

Report On HackTheBox challenge puzzles:

Introduction:

HackTheBox is an online platform which polishes your pen-testing skills with different challenges, it provides a walkthrough for most labs and after reading the walkthrough you can take on different challenges for that lab.

Pre-requisites: For you to complete these challenges, you need to have kali-Linux running on your machine. That can be done in many ways but the way I found it most easy was to install oracle virtual box and install kali linux on the virtual box.

Getting Started:

After getting Kali-Linux up and running on your machine, you need to open the Mozilla Firefox browser provided with the kali-linux machine that you just installed and go to <https://www.hackthebox.eu> . This will take you to the home page of the official HackTheBox platform.

After that you have to establish a connection between your Linux machine and the platform,

To do that we have to click on the “connect-to-HTB” button on the top right corner and choose Open-vpn , this will download a file with the same name as our user-name on this platform and with the .ovpn extension. After that we have to open our terminal on our Linux machine and open the directory in which the .ovpn file is downloaded i.e the Downloads directory. Once we are in the downloads directory we have to run the following command:

```
sudo openvpn starting_point_yourusername.ovpn
```

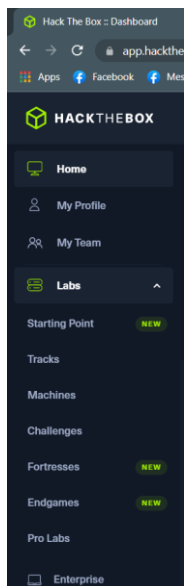
This will connect our linux machine to the HackTheBox platform and we are good to go!

Lets get hacking!!

Solving The First Challenge:

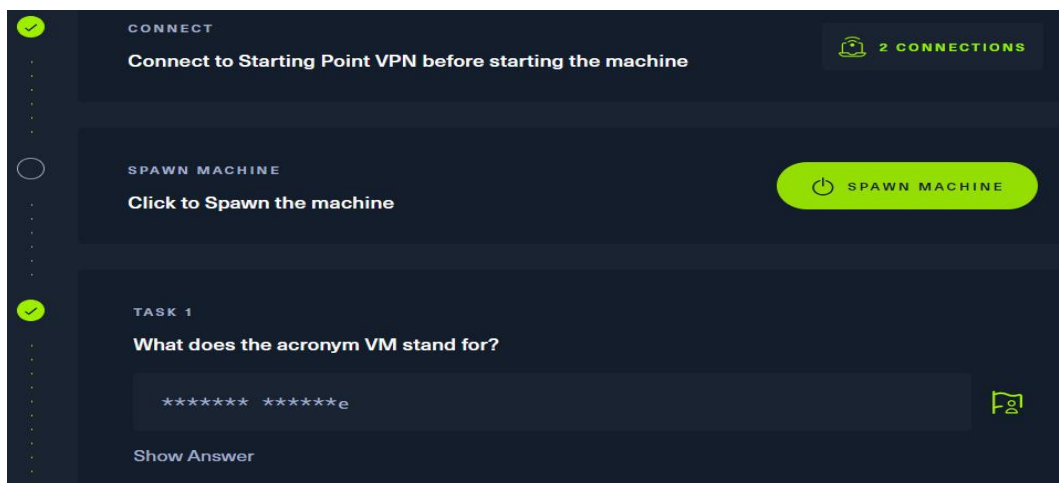
To solve each challenge we have to spawn a said “vulnerable” virtual machine on the platform and hack it.

After you are on the homepage, click on the “Labs” section on the left, and a sub-menu will open

