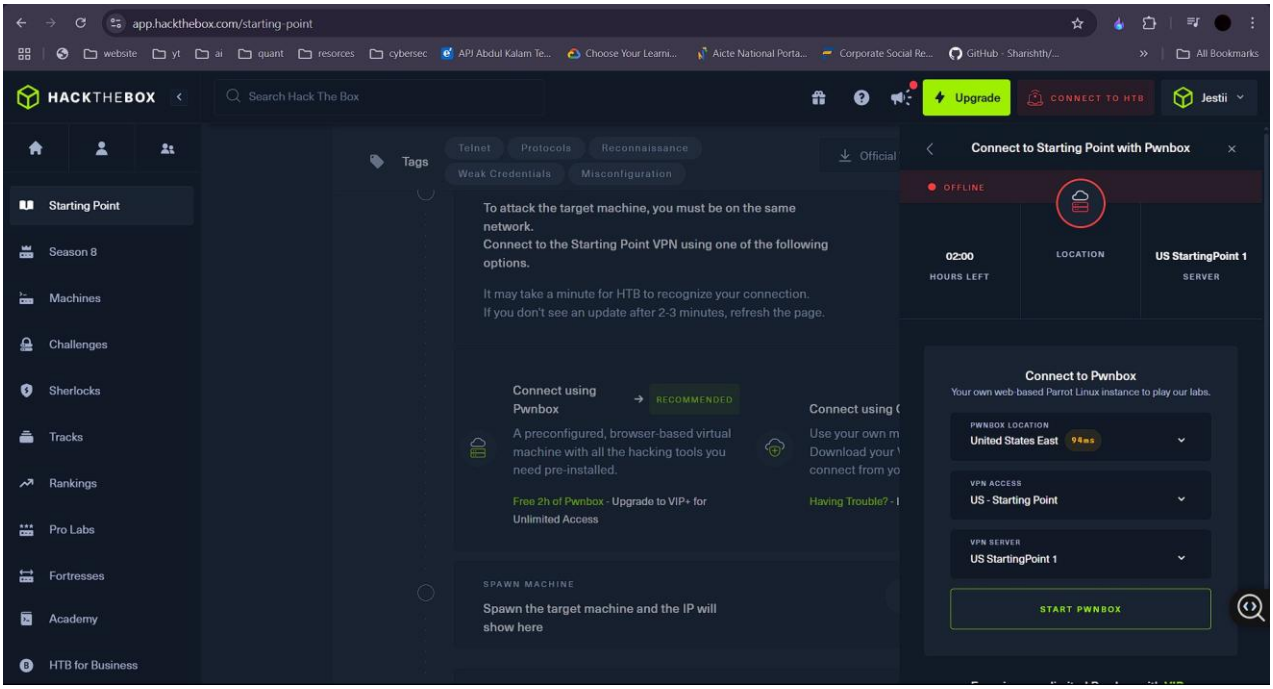
CTF Writeup: Meow

Prepared By: Jestine Thomas Mathew

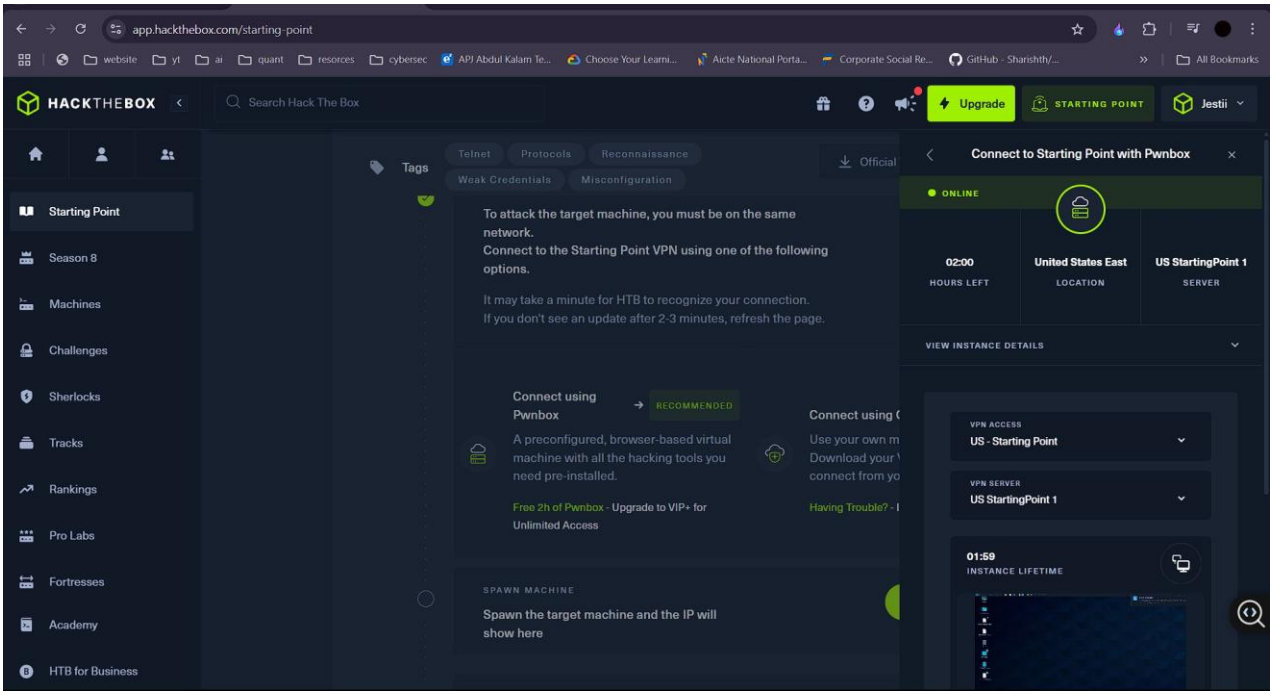
This writeup details the steps taken to solve the 'Meow' machine from Hack The Box's Starting Point series. This machine is categorized as 'very easy' and focuses on basic reconnaissance and exploitation techniques.

