Meow Notes

Objective:

- The objective was to identify and exploit vulnerabilities within the **Meow** machine on hack-the-box and retrieving a flag to submit.

Tools Used:

I used some known tools to identify and exploit the vulnerabilities;

- **Nmap;** Which this is a powerful network scanning tool used for network discovery and security auditing.
- **Telnet Client;** A command line tool for connecting to remote systems over the Telnet protocol.
- **Hashcat / Online Hash Cracker;** Out of curiosity on how to crack a hash. For cracking the MD5 hash I got from the flag I had obtained on the machine.

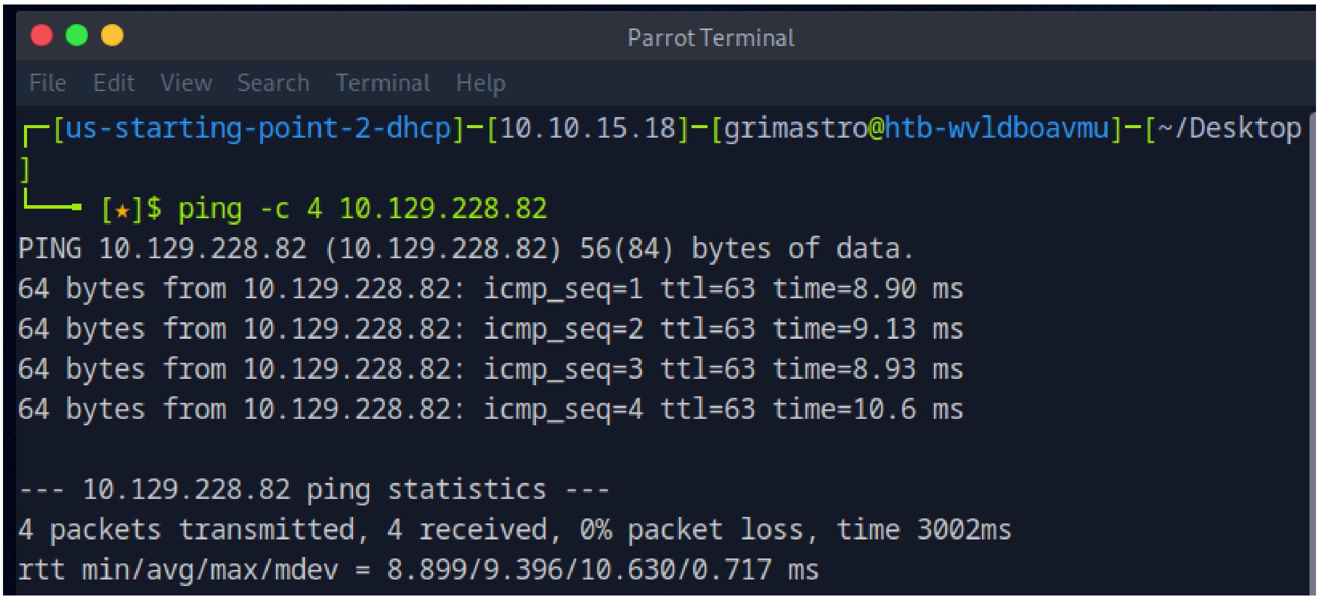
Methodology:

Information Gathering (Reconnaissance):

Ping the machine; I started off by pinging the machine to check if the target machine is reachable, by pinging it's IP address;

```
`ping -c 4 10.129.219.40
```

- **ping;** This command sends ICMP echo request packets to the specific IP address to check if the host is reachable.
- **-c 4;** This sends 4 ping requests and then stops (so we can adjust the number of ping requests to send).
- **10.129.219.40** This is the IP address of the target Machine



```
┌─[us-starting-point-2-dhcp]─[10.10.15.18]─[grimastro@htb-wvldboavmu]─[~/Desktop
]
└──╼ [★]$ ping -c 4 10.129.228.82
PING 10.129.228.82 (10.129.228.82) 56(84) bytes of data.
64 bytes from 10.129.228.82: icmp_seq=1 ttl=63 time=8.90 ms
64 bytes from 10.129.228.82: icmp_seq=2 ttl=63 time=9.13 ms
64 bytes from 10.129.228.82: icmp_seq=3 ttl=63 time=8.93 ms
64 bytes from 10.129.228.82: icmp_seq=4 ttl=63 time=10.6 ms

--- 10.129.228.82 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 8.899/9.396/10.630/0.717 ms
```

Network Scanning:

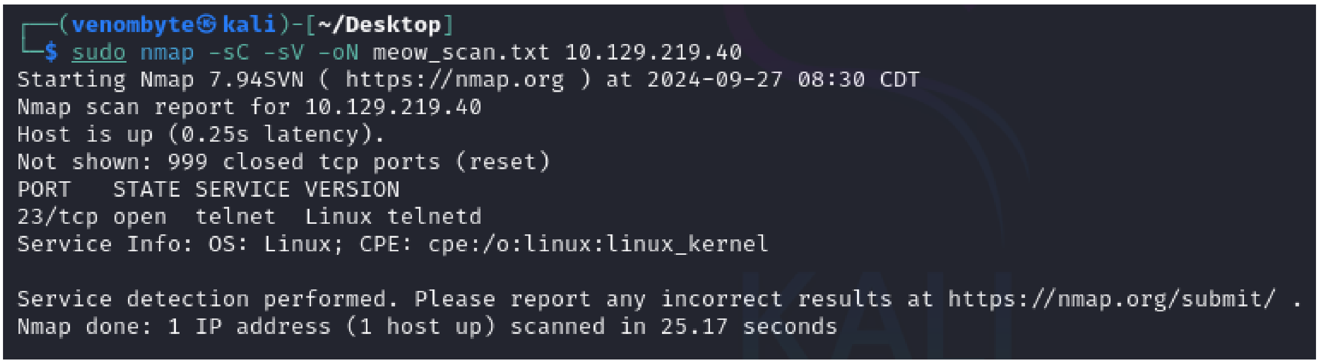
Nmap scan; After pinging the target machine to check if it was reachable I then proceeded to conduct a comprehensive Nmap scan, to identify open port and services using the command below;

```
sudo nmap -sC -sV -oN meow_scan.txt 10.129.219.40
```

