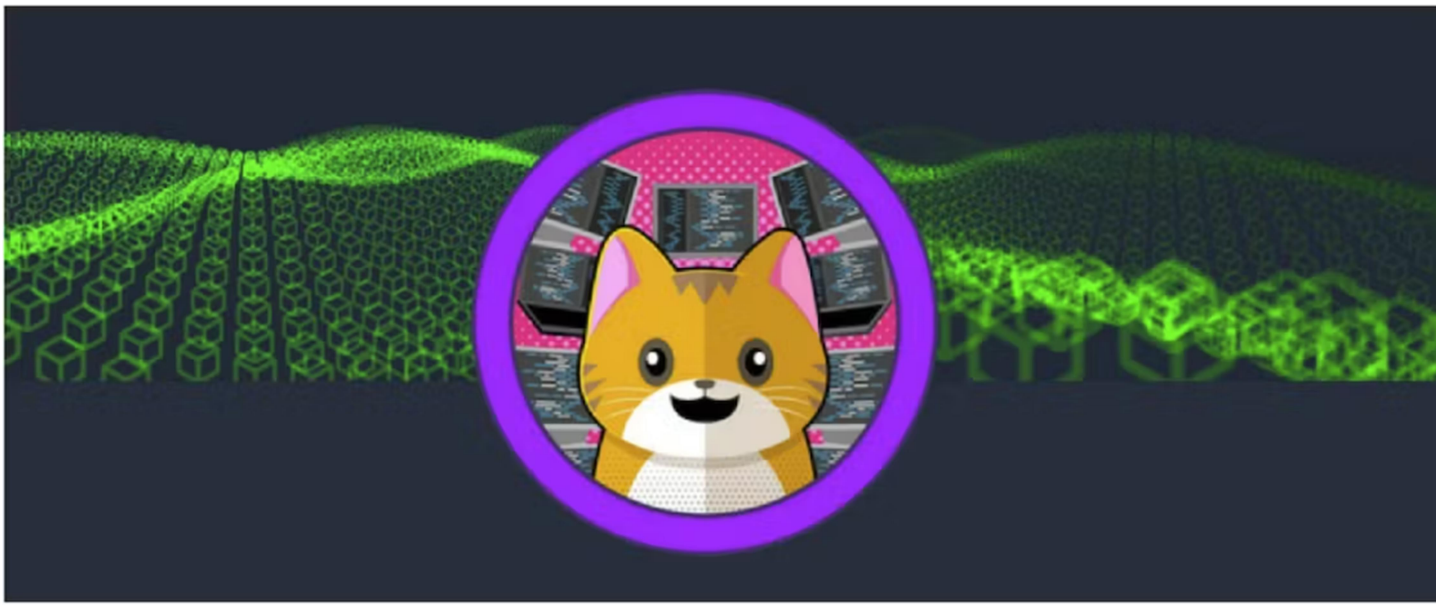
Tier 0 Meow Report

Prepared by: **Chanpreet Kaur**



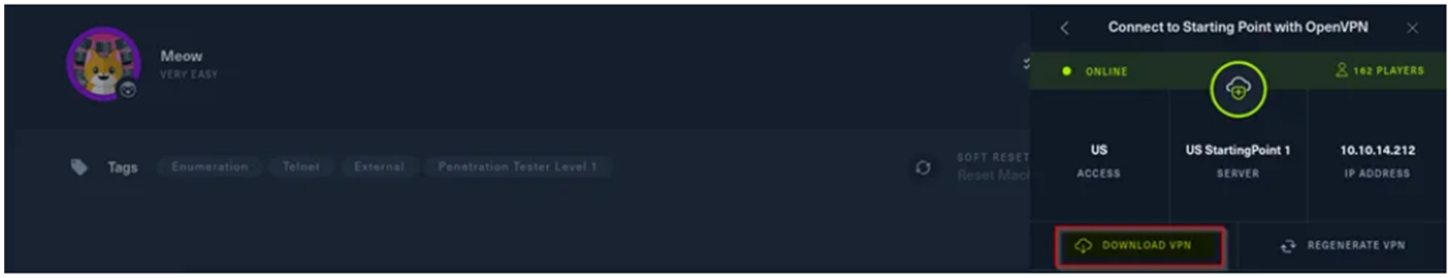
Tools Used

- NMAP

Procedure

I will cover solution steps of the "**Meow**" machine, which is part of the '**Starting Point**' labs and has a difficulty rating of '***Very Easy***'.

