8F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds

┌──(adi07㉿demon77)-[~]
└─$ telnet 172.20.10.4
Trying 172.20.10.4...
Connected to 172.20.10.4.
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: Fri Jul 25 03:04:05 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:~$ █
```

□ Result:

Successfully logged in using **default credentials** (msfadmin/msfadmin). No encryption or authentication restrictions were enforced.

□ Step 3: Privilege Escalation

Cyber Kill Chain Stage: Exploitation

✅Objective:

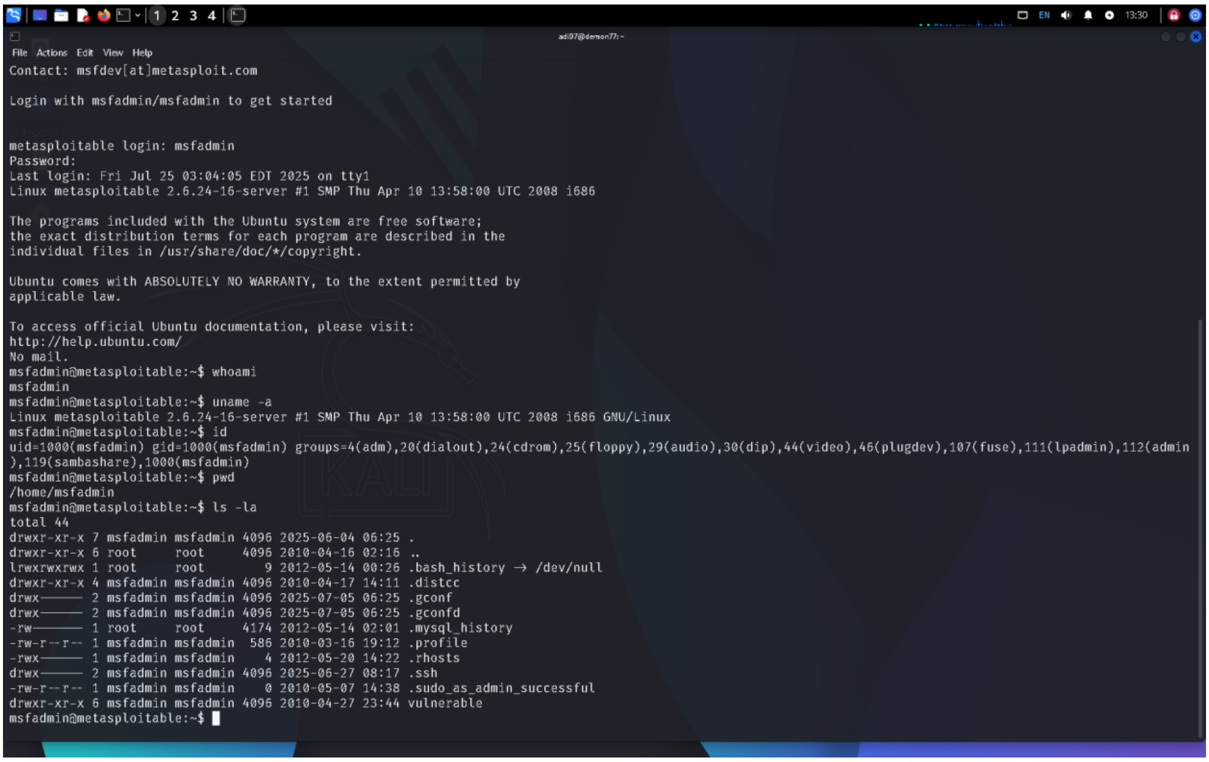
Verify current access level.

□ Commands Used:

bash
CopyEdit
whoami

□ Output:

nginx
CopyEdit
root