2.1 Connecting to the VPN

First, we need to connect to the Hack The Box VPN to access the target machine. This can be done using either Pwnbox or OpenVPN. For this writeup, I used Pwnbox.

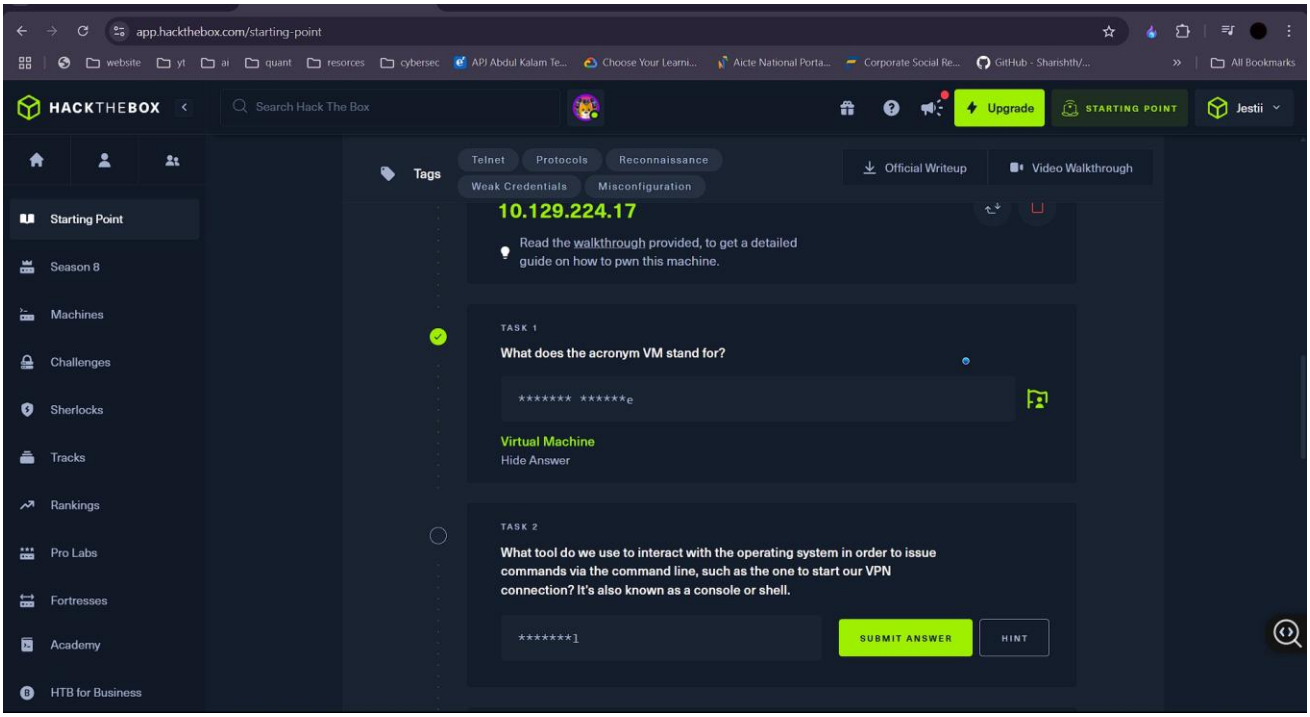


After starting Pwnbox, the VPN connection is established, and we are ready to interact with the target.



