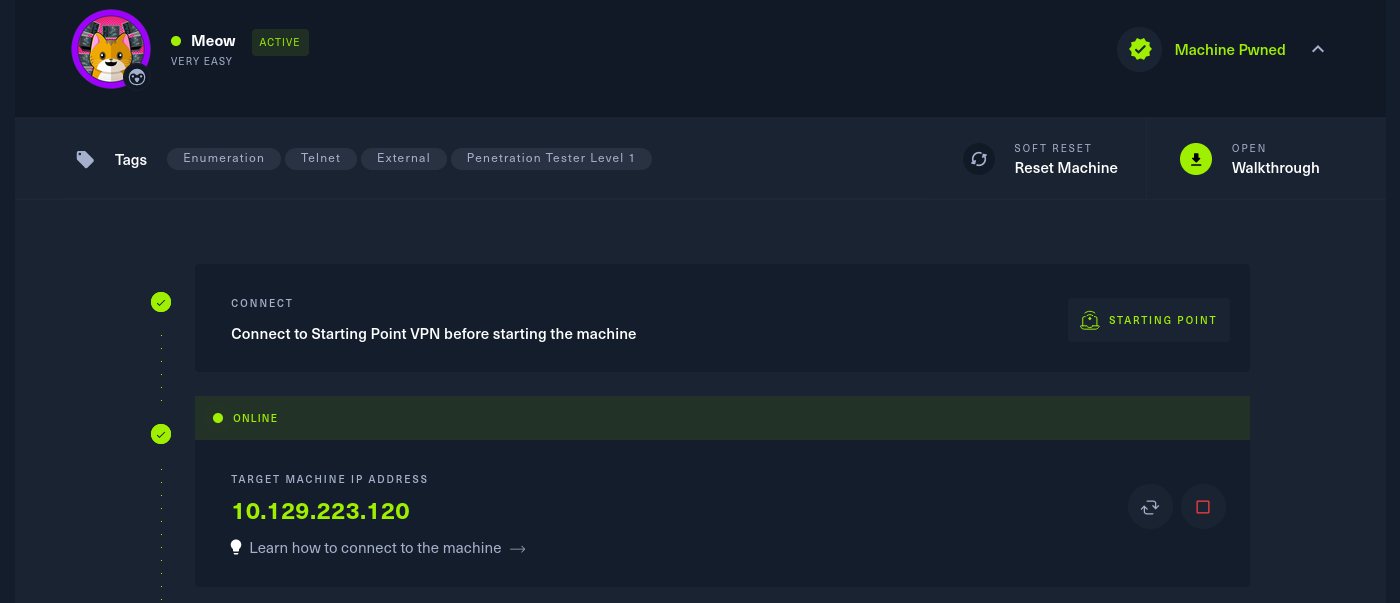
# MEOW

* This writeup is a direct walkthrough to the flag. Hoping that you have given your best before referring this writeup.
* Assuming that you have using pwnbox or connected to **OPENVPN.** If not, do refer to [vpn-connection](https://github/shybu9/HACK-THE-BOX/vpn_connection) file.
* Once the is spawned, machine ip will be given. Looks as below:



**ENUMERATION:**

## Screenshot 2022-10-30 at 04-55-14 ENUMERATION at DuckDuckGo

* For enumeration we use tool called **nmap** which comes by default in kali-Linux .
* Open a new terminal type the following command to perform nmap scan:

# **nmap -sVC -v -T4 <ip>**

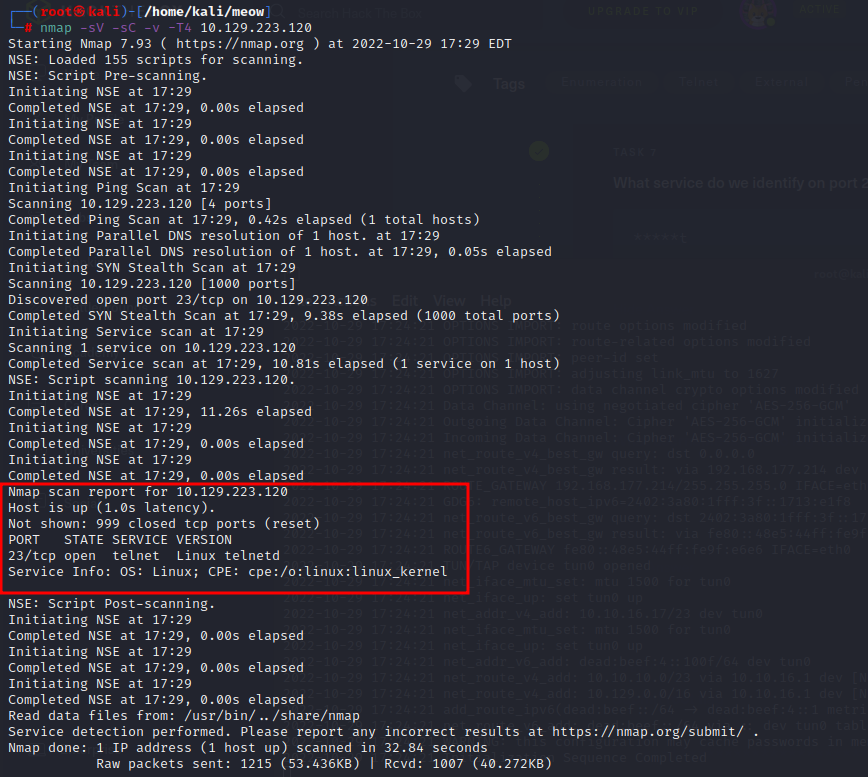
-sVC : combination of -sV & -sC, used scan version of the open ports & perform basic scripts on open port ( -sC is illegal to use on public ip)

-v : used to make output more verbose and readable.

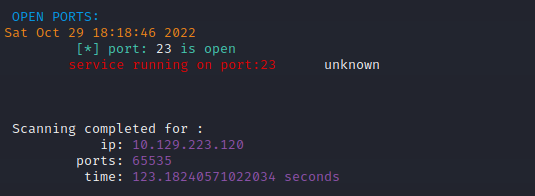
-T4: used for decent balance of speed and info.

<ip> : ip address of spawned machine.

Try cmd: **nmap --help** for more info about the tool



* *I usually perform one more scan using my* ***personal tool: [portscanner](https://github/shybu9/portscanner)*** *before analysing the nmap report.*

**

~ I prefer this tool because of its speed as you can see it took just **123 seconds** for scanning **65535 ports.**

Even still some improvements should be done.

**ANALYSING BOTH SCANS :**

Operating System: **Linux**

Number of open ports : **1**

Port Number : **23**

Service Running : **telnet**

Version : **Linux Telnetd**

**FOOTHOLD**

* The **TELNET SERVICE** is running open on **port 23.**
* We could try to connect with TELNET using IP address and default credentials.
* Command for connecting TELNET :

# **telnet <ip>**

Default Credentails used:

* Username : admin

Password : password

* Username : administrator

Password : password123

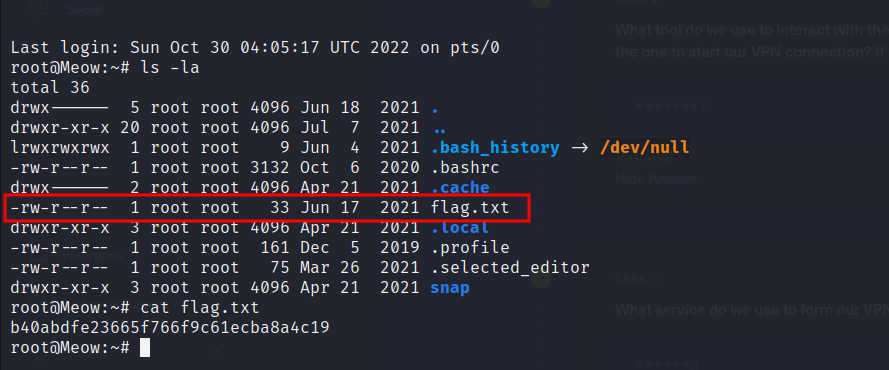
* Username : root

Password : root



* When we try to login with username: **root**, we have been directed to root terminal.
* For listing the files and directories on this terminal we use the command :

# **ls -la**



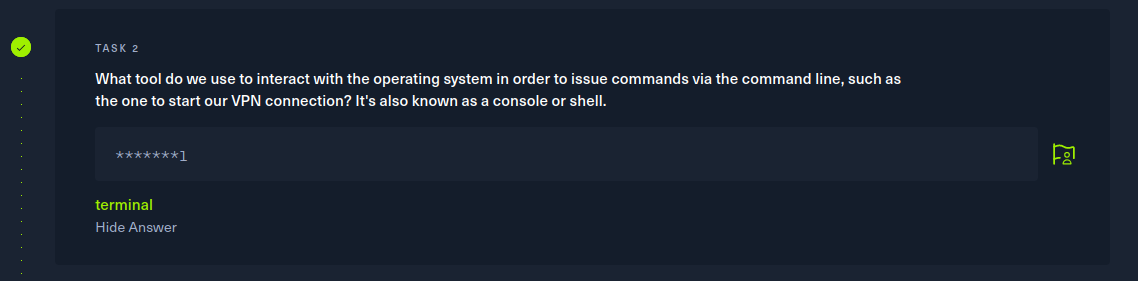
* There is one file name called **flag.txt**, we have seen the contents of flag.txt on command line using cat command :

