

MEOW MACHINE RESOLUTION

INTRODUCTION

Ok, this is my first machine solved in hackthebox, it is worth mentioning that I already have some experience in the world of hacking but I had never dealt with this website which, by the way, is quite interesting, intuitive and very dynamic.

The starting point begins with "Meow", an extremely simple machine for you to enter and familiarize yourself with the world of hacking.

Without further ado, let's begin.

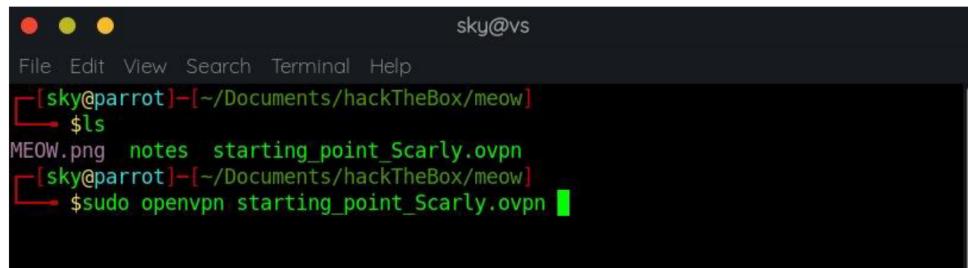
RESOLUTION

Machine itself.

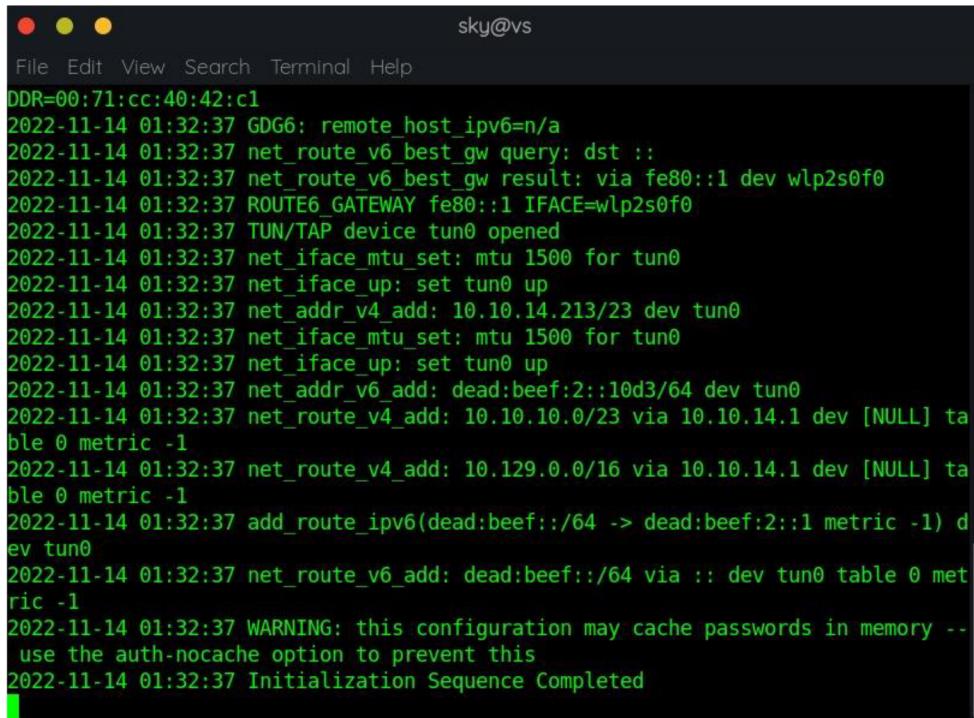
The screenshot shows the HackTheBox platform interface. On the left is a sidebar with navigation links: Home, My Profile, My Team, Labs, Rankings, Battlegrounds, Academy, Careers, Universities, Enterprise, Customer Support, and a version number v 3.18.0. The main content area displays a machine card for "Meow" (Very Easy). The card includes a profile picture of a cat, the machine name "Meow", its difficulty level "VERY EASY", and a "Machine Pwned" status indicator. Below the card are tabs for Tags (Enumeration, Telnet, External, Penetration Tester Level 1), a "SOFT RESET" button, and "Reset Machine" and "Walkthrough" links. A large "CONNECT" button at the bottom prompts the user to "Connect to Starting Point VPN before starting the machine". Below this are two options: "OVPN" (Download your files and connect from your own environment) and "PWNBOX" (A preconfigured, browser-based virtual machine). A note states "Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access".