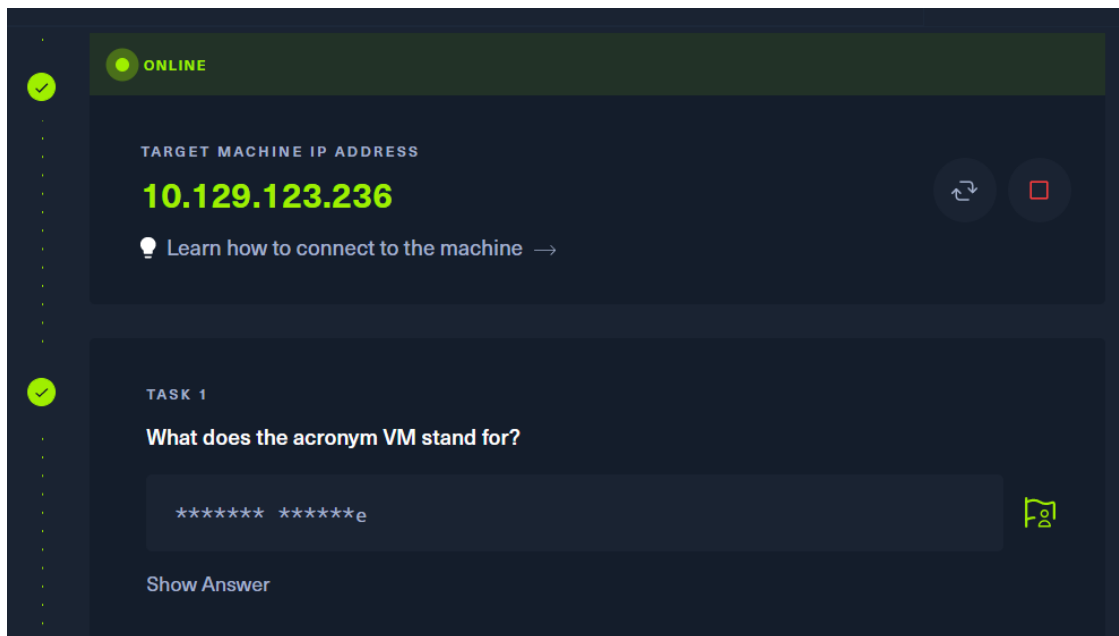


From that sub-menu, click on Starting-point, and scroll down to see the different challenges, each challenge has 9 tasks, and we have to solve all of them to complete the challenge.

The first challenge is called “Meow”, in which we have to spawn a machine called meow.

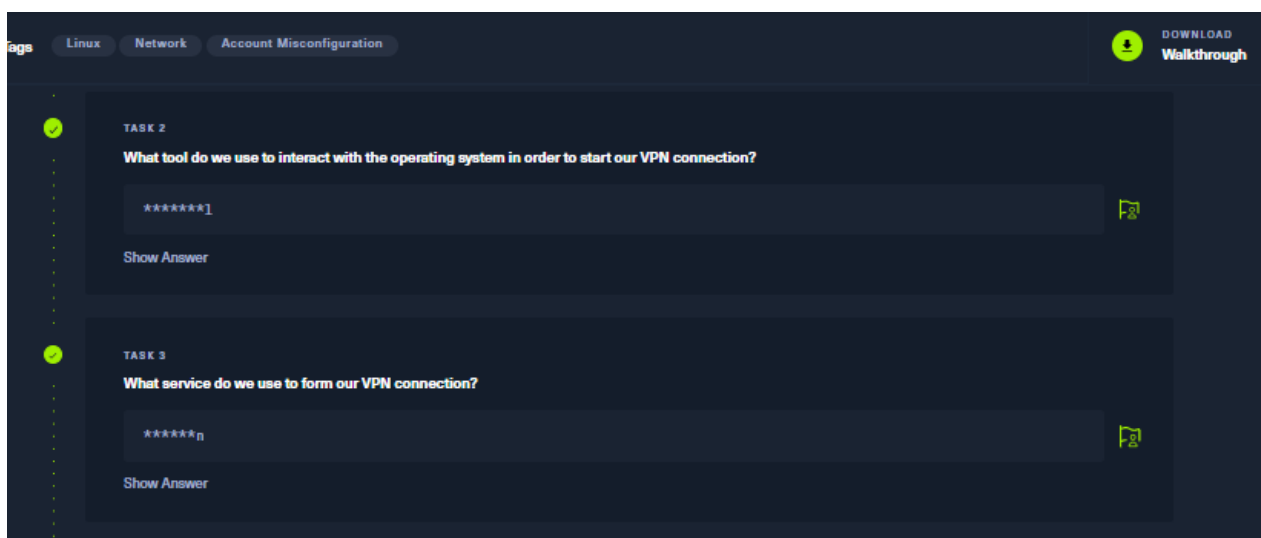


After we've spawned the machine it will give us its ip address through which we can connect with the machine, (which we'll do while solving the tasks).



