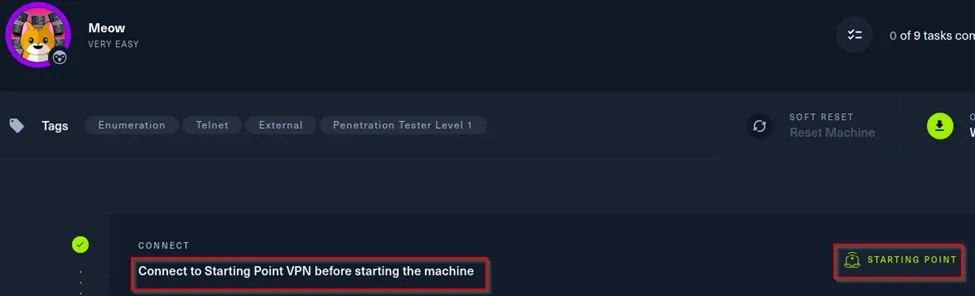
**HACK THE BOX- MEOW (TELNET)**

Connect to the VPN before starting machine because machine should be in same network .



Then the machine is active and it will display the target IP address.

Completing the tasks:

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

Virtual machine

* **Task 2:** What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It’s also known as a console or shell.

Terminal

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

Openvpn

* **Task 5:** What tool do we use to test our connection to the target with an ICMP echo request?

Ping

* **Task 6:** What is the name of the most common tool for finding open ports on a target?

Nmap

* **Task 7:** What service do we identify on port 23/tcp during our scans?

telnet

* **Task 7:** What service do we identify on port 23/tcp during our scans?