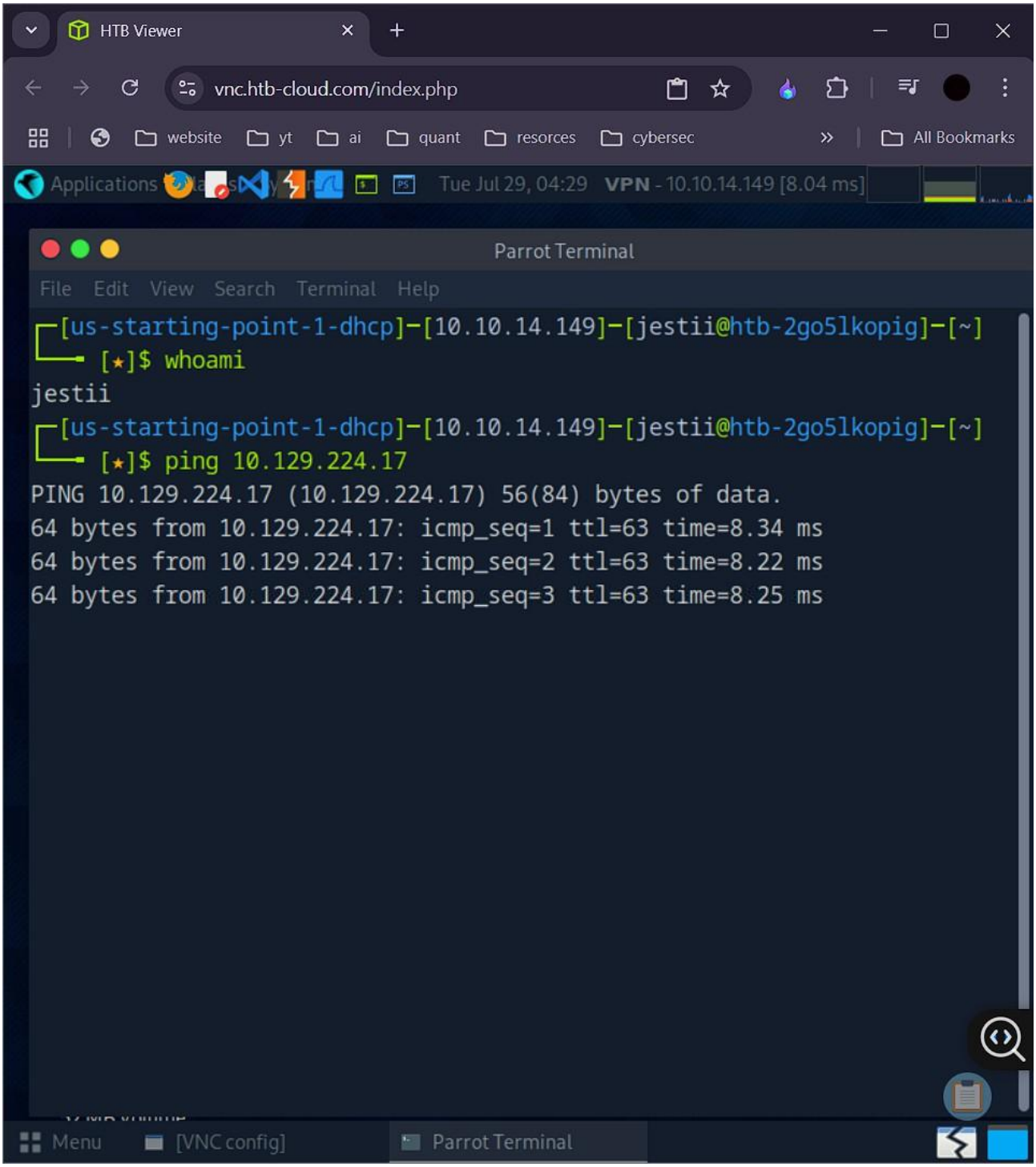
2.2 Identifying the Target IP Address

Once connected, the target machine's IP address is revealed on the Hack The Box platform. In this case, the IP address is 10.129.224.17



To confirm connectivity to the target, a simple ping command was executed from the Pwnbox terminal.

```
ping 10.129.224.17
```

