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

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."*

Flag

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

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

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

Our flag : b40abdfe23665f766f9c61ecba8a4c19