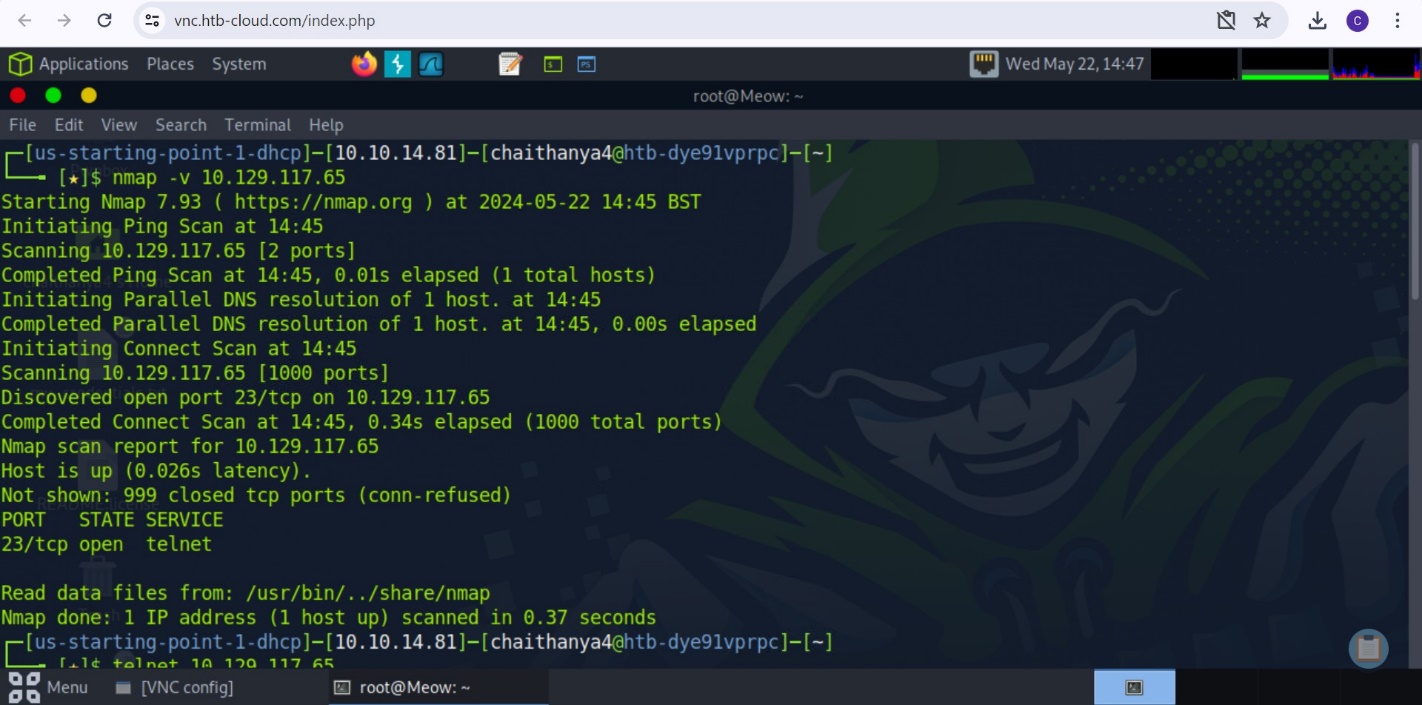
Root

Next task is to capture the flag:

Go to the virtual machine, open the terminal and start hacking the target machine

1. **Scanning :** for scanning we use the nmap tool. Which display the open ports in the target IP. So, use the command nmap –v [IP-address of target machine].