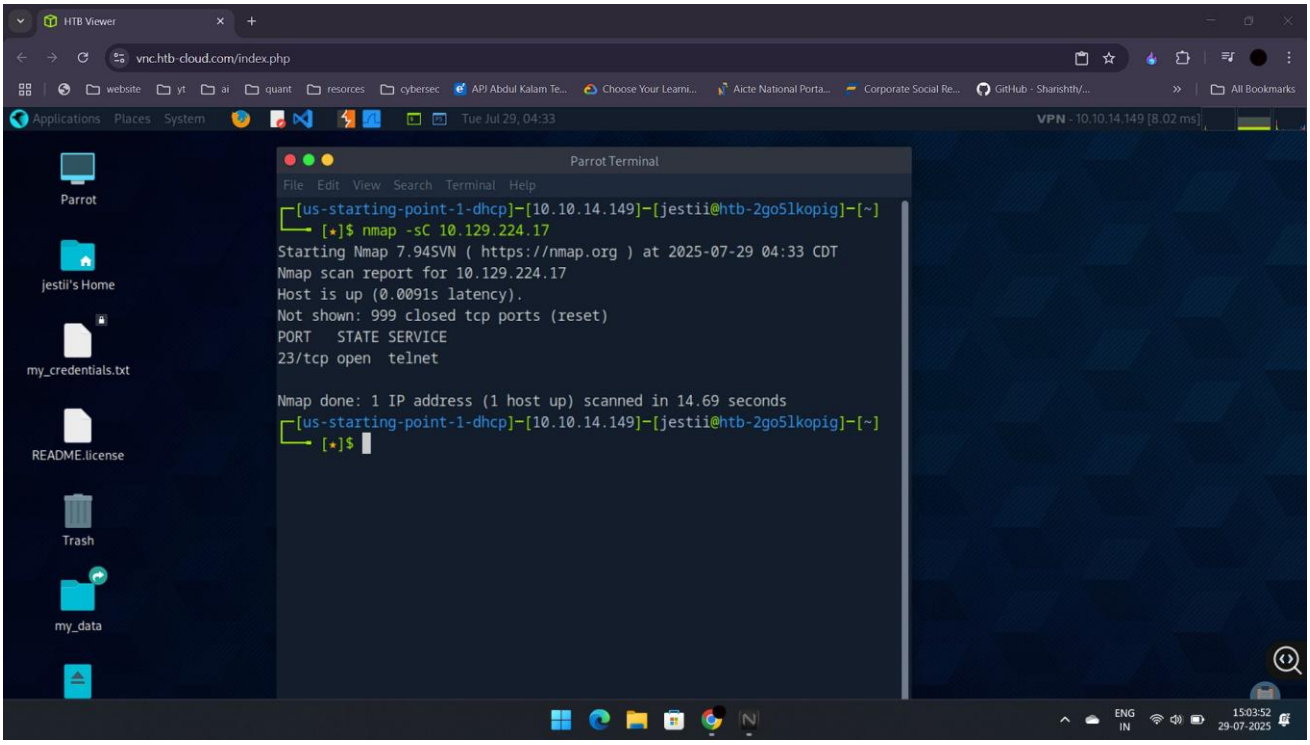


2.3 Port Scanning with Nmap

Next, I performed a port scan using nmap to identify open ports and services running on the target machine. The command used was:

```
nmap -sC -sV 10.129.224.17
```

This scan revealed that the port 23/tcp is open, running the telnet service.

