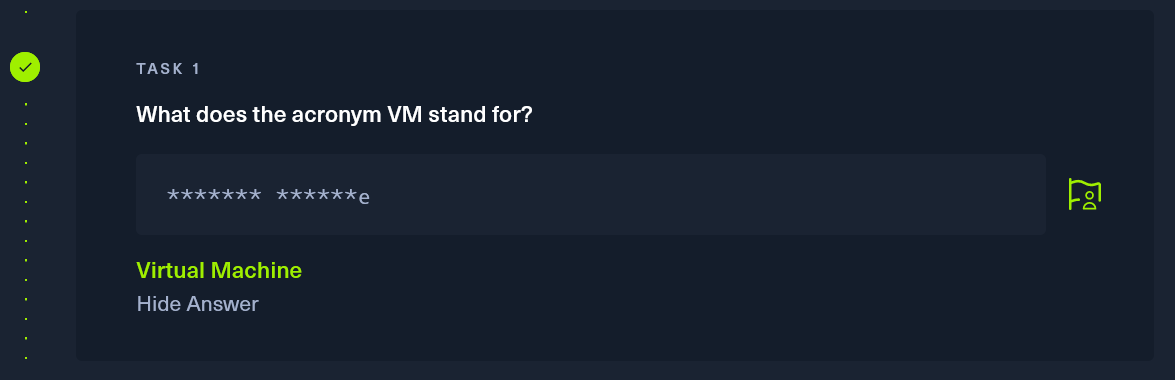
Connect to Starting Point VPN before starting the machine



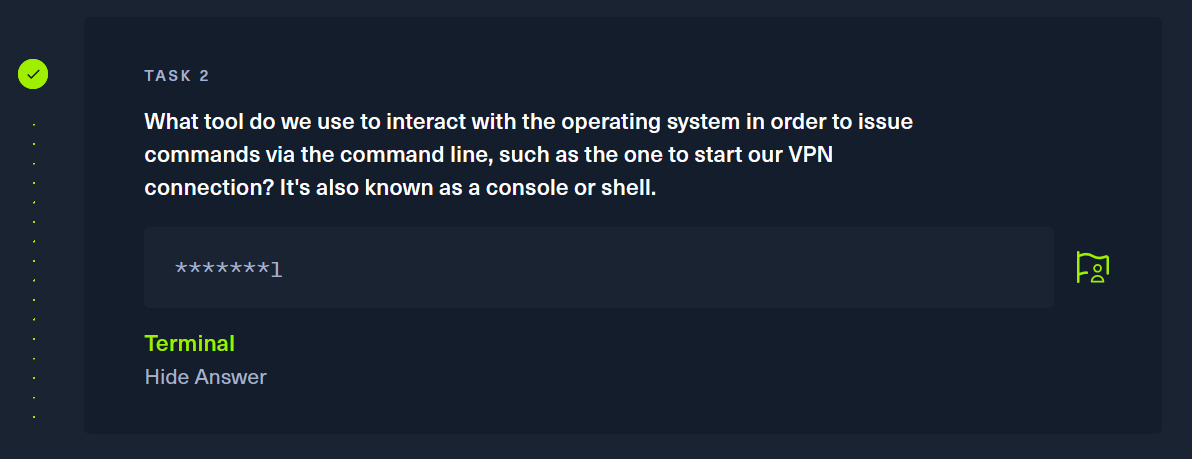
Task 1

What does the acronym VM stand for?