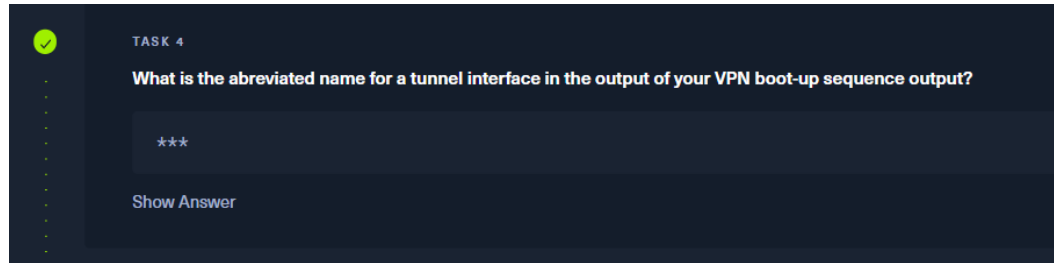
Task 1) As you can see the first task is to answer a simple question: **“What does the acronym VM stand for”**. As we’ve read the walkthrough pdf so we know that it stands for “Virtual machine”, we’ll type that in and submit the answer, and if we are correct, it will show a “green check” on the task. (as we’ve already solved it, you can see the green check.)

Task 2) “What tool do we user to interact with the operating system to start our vpn connection?”



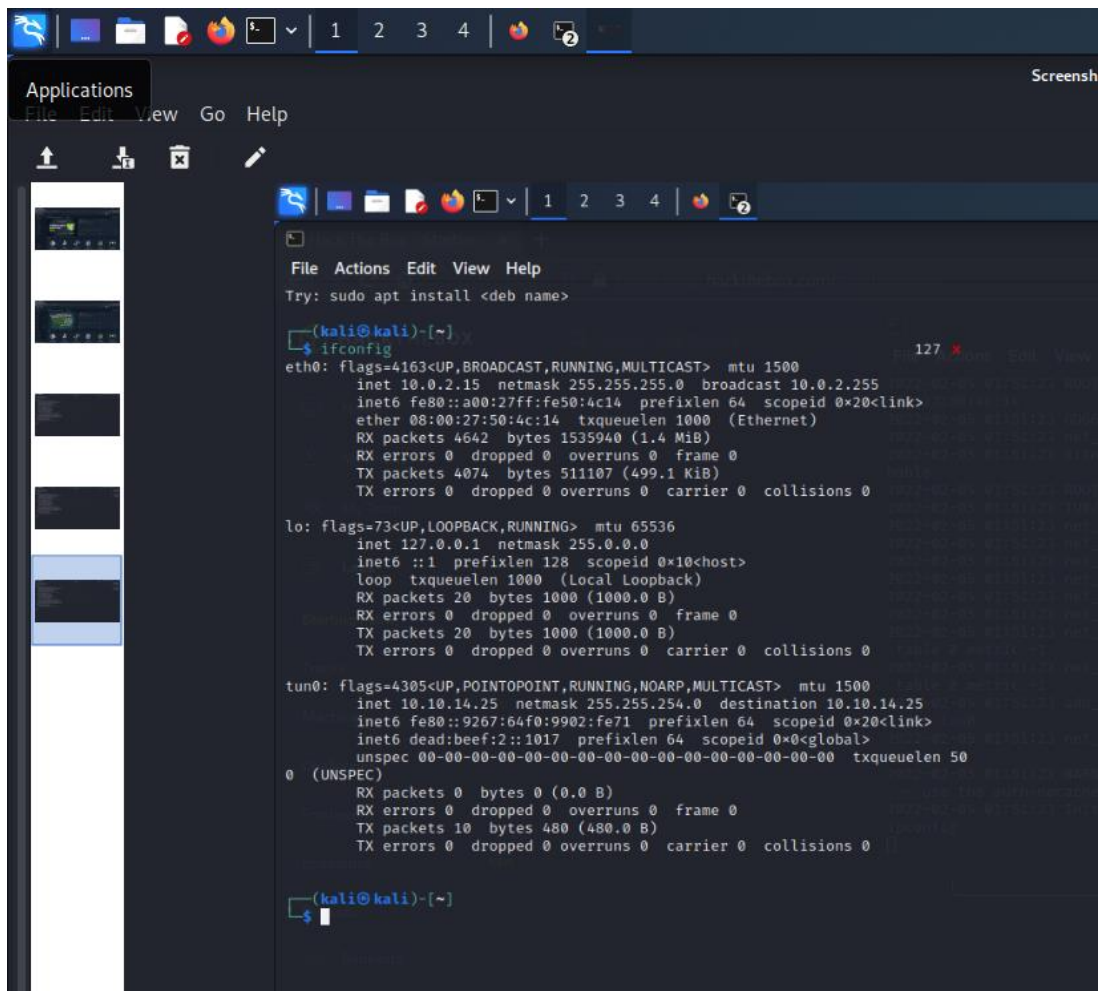
As we saw in the “Getting started” section, the tool we used to establish our vpn connection to the platform was our linux terminal, so the answer to this task is “Terminal”.