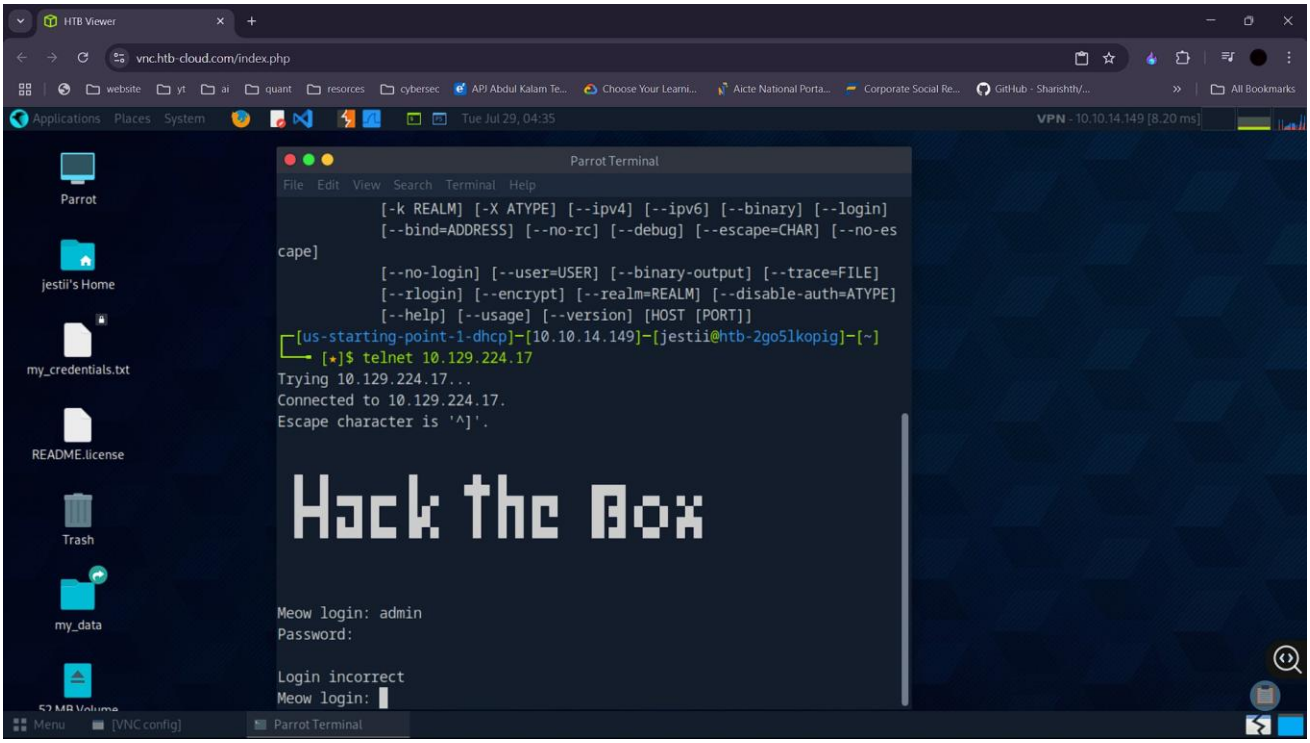


3. Exploitation

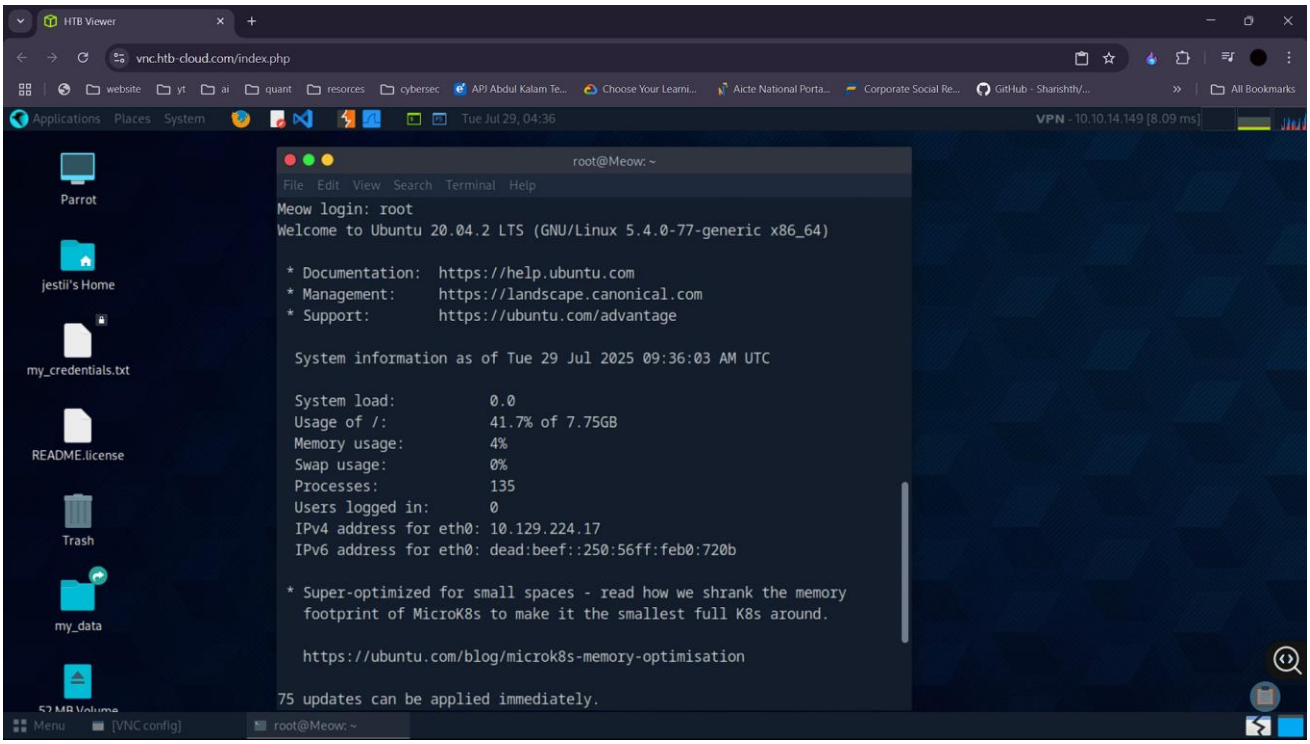
Given that port (Telnet) is open, I attempted to connect to the machine using the telnet command.

```
telnet 10.129.224.17
```

Upon connecting, I was prompted for a login. first I tried common credentials, such as admin with a blank password, which resulted in a login incorrect message.