- **sudo;** sudo runs the command with superuser privileges, which are often required for certain network operations.
- **nmap;** This command line tool is used for network discovery and security auditing.
- **-sC;** This nmap option runs defaults scripts, which helps in service detection and vulnerability enumeration.
- **-sV;** This nmap option enables version detection, allowing Nmap to determine the version of the services running on the open ports.
- **-oN meow_scan.txt;** I used this option to output the can results to a file named "meow_scan.txt" for later analysis in case.
- **10.129.219.40;** This is the IP address of the target machine.

Nmap Results

- The scan revealed that port 23 (which is Telnet) is open.



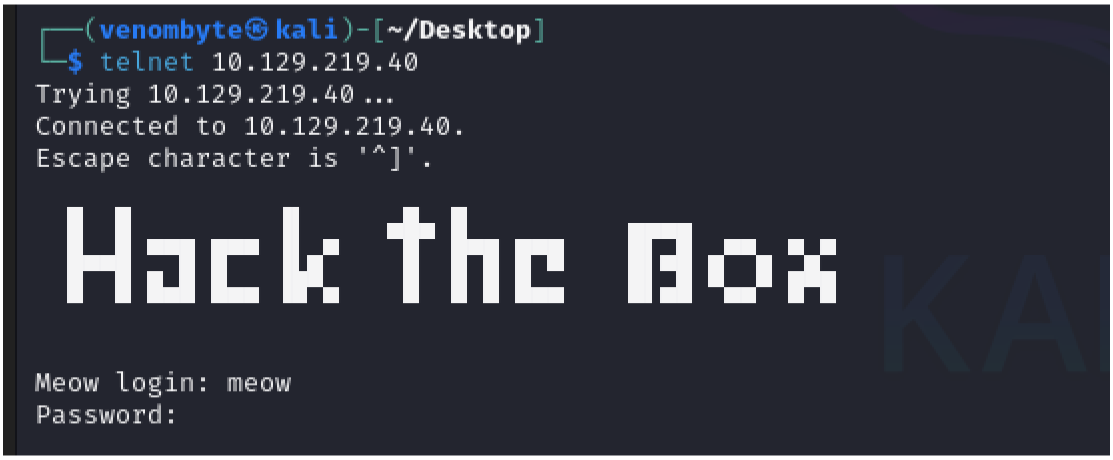
```
┌──(venombyte㉿kali)-[~/Desktop]
└─$ sudo nmap -sC -sV -oN meow_scan.txt 10.129.219.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 08:30 CDT
Nmap scan report for 10.129.219.40
Host is up (0.25s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
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 25.17 seconds
```

Exploitation:

Connecting to Telnet; After scanning the target machine I proceeded to connect to the Telnet service on port 23 using the command below;

`telnet 10.129.219.40 23`

- **telnet;** This command is used to create a connection to the remote host over the **Telnet protocol**.
- **10.129.219.40;** The IP address of the target machine.
- **23** The port number where the Telnet service is running.



```
┌──(venombyte㉿kali)-[~/Desktop]
└─$ telnet 10.129.219.40
Trying 10.129.219.40...
Connected to 10.129.219.40.
Escape character is '^]'.
```

```
Meow login: meow
Password:
```

Authentication; Upon connecting to telnet, I was prompted to enter the username and password, in which I tried various word like **(meow, admin, user, root)** until I used root and I was granted permission.

Retrieving the flag; After successfully logging in, I navigated to the location of the flag and retrieved its content using the commands below;

```
ls
cat flag.txt
```

- **ls;** This lists the files and directories on the server / machine.
- **cat;** This command reads the content of the file and display in the terminal.
- **flag.txt;** This is the name of the file which contained the MD5 hash.

Results;

- The flag was successfully retrieved, in which it was an MD5 hash `b40abdfe23665f766f9c61ecba8a4c19`.

Conclusion:

- To me the **Meow** challenge demonstrates the importance of network scanning and service enumeration in Penetration Testing. Highlighting the vulnerabilities associated with using insecure protocols like Telnet.

Recommendations for Securing Telnet (Port 23):

To protect against unauthorized access to the Telnet service, the following measures are recommended:

- **Disable Telnet**: Telnet is an insecure protocol. It should be disabled in favor of **SSH** (Secure Shell) to provide encrypted communications.
- **Implement Strong Authentication**: If Telnet must be used, enforce strong password policies and consider implementing multi-factor authentication (MFA).
- **Access Control Lists (ACLs)**: Limit access to the Telnet service by using firewall rules or ACLs to restrict access to trusted IP addresses only.
- **Regular Audits and Monitoring**: Conduct regular audits of access logs and use intrusion detection systems (IDS) to monitor for unauthorized access attempts.
- **Update and Patch**: Regularly update and patch the system to protect against known vulnerabilities in Telnet or related services.