Task 3) “What service do we use to form our vpn connection?” : We’ve seen this too in our getting started section, the service that we used to form our vpn connection was “openVpn”. So we’ll type that in and as you can see, theres already a green check, so we are ready to move on the next task.



Task 4) “What is the abbreviated name for a tunnel interface in the output of your vpn boot-up sequence output?”

To answer this task, we have to open our linux terminal and run the command “ifconfig”



```
File Actions Edit View Help
Try: sudo apt install <deb name>

(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe50:4c14 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:50:4c:14 txqueuelen 1000 (Ethernet)
    RX packets 4642 bytes 1535940 (1.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4074 bytes 511107 (499.1 KiB)
    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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1000 (1000.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1000 (1000.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

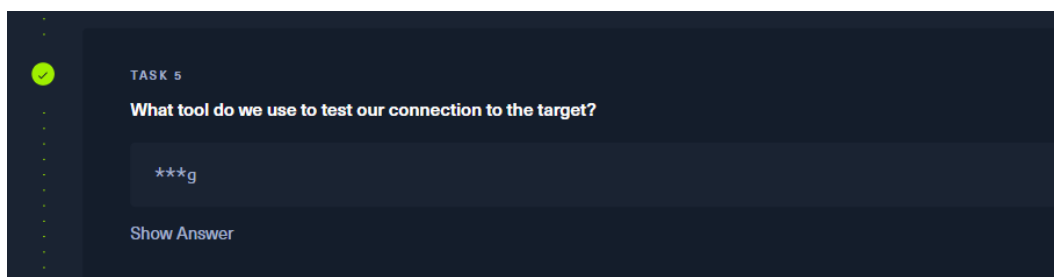
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.14.25 netmask 255.255.254.0 destination 10.10.14.25
    inet6 fe80::9267:64f0:9902:fe71 prefixlen 64 scopeid 0x20<link>
    inet6 dead:beef:2::1017 prefixlen 64 scopeid 0x0<global>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 50
    0 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$
```

As we can see in the second last section of our output, it shows tun0, which is short for tunnel.

It shows that we are tunneling our connection to the target machine, as you can see the target machine IP address in the tun0 section.