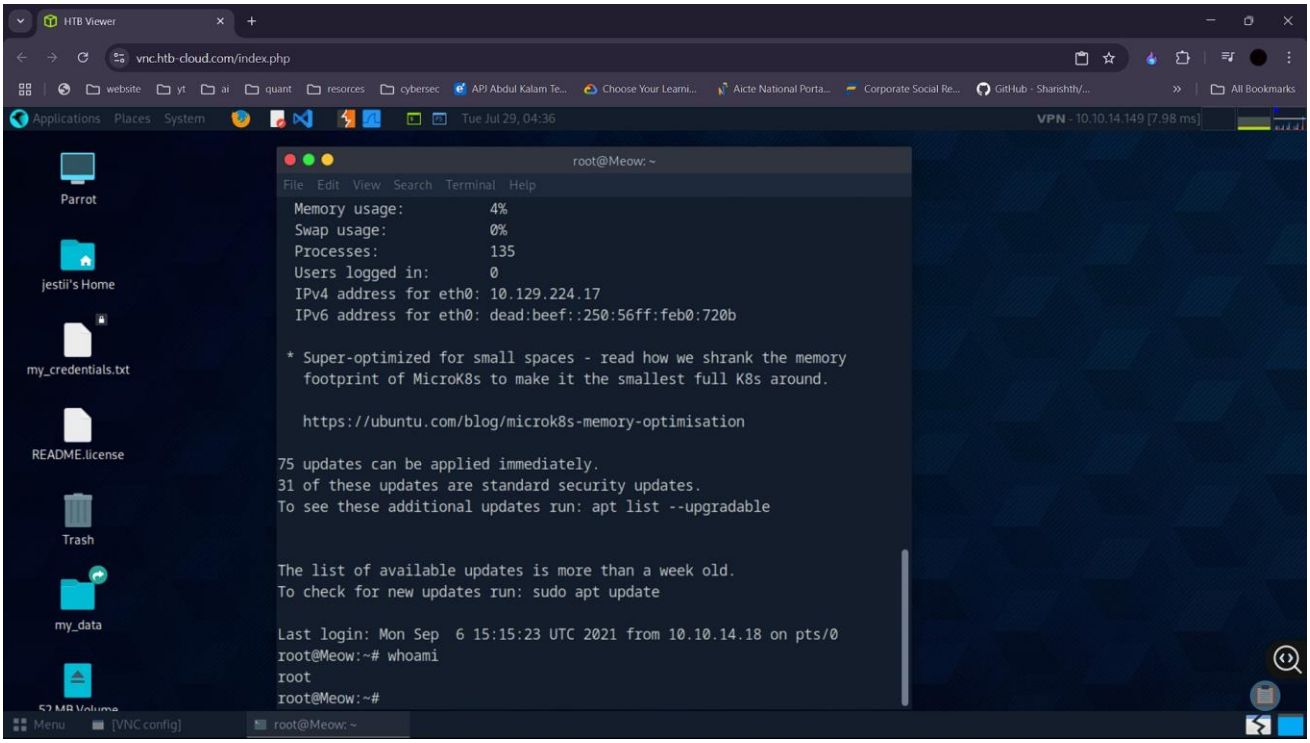


However, recalling that this is a very easy machine, I then attempted to log in as root with a blank password. This attempt was successful, granting us access to the machine.