# **cat flag.txt**

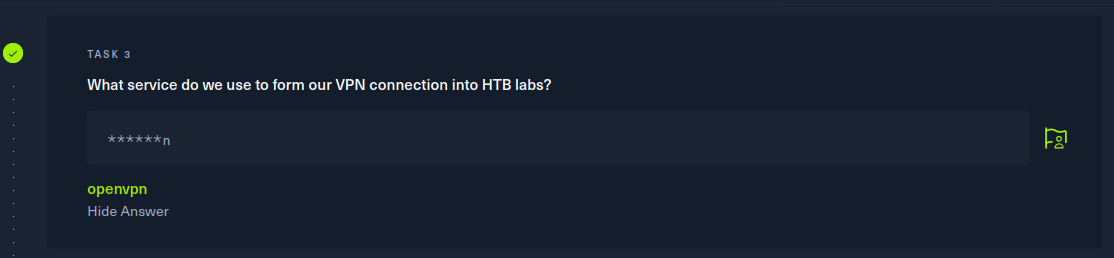
* Finally the **flag has been captured…………**
* Do submit the flag once all the questions are answered.
* I think all the questions are covered in our walkthrough. The following are the solutions for tasks:



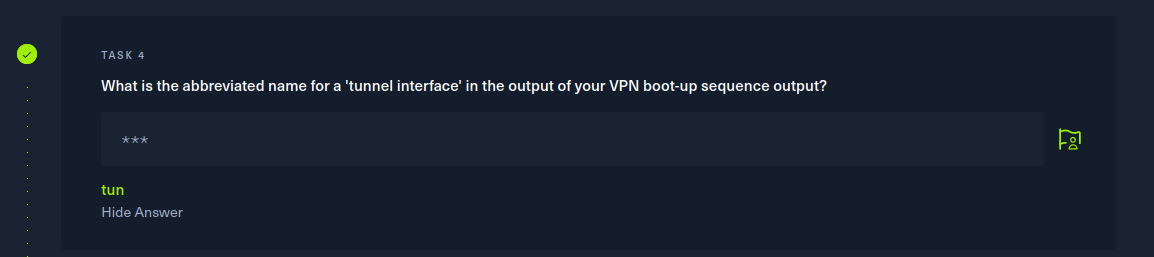
~ Virtual Machines are the best way to try linux or other operating systems. EXAMPLES : virtual box & vm ware



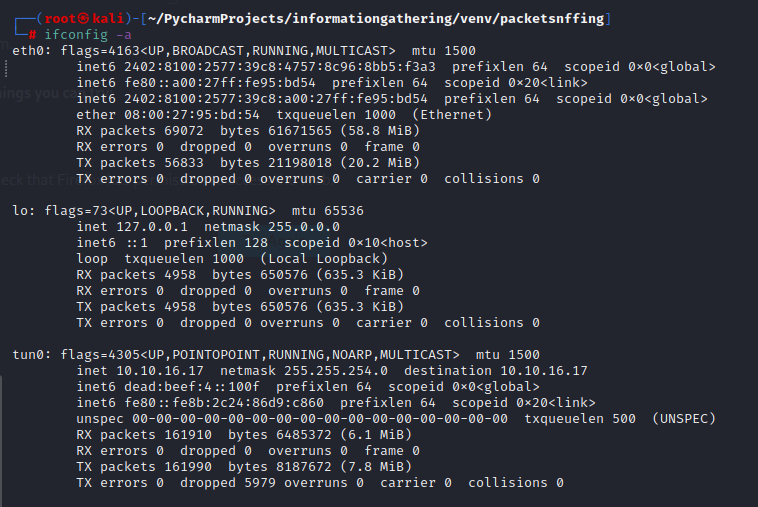
~ Most of the penetration testing done on command line known as TERMINAL . As this tools are Command Line Based.