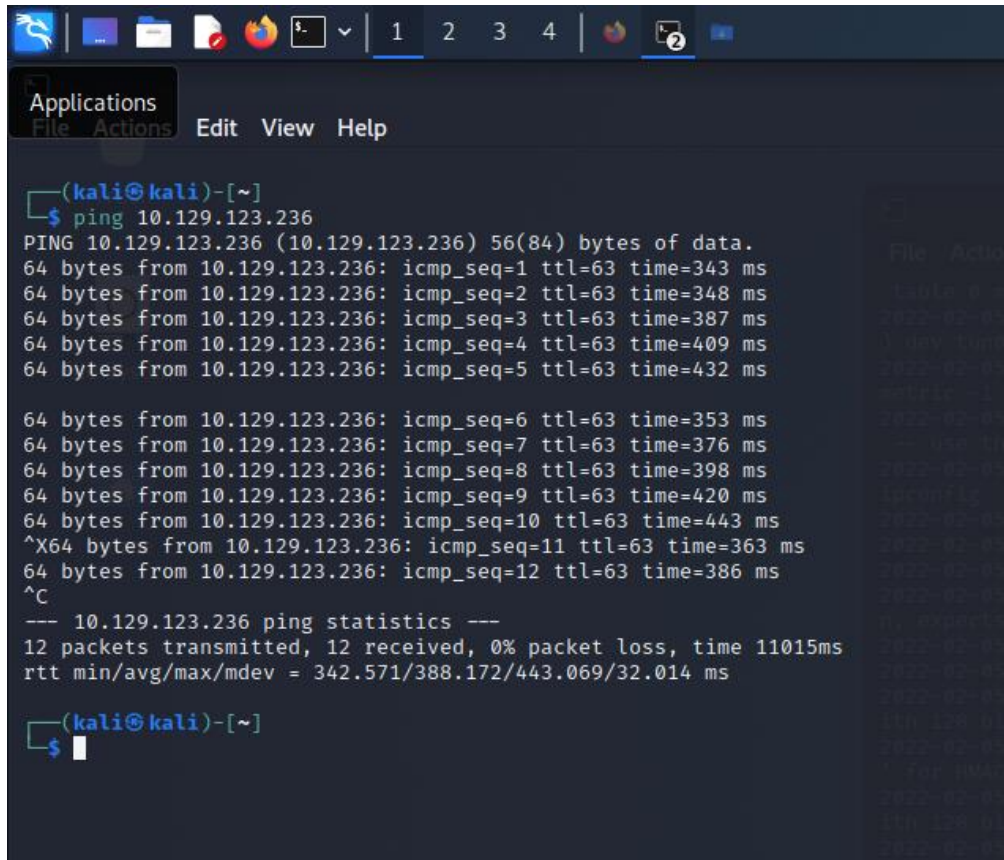
So, we'll type in "tun" as our answer and we've got the good green check.



Task 5) "what task command do we use to test our connection to the target?"

As we are no new to networking, we already know the popular command to test our connection to the target called “ping” command. Lets test this out:

we’ll type ping followed by the ip address of our target machine in our linux terminal:

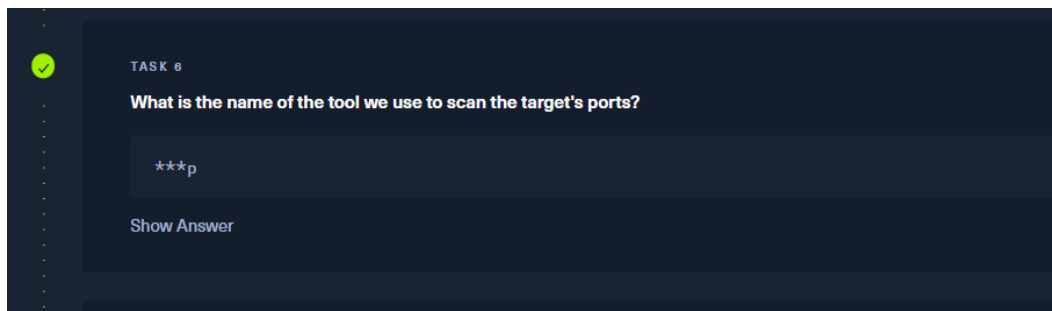


```
(kali@kali)-[~]
$ ping 10.129.123.236
PING 10.129.123.236 (10.129.123.236) 56(84) bytes of data.
64 bytes from 10.129.123.236: icmp_seq=1 ttl=63 time=343 ms
64 bytes from 10.129.123.236: icmp_seq=2 ttl=63 time=348 ms
64 bytes from 10.129.123.236: icmp_seq=3 ttl=63 time=387 ms
64 bytes from 10.129.123.236: icmp_seq=4 ttl=63 time=409 ms
64 bytes from 10.129.123.236: icmp_seq=5 ttl=63 time=432 ms

64 bytes from 10.129.123.236: icmp_seq=6 ttl=63 time=353 ms
64 bytes from 10.129.123.236: icmp_seq=7 ttl=63 time=376 ms
64 bytes from 10.129.123.236: icmp_seq=8 ttl=63 time=398 ms
64 bytes from 10.129.123.236: icmp_seq=9 ttl=63 time=420 ms
64 bytes from 10.129.123.236: icmp_seq=10 ttl=63 time=443 ms
^X64 bytes from 10.129.123.236: icmp_seq=11 ttl=63 time=363 ms
64 bytes from 10.129.123.236: icmp_seq=12 ttl=63 time=386 ms
^C
--- 10.129.123.236 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11015ms
rtt min/avg/max/mdev = 342.571/388.172/443.069/32.014 ms

(kali@kali)-[~]
$
```

As we can see that it works just llike we expected, we’ll type ping as our answer to this task and after doing this we’ve got another green check to our name, lets move on to the next one.