STEPS

1. Ok so it's really simple. First we have to download the VPN of our choice and save it in a comfortable place within our Linux.
2. We got to connect to it via "openvpn" command to the downloaded VPN

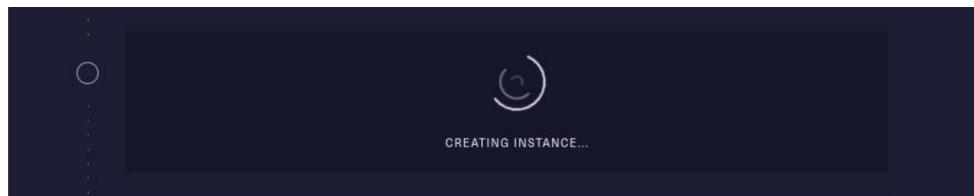


```
sky@vs
File Edit View Search Terminal Help
[sky@parrot]~[~/Documents/hackTheBox/meow]
└─$ls
MEOW.png notes starting_point_Scarly.ovpn
[sky@parrot]~[~/Documents/hackTheBox/meow]
└─$sudo openvpn starting_point_Scarly.ovpn
```

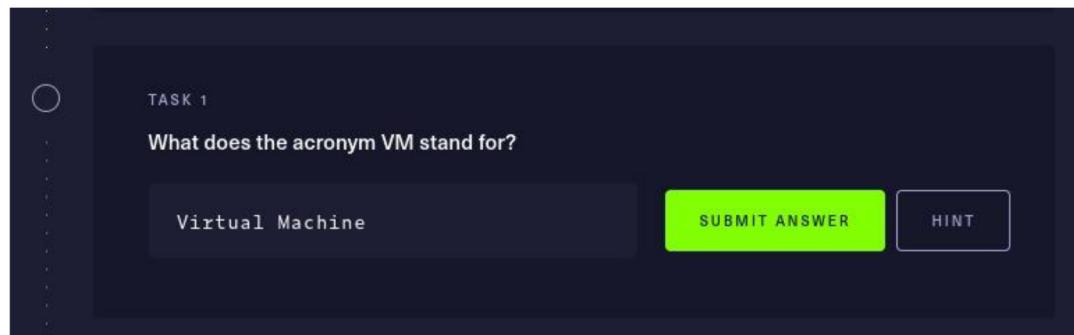


```
sky@vs
File Edit View Search Terminal Help
DDR=00:71:cc:40:42:c1
2022-11-14 01:32:37 GDG6: remote_host_ipv6=n/a
2022-11-14 01:32:37 net_route_v6_best_gw query: dst ::
2022-11-14 01:32:37 net_route_v6_best_gw result: via fe80::1 dev wlp2s0f0
2022-11-14 01:32:37 ROUTE6_GATEWAY fe80::1 IFACE=wlp2s0f0
2022-11-14 01:32:37 TUN/TAP device tun0 opened
2022-11-14 01:32:37 net_iface_mtu_set: mtu 1500 for tun0
2022-11-14 01:32:37 net_iface_up: set tun0 up
2022-11-14 01:32:37 net_addr_v4_add: 10.10.14.213/23 dev tun0
2022-11-14 01:32:37 net_iface_mtu_set: mtu 1500 for tun0
2022-11-14 01:32:37 net_iface_up: set tun0 up
2022-11-14 01:32:37 net_addr_v6_add: dead:beef::10d3/64 dev tun0
2022-11-14 01:32:37 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-11-14 01:32:37 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2022-11-14 01:32:37 add_route_ip6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2022-11-14 01:32:37 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2022-11-14 01:32:37 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2022-11-14 01:32:37 Initialization Sequence Completed
```

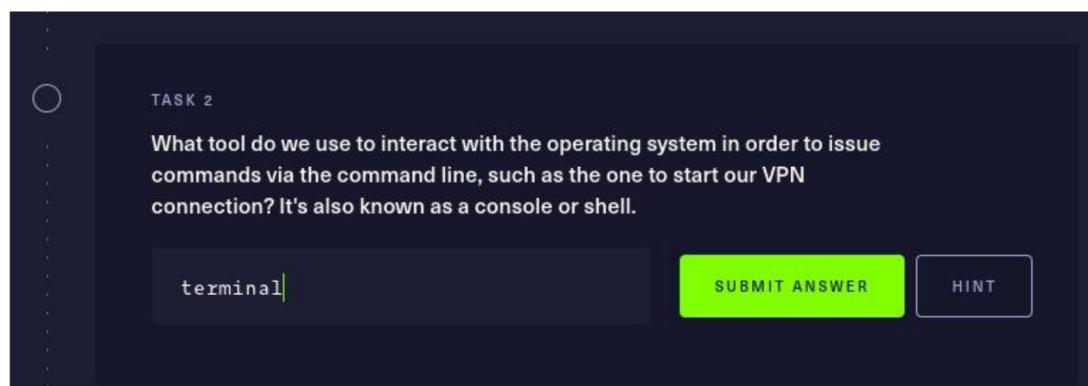
3. We should see this on HackTheBox site.