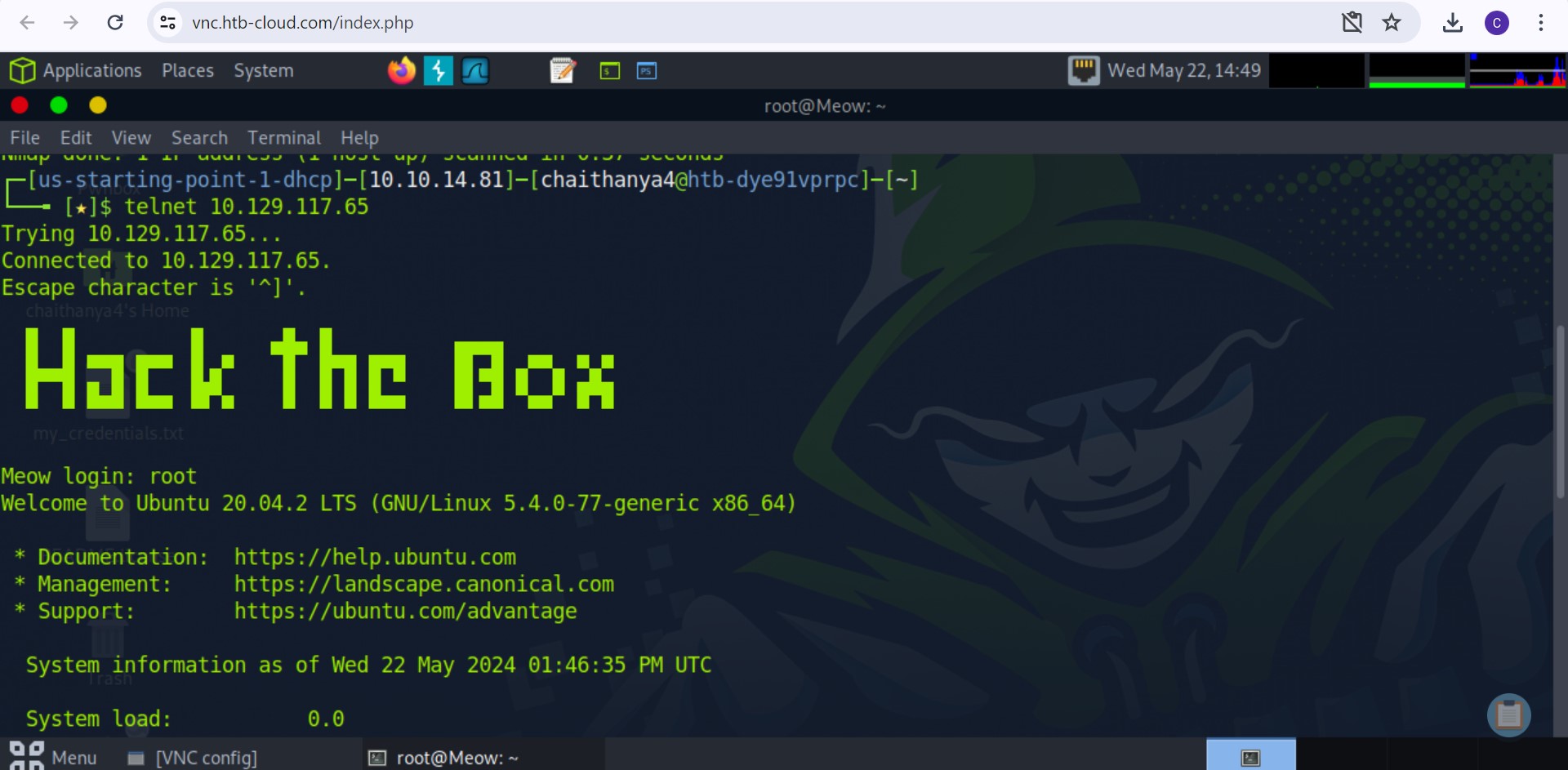
$ nmap –v 10.129.117.65



Here we found that the port 23 is opened and it is running telnet sevices. So, we are going to gain access to the target machine through this port.

1. **Gaining access:** since the service is telnet, we are using telnet tool to login into the target machine.

More about telnet : **Telnet** is one of the earliest and most basic network protocols used on the Internet or local area networks. It provides a command-line interface for communication with remote devices or servers. Telnet operates over a network using TCP (Transmission Control Protocol)