Task 6) “What is the name of the tool we use to scan the target’s ports?”

As we've learned by reading the walkthrough , Network mapper (NMap), is a tool to scan which ports are open on the target machine. lets scan the ports of our target machine with the nmap command.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ nmap 10.129.123.236
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-05 04:14 EST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 19.26% done; ETC: 04:15 (0:00:46 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 29.36% done; ETC: 04:15 (0:00:34 remaining)
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 64.96% done; ETC: 04:15 (0:00:11 remaining)
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 90.96% done; ETC: 04:15 (0:00:03 remaining)
Nmap scan report for 10.129.123.236 (10.129.123.236)
Host is up (0.30s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 31.39 seconds
(kali@kali)-[~]
$
(kali@kali)-[~]
$
```

In the highlighted section, we can see that it doesn't bother to show us the closed ports right now, and shows us the port that's open, namely 23/tcp port and the service that the said port is running, namely telnet.

As we saw the nmap command in action, we'll type in "nmap" as the answer to this question and as the good ol' green check indicates, we are good to move onto the next task.

✓

TASK 7

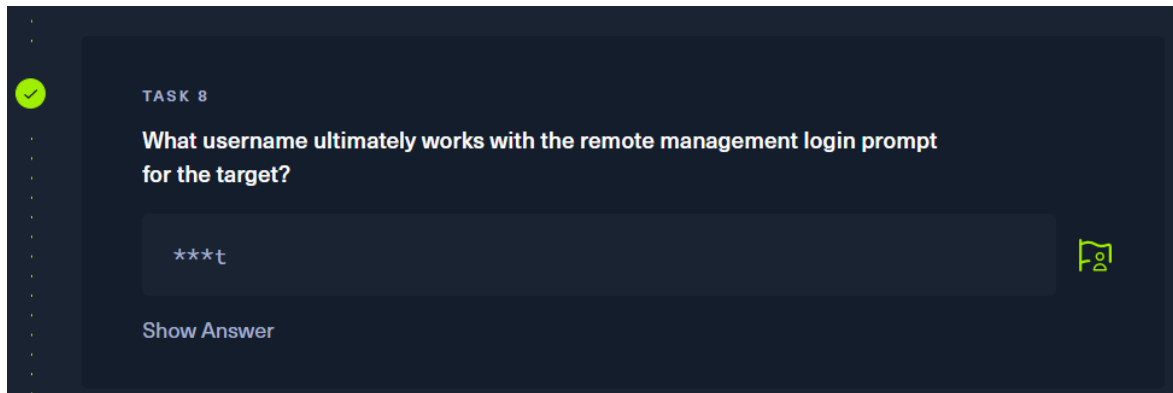
What service do we identify on port 23/tcp during our scans?

*****t

Show Answer

Task 7) What service do we identify on port 23/tcp during our scans

As we've learning from **Task 6**, the service that we identified on port 23/tcp was telnet, which is a service that lets us connect to our target host remotely. So we'll type in "telnet" as our answer to this question aaaand you guesed it! The green check, our friend, is there once again, two more to go, so we'll move onto the next one.



Task 8) “What username ultimately works with remote management login prompt for the target?”

We know that we use the telnet command to connect to a target host, and when we do, we are asked to login to the host machine, as we know that by default theres an account on every Linux machine called “root” which is the super user meaning it as all the access rights there are.


