



OVPN Phase

Started by installing the `.ovpn` file from HTB and transferred the file from my computer to my Kali Linux VM.

I then ran `sudo openvpn starting_point-AliyahMillan.ovpn` to run the vpn.

After that was complete, I am now able to connect to the HTB machine and can begin.

Machine Details

- Target Machine IP Address: `10.129.33.255`
-

Enumeration

NMAP Scan

Nmap is a network mapper. It will tell us what ports are open on the target machine. With that information, we can determine what our next step would be.

Terminal:

```
(adhd@kali)-[~/Desktop/HTB/Notes/Starting Point/1 - Meow]
└─$ sudo nmap -sV 10.129.33.255
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-29 16:16 PDT
Nmap scan report for 10.129.33.255
Host is up (0.099s 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
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 12.17 seconds

Command Breakdown:

- `-sV` : Version Detection; Looks for the version the target machine is running on. Includes version number, service type, OS, hostname, and more.

Key information:

```
PORT      STATE SERVICE VERSION
```

```
23/tcp    open  telnet  Linux telnetd
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Result Breakdown:

- Port 23 is open on the target
 - It's running telnet
- The OS for the target machine is Linux

With this information we know there's no other ports open so we can work on getting a foothold into the telnet that's running on port 23. In order to do that, we need to find credentials.

Foothold

Bruteforce telnet login

Start with accessing telnet:

```
telnet 10.129.33.255
```

Terminal:

```
—(adhd@kali)—[~/Desktop/HTB/Notes/Starting Point/1 - Meow]
└─$ telnet 10.129.33.255
Trying 10.129.33.255...
Connected to 10.129.33.255.
Escape character is '^]'.
```

Hack the Box

Meow login:

We're given a login prompt. I'm going to try basic logins such as admin/admin, administrator/administrator, and root/root.

Successful telnet login - root

Terminal:

```
(adhd@kali)-[~/Desktop/HTB/Notes/Starting Point/1 - Meow]
└─$ telnet 10.129.33.255
Trying 10.129.33.255...
Connected to 10.129.33.255.
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 Mon 29 Jul 2024 11:37:22 PM 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: 10.129.33.255
IPv6 address for eth0: dead:beef::250:56ff:feb0:6c6c
```

* 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
```

```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~#
```

I was able to login to telnet using the user `root`.

The root user is a superuser. They have admin privileges and have the highest access on a system.

Upon logging in, it gives the OS (`Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)`) and the number of users logged in (0).

Since we are now logged into the target, we can poke around some more.

Enumeration pt.2

We can look to see where we are, and what files are there:

Terminal:

```
root@Meow:~# ls
flag.txt  snap
```

We're looking for the flag. In order to read it, we need to `cat` the file.

Terminal:

```
root@Meow:~# cat flag.txt
```

We're then given the flag and have finished the box!

Flag

```
b40abdfе23665f766f9c61ecba8a4c19
```


HTB Tasks

HTB Task 1:

 **What does the acronym VM stand for? >**


```
Virtual Machine
```

HTB Task 2:

 **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. >**

```
Terminal
```

HTB Task 3:

 **What service do we use to form our VPN connection into HTB labs? >**

```
openvpn
```

HTB Task 4:

② What tool do we use to test our connection to the target with an ICMP echo request? >

ping

HTB Task 5:

② What is the name of the most common tool for finding open ports on a target? >

nmap

HTB Task 6:

② What service do we identify on port 23/tcp during our scans? >

telnet

HTB Task 7:

② What username is able to log into the target over telnet with a blank password? >

root

Root Flag

b40abdfе23665f766f9c61ecba8a4c19

#telnet

#protocols

#reconnaissance

#weakcredentials

#misconfiguration