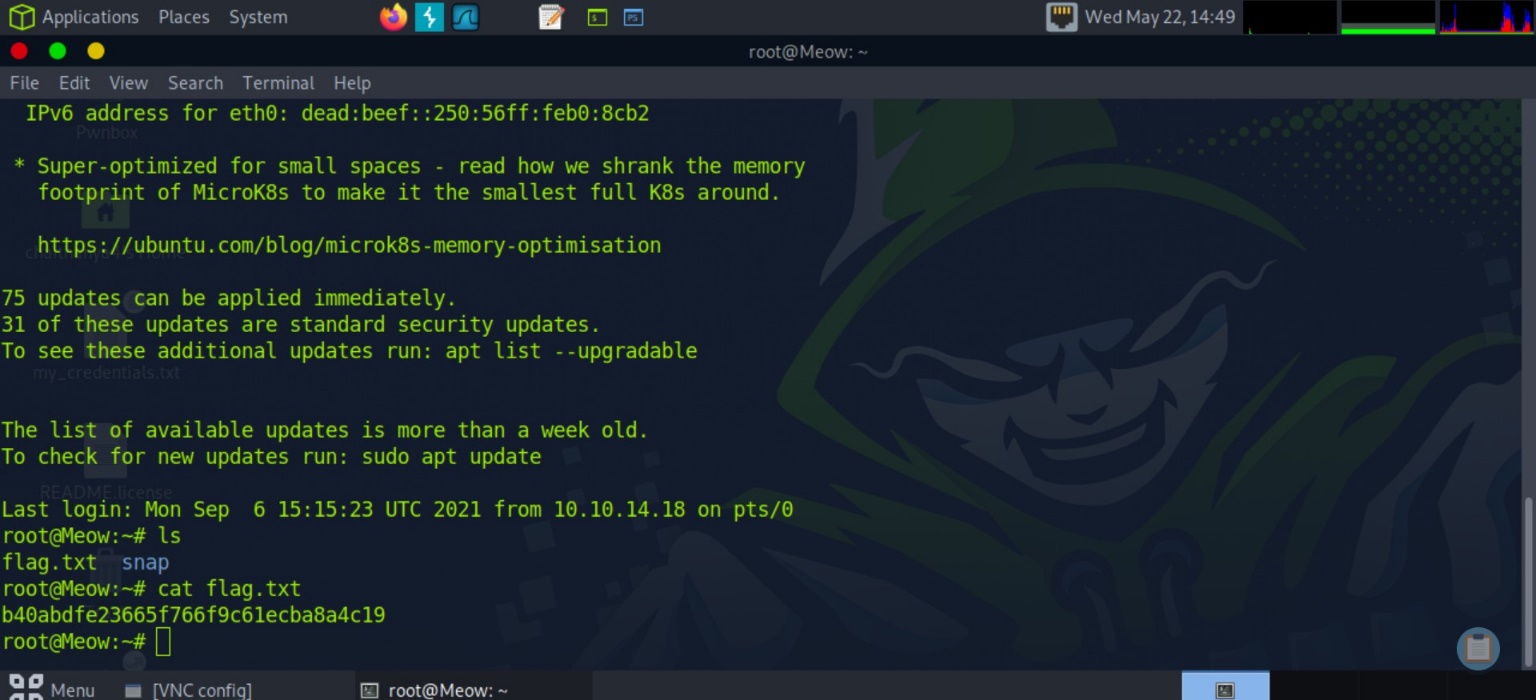


We will login to meow using the name “root” . finally, we logged in into the target using the port 23 (telnet). Now we need to look for file which has the capture file password.

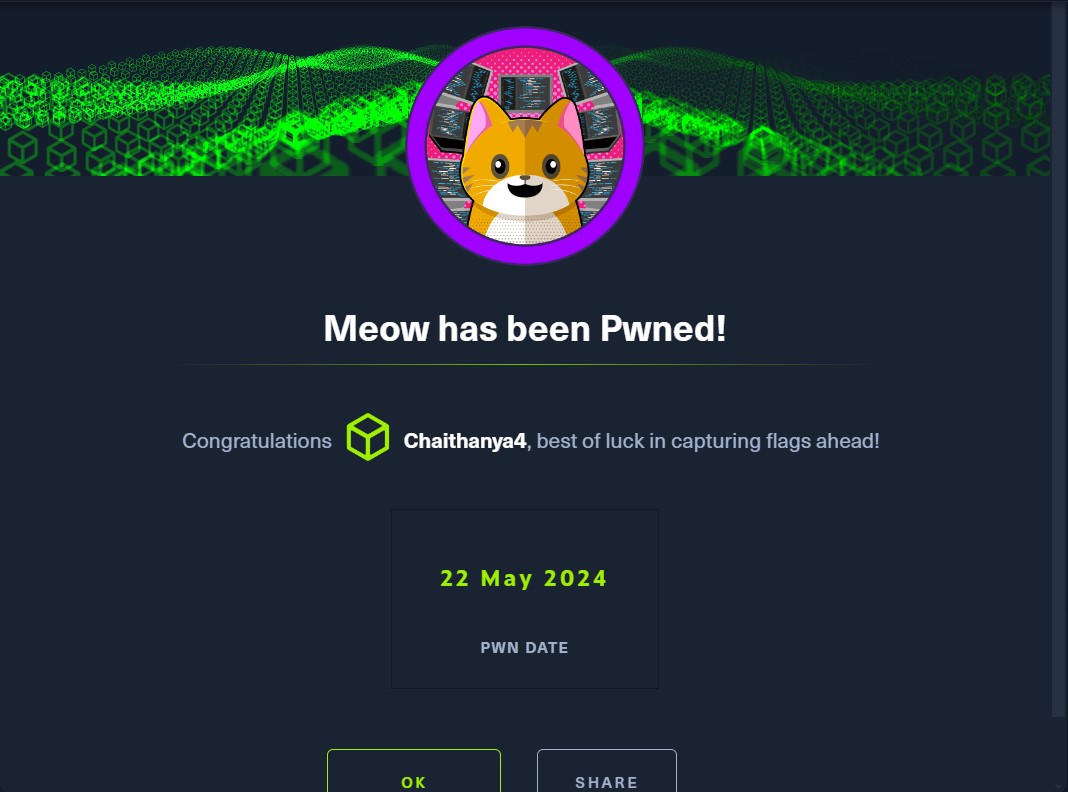
1. **Capturing the flag:** since we gained access to the target. We can look for the files present in the target. In terminal we use the command “ls” to list the life. Then we use command “cat” to display the content in the file. Copy the flag, submit the root flag

#ls

flag.txt snap

#cat flag.txt

 Received message as “**Meow has been Pwned**” and Challenge solved successfully.



**Conclusion :**

Run **nmap**scan on [target\_ip] and we have noticed port 23/tcp in an open state, running the telnet service. Now use mentioned command to connect to the target server “**telnet [target\_ip]**” and provide “**root**” as username. After login use “**ls**” command to check all available directories/files. We can notice “flag.txt” file and to view content use “**cat flag.txt**” command and solve this machine.