```
root@Meow: ~
File Actions Edit View Help
2022-02-05 04:07:30 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
(kali㉿kali)-[~]
$ telnet 10.129.123.236
Trying 10.129.123.236... remote_host_ip=10.129.123.236
Connected to 10.129.123.236.
Escape character is '^]'.
2022-02-05 04:07:30 ROUTER: default_gateway=UNDEF
Meow login:
Password:
Login incorrect
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

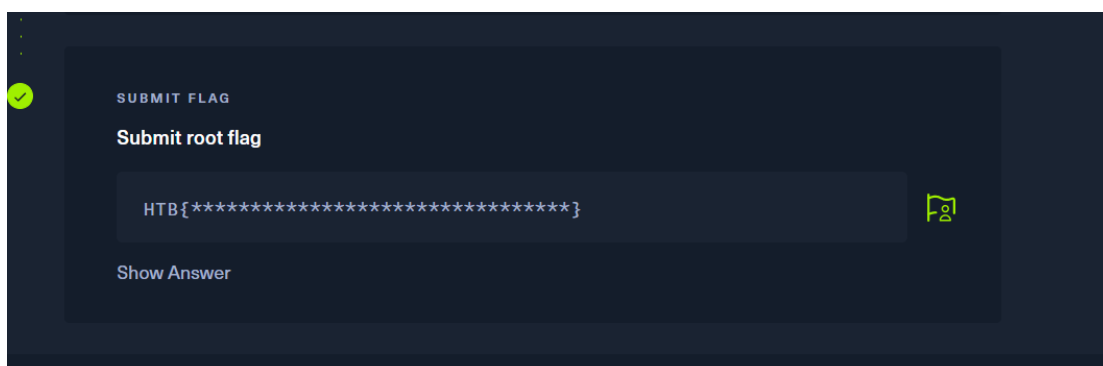
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat 05 Feb 2022 09:30:03 AM UTC

System load: 0.0
```

As you can see that we put root in the login prompt and got successfully logged in.

So we'll put root in as the answer and claim our second last green check.



Task 9) In the last task we are asked to submit a flag, we know that using telnet we can access our remot host, so we'll look for the flag on the target machine that we logged in to using the root account.

We know that the “ls” command shows us the available files on a machine,so we'll type that in the target machines terminal and see if we can find anything.