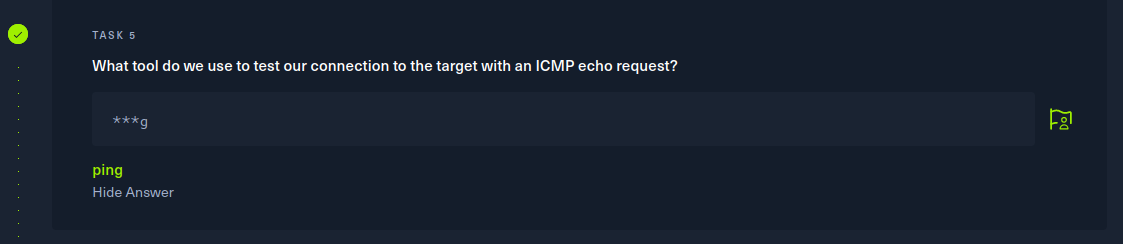


~ We have downloaded a vpn file and run command : openvpn <filename> for connecting to server and practicing on machines.

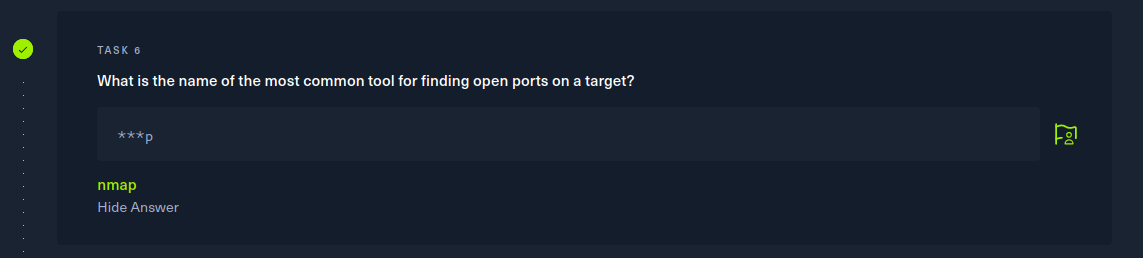


~ Try command : # ifconfig -a , you observe 3 interfaces eth0, lo, and tun0. Which is the IP address after connecting to openvpn.

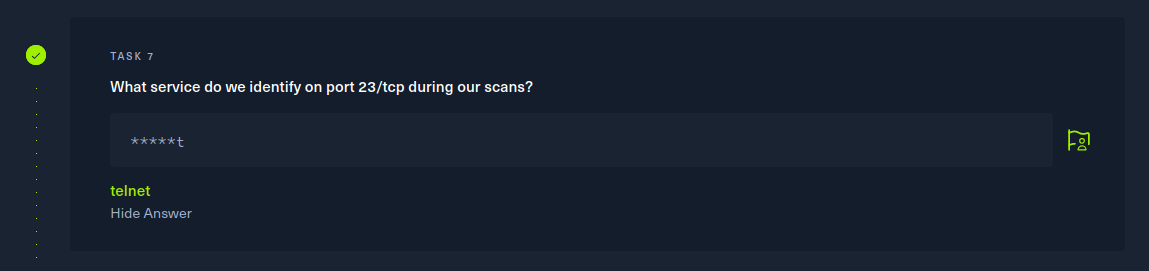




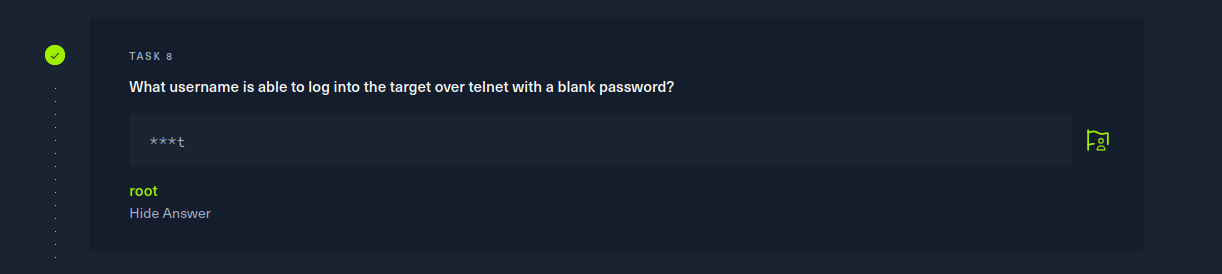
~ Command : # ping <IP address> send packets to IP and checks wheather the IP is online or not. This is preferred to be done before nmap scan. Just to check wheather the host is up or not.



~ We just have performed an nmap scan in our ENUMERATION process.



~ At nmap scan report we have seen open ports and their services running ( marked in red block ).



~ root is one of the default credential, whick we used to login.

* Submit your flag from flag.txt file to accomplish the machine.