```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Jul 25 03:04:05 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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin
),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls -la
total 44
drwxr-xr-x 7 msfadmin msfadmin 4096 2025-06-04 06:25 .
drwxr-xr-x 6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root     root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx------ 2 msfadmin msfadmin 4096 2025-07-05 06:25 .gconf
drwx------ 2 msfadmin msfadmin 4096 2025-07-05 06:25 .gconfd
-rw------- 1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx------ 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx------ 2 msfadmin msfadmin 4096 2025-06-27 08:17 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ 
```

□ Result:

The attacker gained **root access**, meaning full administrative control without any privilege escalation exploit — a major security flaw.

□♂ Step 4: Post-Exploitation

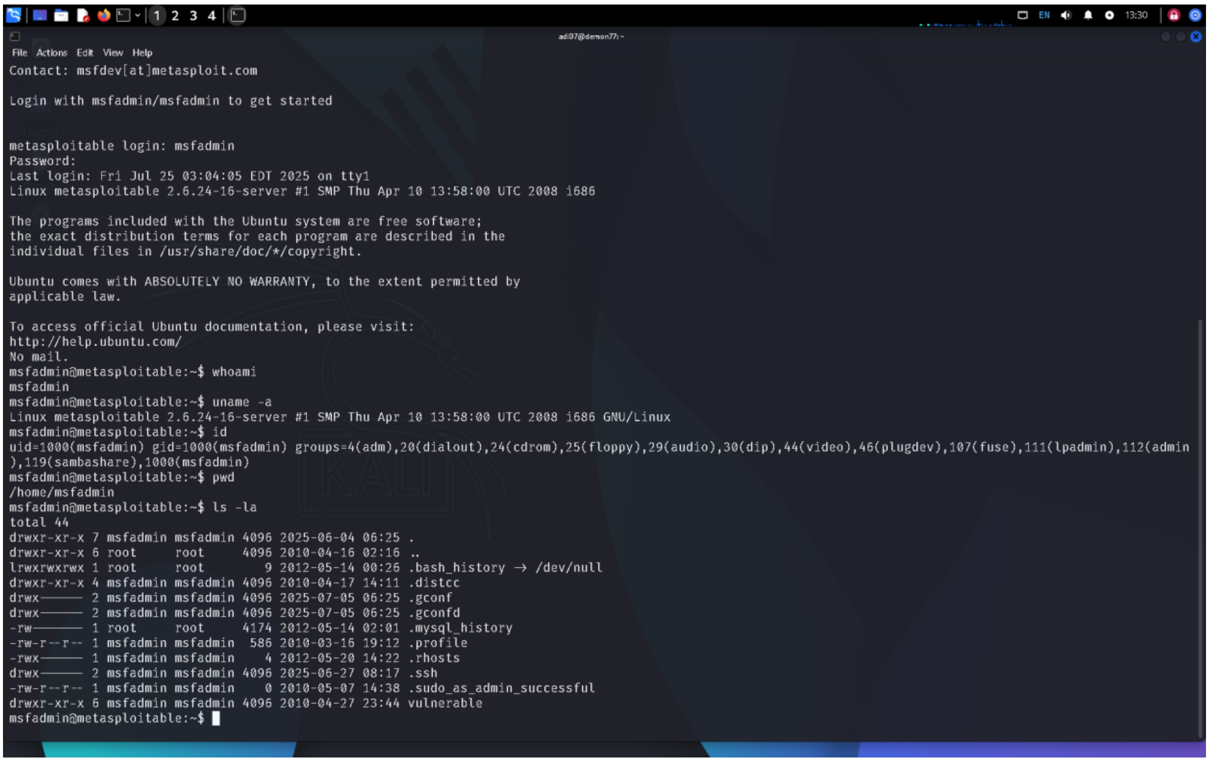
Cyber Kill Chain Stage: Actions on Objectives

✅Objective:

Demonstrate the risks of exposed root access.

□ Commands Used:

bash
CopyEdit
uname -a
id
pwd
ls -la
cat /etc/passwd