```
root@Meow: ~  
File Actions Edit View Help  
root@Meow:~# ls  
flag.txt snap  
root@Meow:~#
```

We can see that there is a file called flag, so we'll try and read this file using the cat command.

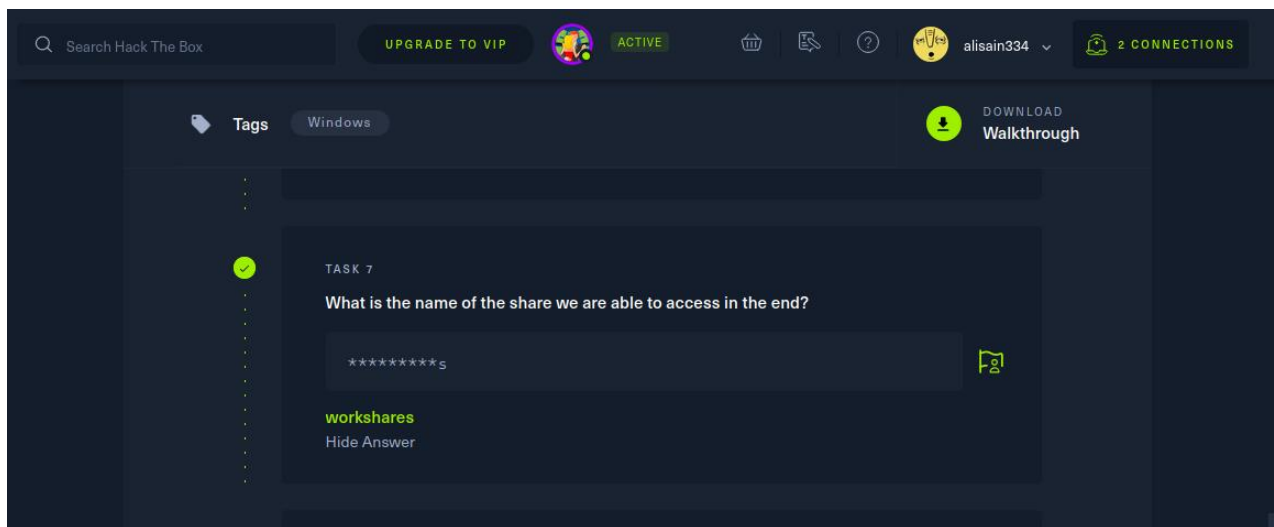
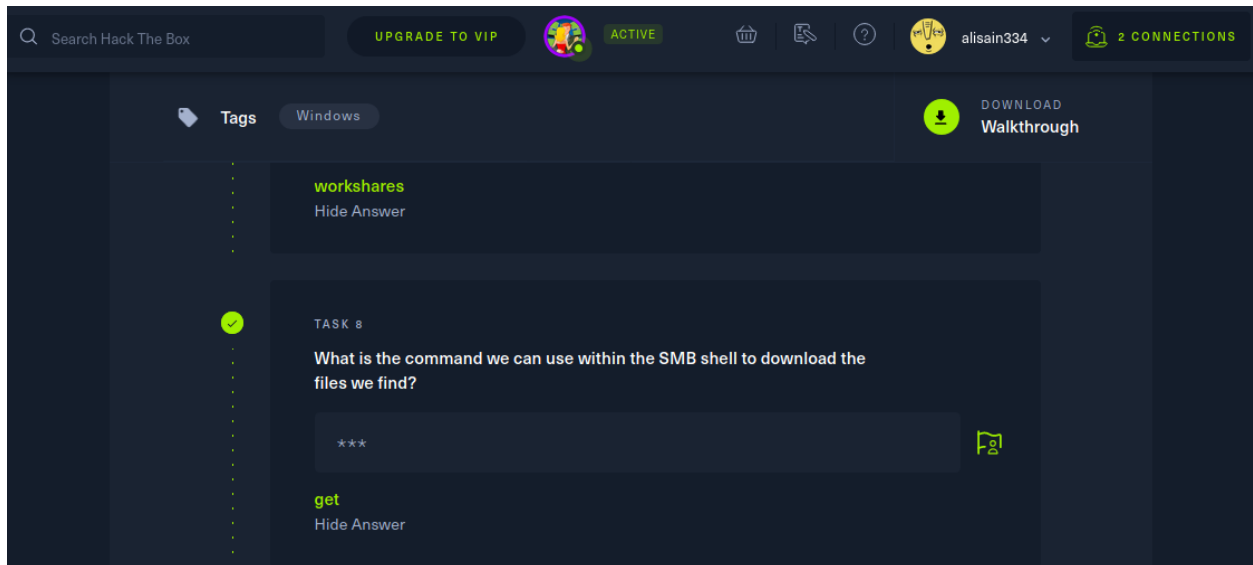
```
root@Meow: ~  
File Actions Edit View Help  
root@Meow:~# ls  
flag.txt snap  
root@Meow:~# cat flag.txt  
b40abdfе23665f766f9c61ecba8a4c19  
root@Meow:~#
```

As you can see we've got the flag, we'll copy this flag and paste it into the answer box in the format that it shows, which such as HTB{b40abdfе23665f766f9c61ecba8a4c19} and as you can see in the screen shot with the question, we've got the last remaining flag, and with this, we have completed this challenge.



“For each challenge we are given a walkthrough pdf, which educates us about the coming challenge and how we can solve it, as you saw how we solved the first challenge, all the other challenges can be completed in the similar way by applying our knowledge that we got from the walkthrough and our knowledge of linux.”

Screenshots for second challenge:



Search Hack The Box

UPGRADE TO VIP

ACTIVE

alisain334

2 CONNECTIONS

Tags

Windows

DOWNLOAD Walkthrough

smbclient

Hide Answer

TASK 6

What is the 'flag' or 'switch' we can use with the SMB tool to 'list' the contents of the share?

Hide Answer

Search Hack The Box

UPGRADE TO VIP

ACTIVE

alisain334

2 CONNECTIONS

Tags

Windows

DOWNLOAD Walkthrough

microsoft-ds

Hide Answer

TASK 5

What is the tool we use to connect to SMB shares from our Linux distribution?

*****t

Hide Answer

smbclient

Hide Answer

Search Hack The Box

UPGRADE TO VIP

ACTIVE

alisain334

2 CONNECTIONS

Tags

Windows

DOWNLOAD Walkthrough

client-server model

Hide Answer

TASK 4

What is the service name for port 445 that came up in our nmap scan?

*****-s

Hide Answer

microsoft-ds

Hide Answer