After logging in, I confirmed the user with the whoami command.

```
whoami
```

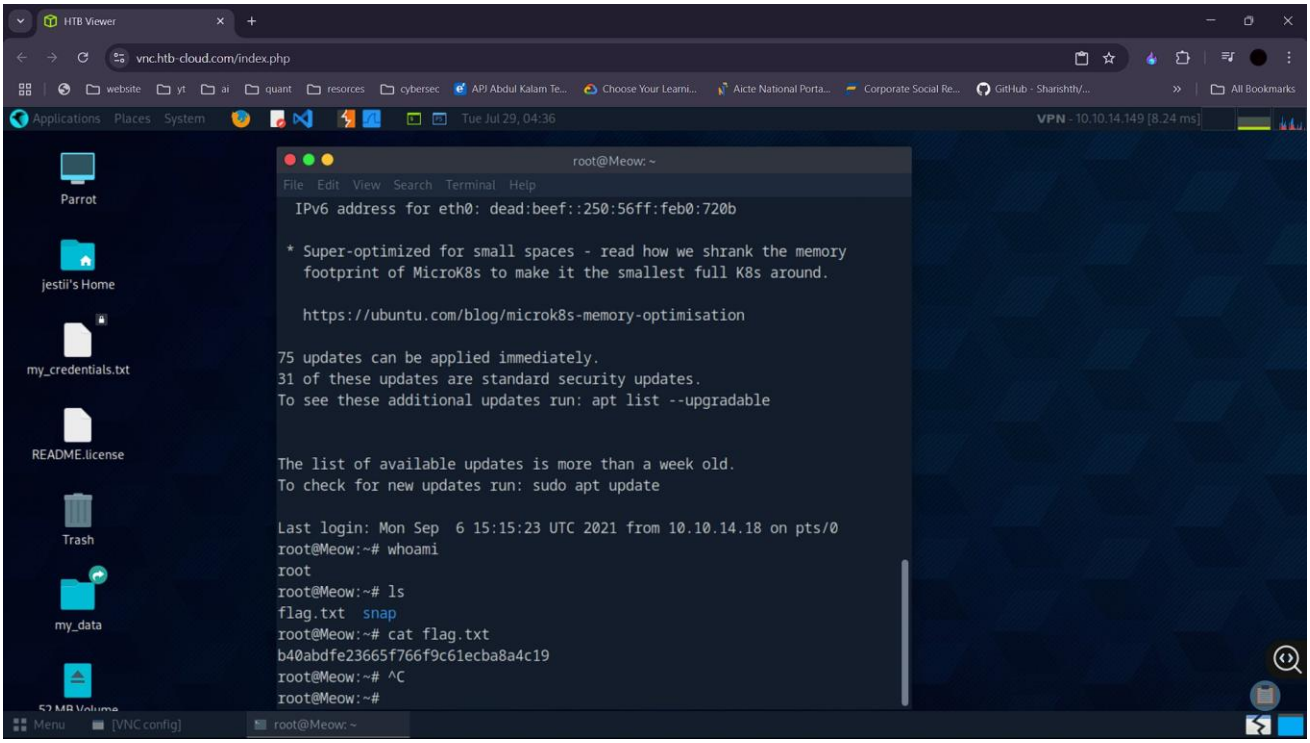


4. Flag

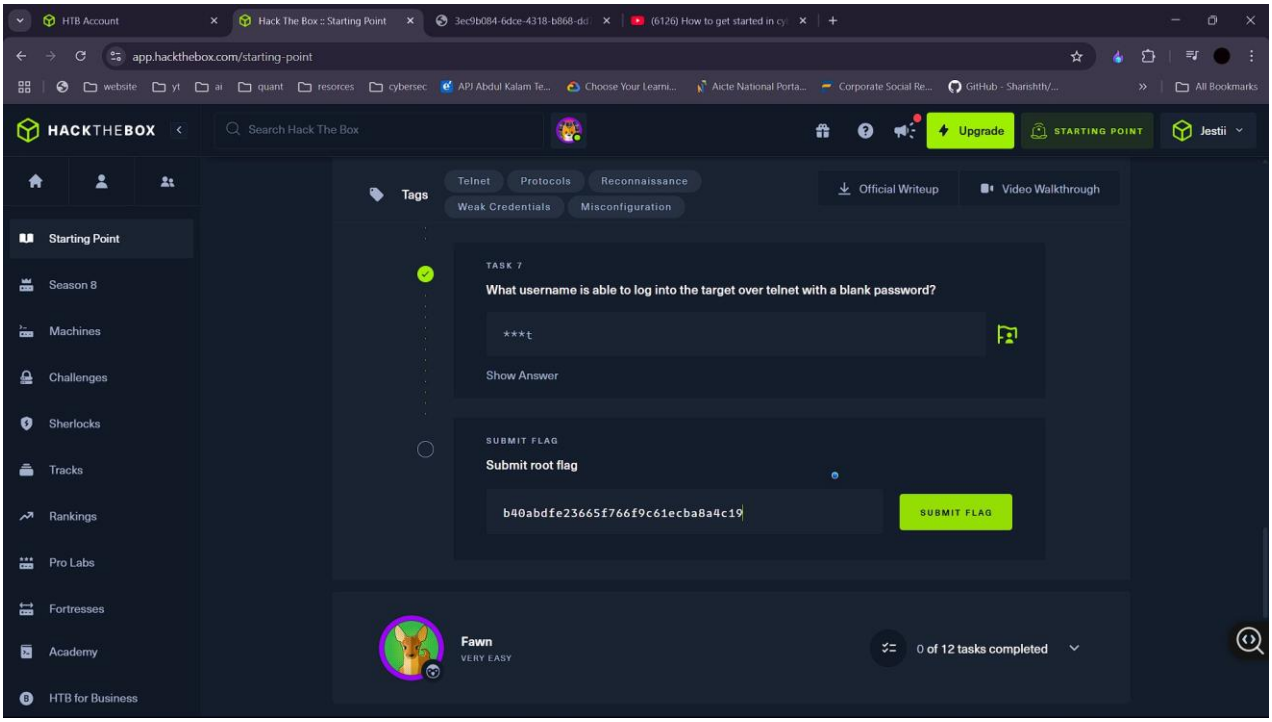
With root access, we proceeded to look for the flag. We listed the contents of the current directory using ls and found a file named flag.txt .