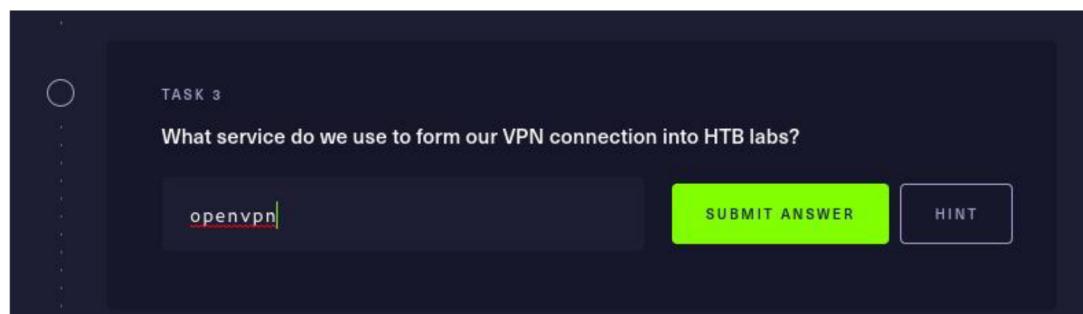
4. Questions section.



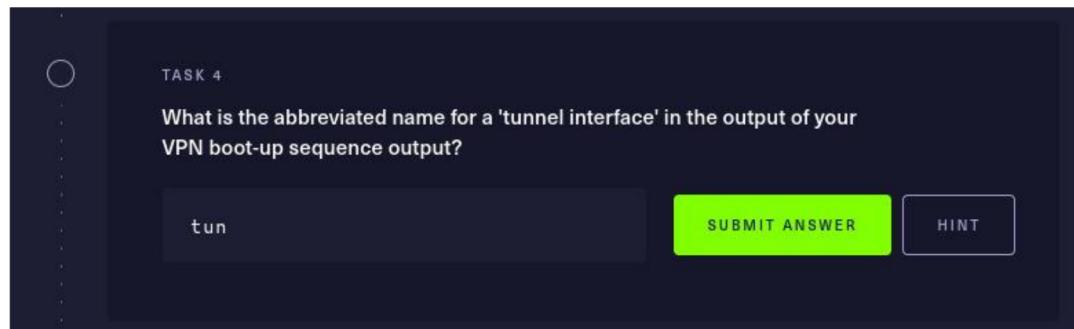
A screenshot of a digital interface for Task 1. It features a dark-themed card with a circular progress indicator on the left. The card is titled "TASK 1". Inside, a question asks, "What does the acronym VM stand for?". Below the question is a text input field containing the answer "Virtual Machine". To the right of the input field are two buttons: a green "SUBMIT ANSWER" button and a white "HINT" button.



A screenshot of a digital interface for Task 2. It features a dark-themed card with a circular progress indicator on the left. The card is titled "TASK 2". Inside, a question asks, "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.". Below the question is a text input field containing the answer "terminal". To the right of the input field are two buttons: a green "SUBMIT ANSWER" button and a white "HINT" button.



A screenshot of a digital interface for Task 3. It features a dark-themed card with a circular progress indicator on the left. The card is titled "TASK 3". Inside, a question asks, "What service do we use to form our VPN connection into HTB labs?". Below the question is a text input field containing the answer "openvpn". To the right of the input field are two buttons: a green "SUBMIT ANSWER" button and a white "HINT" button.



A screenshot of a digital interface for Task 4. It features a dark-themed card with a circular progress indicator on the left. The card is titled "TASK 4". Inside, a question asks, "What is the abbreviated name for a 'tunnel interface' in the output of your VPN boot-up sequence output?". Below the question is a text input field containing the answer "tun". To the right of the input field are two buttons: a green "SUBMIT ANSWER" button and a white "HINT" button.

TASK 5

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

ping|

SUBMIT ANSWER **HINT**

TASK 6

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

nmap|

SUBMIT ANSWER **HINT**

TASK 7

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

telnet|

SUBMIT ANSWER **HINT**

TASK 8

What username is able to log into the target over telnet with a blank password?