```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Jul 25 03:04:05 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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin
),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls -la
total 44
drwxr-xr-x 7 msfadmin msfadmin 4096 2025-06-04 06:25 .
drwxr-xr-x 6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root     root        9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx------ 2 msfadmin msfadmin 4096 2025-07-05 06:25 .gconf
drwx------ 2 msfadmin msfadmin 4096 2025-07-05 06:25 .gconfd
-rw------- 1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx------ 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx------ 2 msfadmin msfadmin 4096 2025-06-27 08:17 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ █
```

□ Findings:

- The attacker can view sensitive system files like /etc/passwd.

- Full system reconnaissance is possible.
- Indicates how plaintext Telnet access can lead to a **total system compromise**.

□ Step 5: Mitigation Strategies

Cyber Kill Chain Stage: Mitigation & Defense

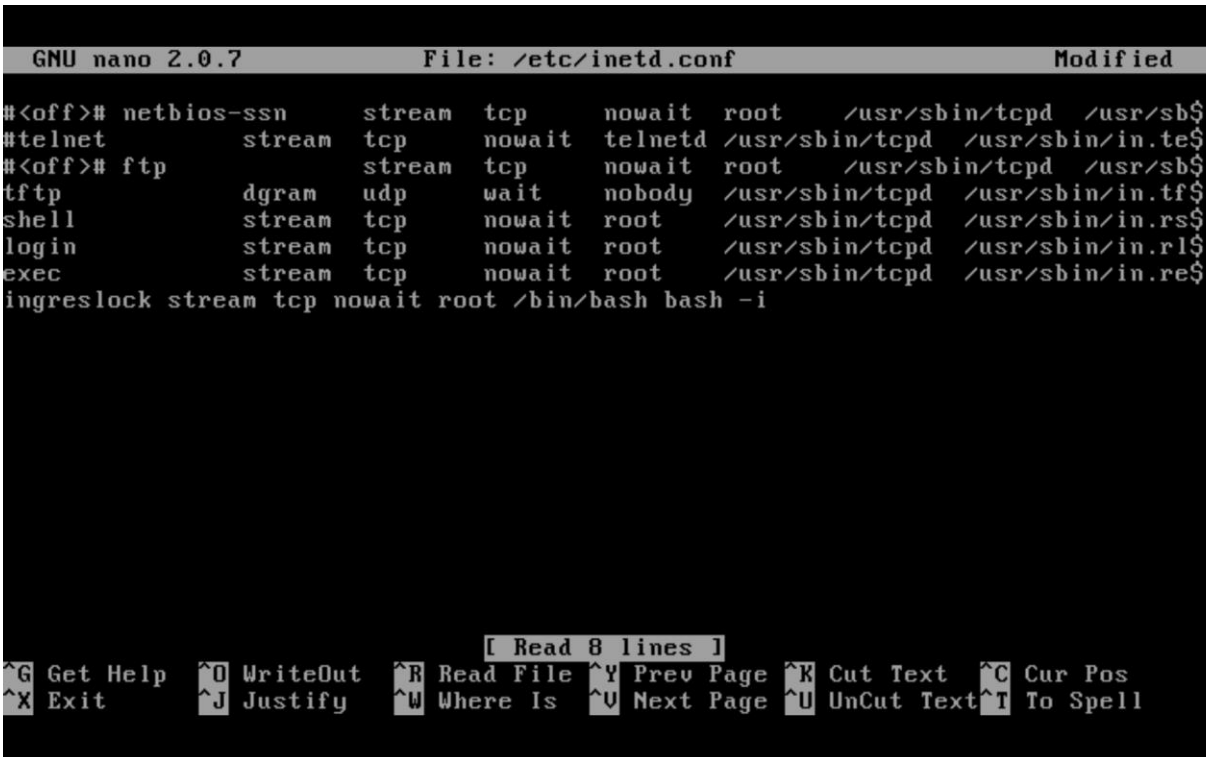
✓Objective:

Protect systems against Telnet-based attacks.

□ Recommendations:

1. **Disable Telnet and Remove Telnetd**

bash
CopyEdit
sudo apt remove telnetd



```
  GNU nano 2.0.7            File: /etc/inetd.conf                     Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
#telnet         stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i









                                [ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

2. **Use SSH Instead of Telnet**

- SSH encrypts communication and enforces key-based auth.

3. **Apply Firewall Rules**

- Block incoming access to port 23 (Telnet)

4. **Enforce Strong Credentials**

- Remove default accounts like msfadmin
- Use non-root login and sudo access only when needed

5. **Monitor Network Traffic**

- Look for unencrypted login attempts using tools like Wireshark

□ Expected Learning Outcomes

By completing this project, I have learned:

✅How to identify open services using **Nmap**
✅How to exploit **Telnet misconfigurations** to gain unauthorized access
✅The risks of **plaintext protocols** like Telnet
✅How to use basic **post-exploitation commands** to explore compromised systems
✅How to **mitigate system-level vulnerabilities** effectively

□ Conclusion

This hands-on project illustrates the dangers of exposed legacy services like **Telnet** on internet-facing or internal systems. With default credentials and no encryption, attackers can easily gain full control. The lab reinforces the importance of proper configuration, service hardening, and replacing legacy protocols with secure alternatives like **SSH**.