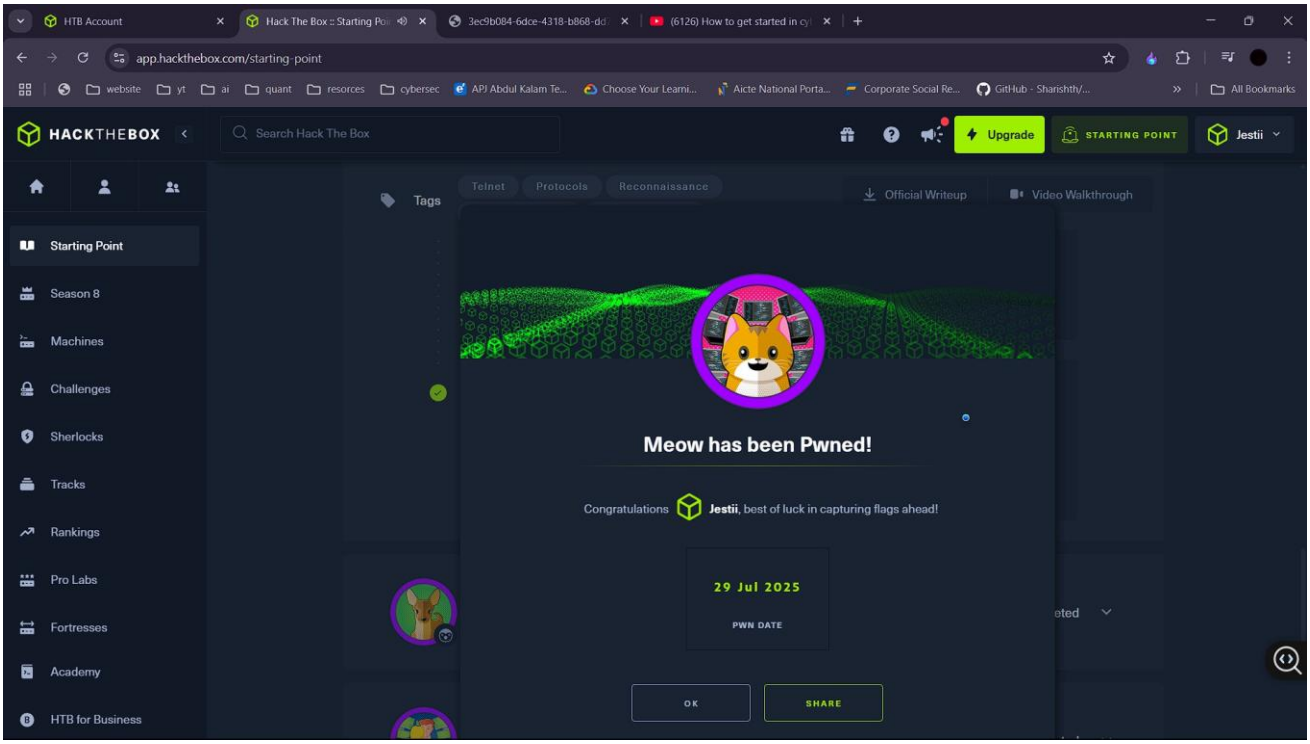
```
 ls
cat flag.txt
```

Reading the flag.txt file revealed the flag: b40abdfa23665f766f9c61ecba8a4c19 .



Finally, I submitted the flag on the Hack The Box platform to complete the challenge.





5. Conclusion

The Meow machine was a straightforward introduction to CTF challenges, focusing on basic reconnaissance (ping, nmap) and exploitation (telnet with default credentials). It highlights the importance of checking for common vulnerabilities and understanding basic network services.