Login to Hack the Box portal and navigate to Starting Point's page, where you will be prompted to choose between a PWNBOX or an OVPN (i.e. OpenVPN) connection. A PWNBOX is a pre-configured, browser-based virtual machine and requires a HackTheBox VIP+ membership for unlimited access.



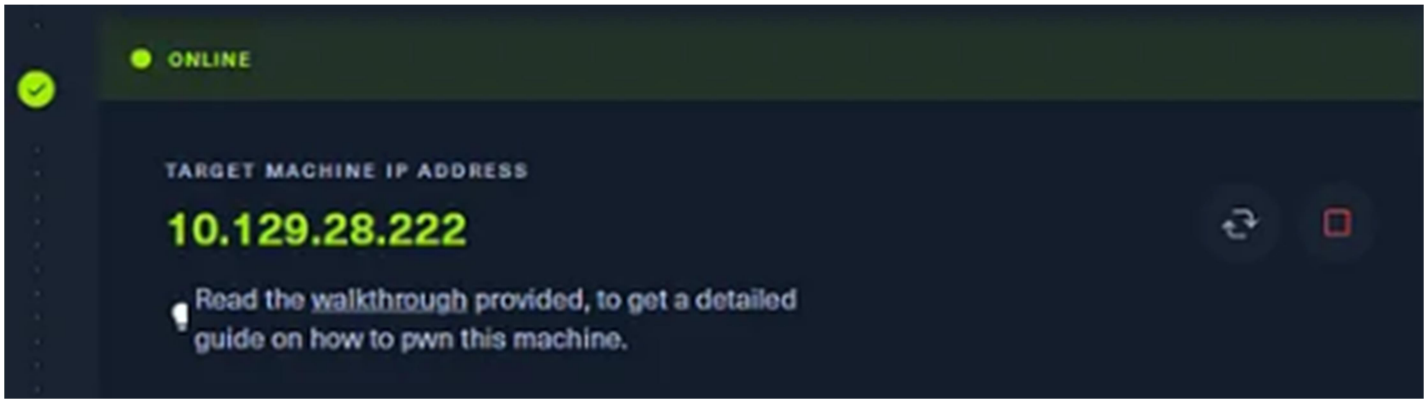
I have used the OVPN method and my Kali Linux machine through VirtualBox. Download the VPN (.ovpn) configuration file and open a terminal window and run below mentioned command –

sudo openvpn [filename].ovpn

([filename] should be replaced with the name of your downloaded .ovpn file for the Starting Point lab.)

Execute this line in the terminal, Now come back to HackTheBox and refresh the page in browser to see the new connection and then we can activate the machine by clicking the '**Spawn Machine**' button.

The machine is now active and showing a target IP address



Now, we have to solve all the available tasks by providing correct inputs, we can also use hints in case we are stuck.

- **What does the acronym VM stand for?**
  virtual machine

- **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

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

- **What is the abbreviated name for a 'tunnel interface' in the output of your VPN boot-up sequence output?**
  tun

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

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

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

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

Key Terms

Virtual Machine

Virtual Machine (VM) is a virtual environment which functions as a virtual computer system with its own CPU, memory, network interface & storage, created on a physical hardware system. Hypervisor separates all the resources of machine from the hardware and provisions them properly so they can be used by the VM. Virtualization technology allows user to share a system with virtual environments.