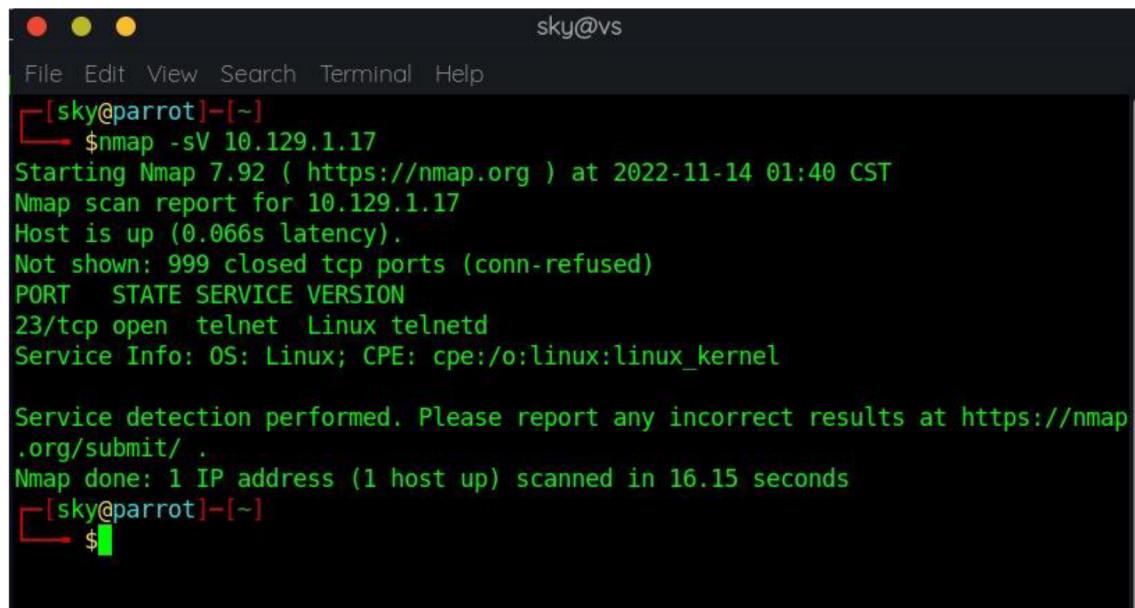
root|

SUBMIT ANSWER **HINT**

5. Simple nmap enumeration for the machine's IP.

6.

Here we are able to see that the PORT 23/tcp is already open, this PORT corresponds to a TELNET service so that leads us to the next step to be able to log into the machine

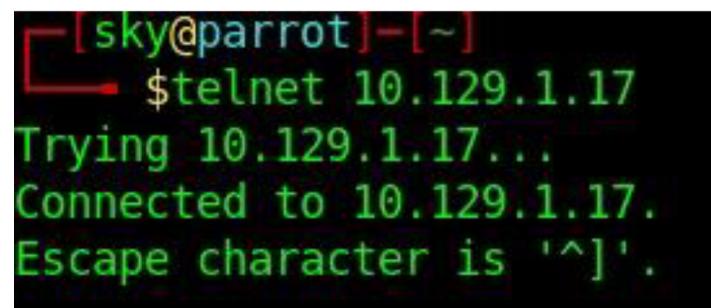


```
sky@vs
File Edit View Search Terminal Help
[sky@parrot]~
└─ $nmap -sV 10.129.1.17
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-14 01:40 CST
Nmap scan report for 10.129.1.17
Host is up (0.066s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.15 seconds
[sky@parrot]~
└─ $
```

7. CONNECTION

With “telnet” command followed by the IP of the machine we can request the connection we are looking for.



```
[sky@parrot]~
└─ $telnet 10.129.1.17
Trying 10.129.1.17...
Connected to 10.129.1.17.
Escape character is '^]'.
```

8. LOG – IN

As the file which is on the page, says. Most common credentials can be:

1. Root
2. Admin
3. Administrator

For this case; that'll be "root"

```
[sky@parrot]~$ telnet 10.129.1.17
Trying 10.129.1.17...
Connected to 10.129.1.17.
Escape character is '^]'.

Hack the Box

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 Mon 14 Nov 2022 07:42:12 AM UTC

System load:          0.0
Usage of /:           41.7% of 7.75GB
Memory usage:         4%
```

9. CAPTURING THE FLAG

Once we are logged in, if we use a "ls", we will be able to see the secret.txt housed in the machine so we will only need "cat" command to that file so we can see the content.

```
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

10. BACK TO THE SITE – FINAL QUESTION

SUBMIT FLAG

Submit root flag

b40abdf... | SUBMIT FLAG

11. COMPLETED