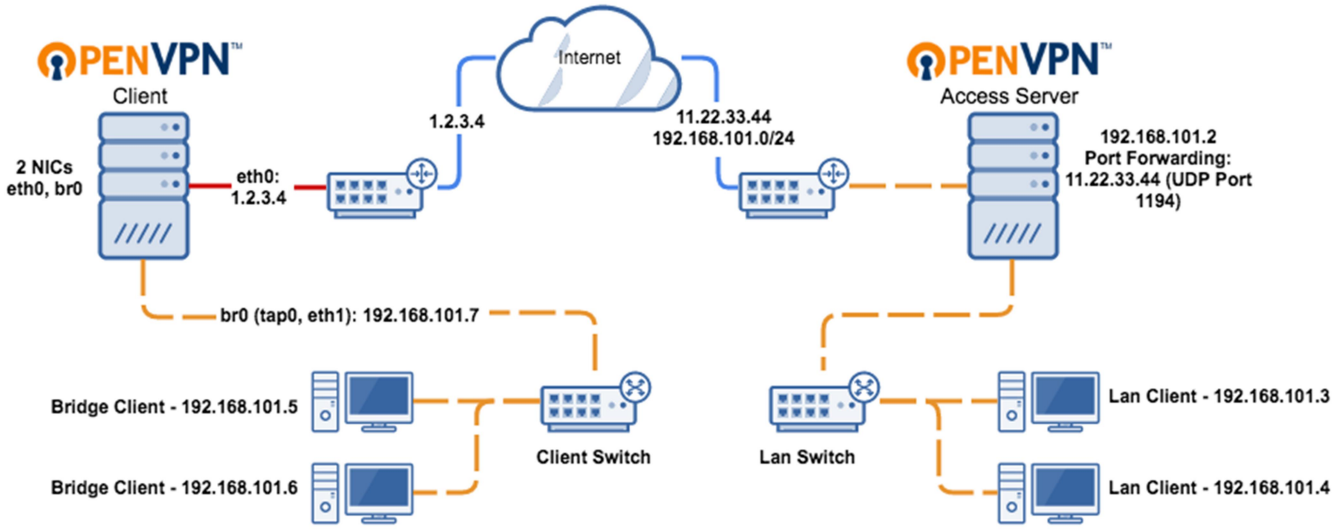
Terminal

Terminal is a text-based interface used to interact with a computer's operating system. It allows users to execute commands, navigate the file system, manage files, run programs, and perform various tasks using text-based commands.

Openvpn

OpenVPN is an open-source software application that creates a secure point-to-point or site-to-site connection in routed or bridged configurations. It uses custom security protocols to establish a secure tunnel for transferring data between devices or networks over the internet.

To use OpenVPN, you typically need a configuration file provided by the VPN service provider. This file contains information like server addresses, encryption settings, and authentication details. Users can then use the OpenVPN software to establish a secure connection to the VPN server by running the OpenVPN client with this configuration file.



Tun

The "tun" refers to a network tunneling interface in Linux and other Unix-like operating systems. Specifically, "tun" interfaces are virtual network kernel devices used for implementing VPNs (Virtual Private Networks) and other tunneling protocols.

When using VPN software like OpenVPN, it often creates a "tun" interface to facilitate the encrypted communication between your device and the VPN server. This interface behaves like a regular network interface but operates at the kernel level to handle encrypted data transfer securely between your device and the VPN server.

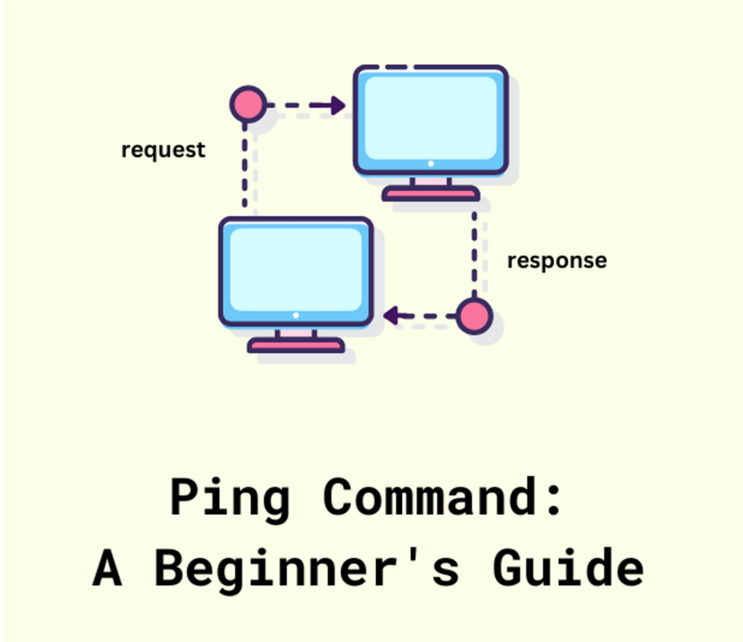
The "tun" interface is responsible for routing packets of data securely over the internet by encapsulating them within a secure tunnel, ensuring privacy and security while transmitting information between different networks or devices.

Ping

"Ping" is a basic networking utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

By sending ICMP (Internet Control Message Protocol) echo request packets to the target host, the "ping" command measures the time it takes for a packet to travel from the source to the destination and back. This allows users to assess the network connectivity and latency between their device and the target host.

In its simplest form, using the "ping" command in a terminal or command prompt involves typing "ping" followed by an IP address or a domain name.

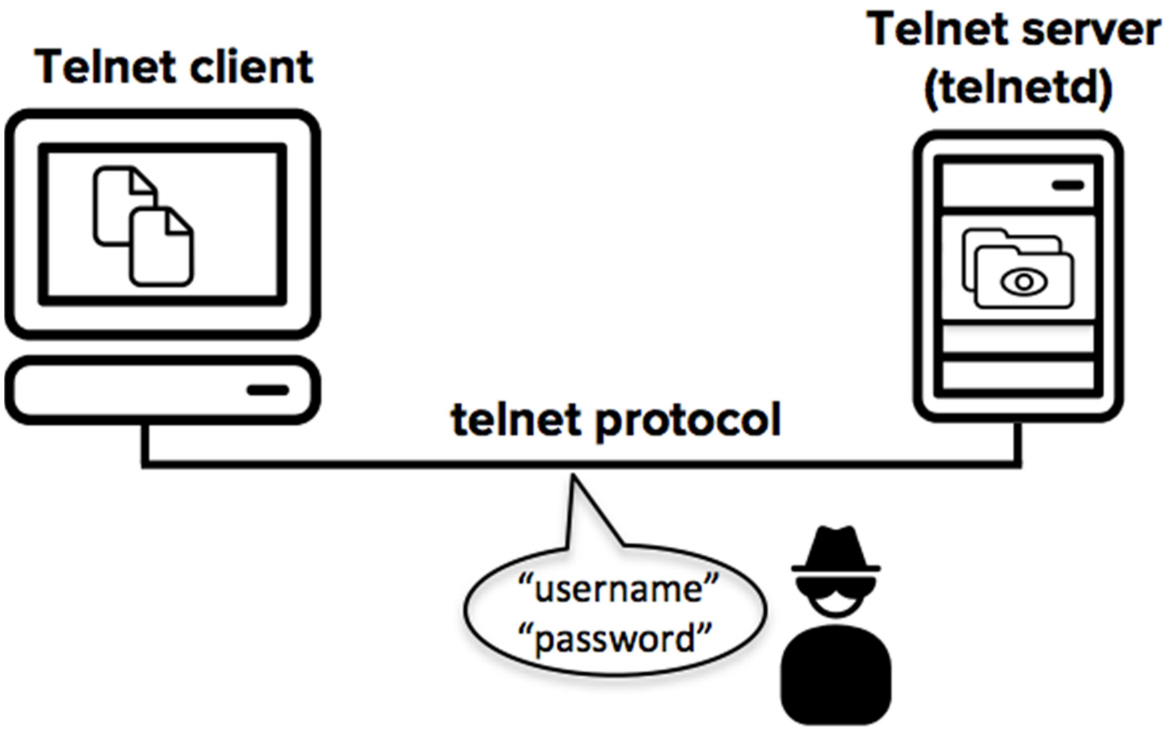


Nmap

Nmap (Network Mapper) is a powerful open-source network scanning tool used for discovering devices and services on a computer network, thus creating a "map" of the network. It's designed to explore networks, perform security assessments, and gather information about hosts and services running on a network.

Telnet

Telnet is a network protocol used on the internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.



Let's get started with the machine. Firstly, let us scan the IP on our machine using nmap:

```
┌──(root㉿kali)-[~]
└─# nmap 10.129.28.222
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 02:11 EDT
Nmap scan report for 10.129.28.222 (10.129.28.222)
Host is up (0.17s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
```

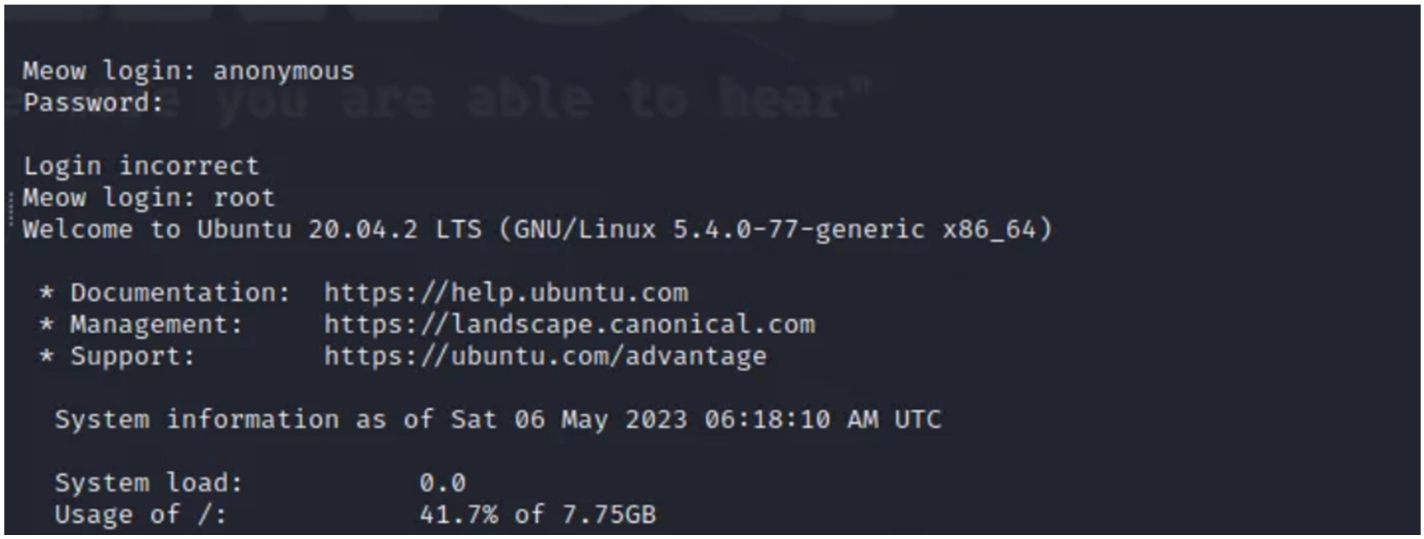
Telnet, as a service, is known to have security vulnerabilities due to its inherent lack of encryption, potential for misconfigurations, and susceptibility to weak passwords. These vulnerabilities make it less secure compared to other communication protocols like SSH, which encrypts data during transmission, reducing the risk of interception or unauthorized access.

It allows anonymous login sometimes, let's try that …

Start first by typing the command:

telnet <IP>

Now we have to input the username to login:



I tried using “anonymous” as we use in ftp to login anonymously. Surprisingly, I found myself in the root shell, which was unexpected because it took me only a few minutes to solve this machine.I was expecting it to be simple, but it is very simple. If you are just starting, then it may be a good start.

After logging in, just “cat” the flag and you are ready to move ahead to the next machine.

```
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:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

Congratulations!! You found your first flag …