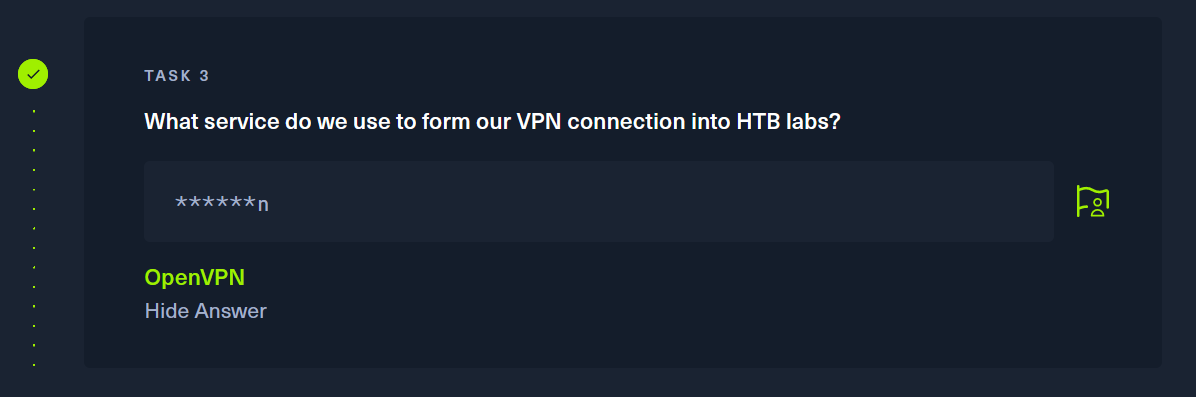
Task 2

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.



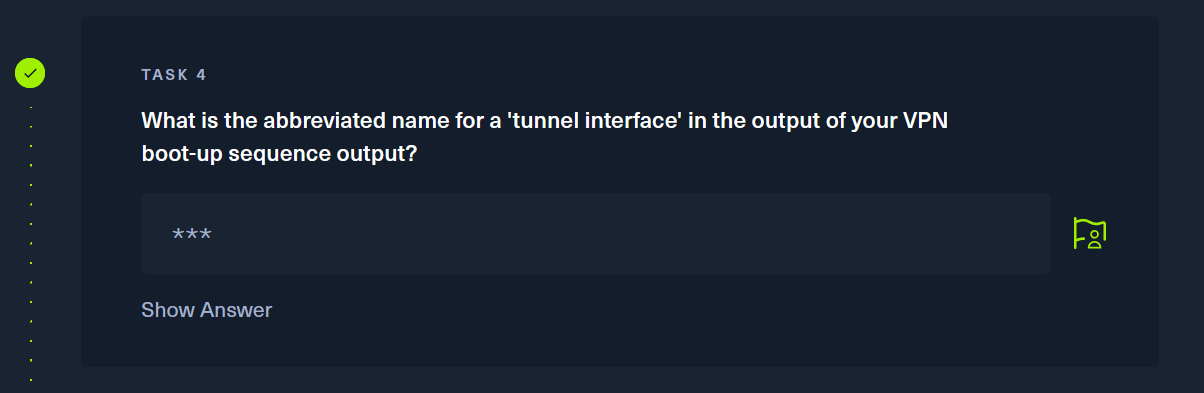
Task 3

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



Task 4

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



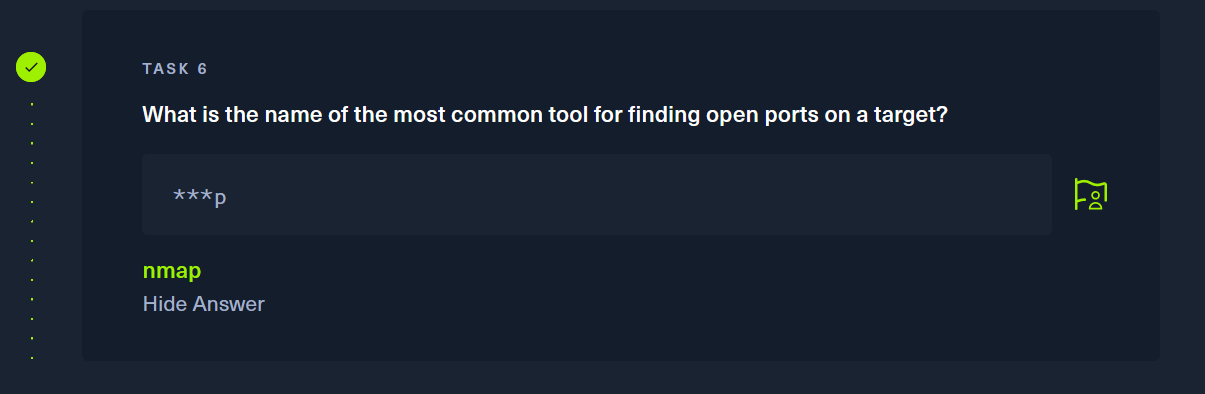
Task 5

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



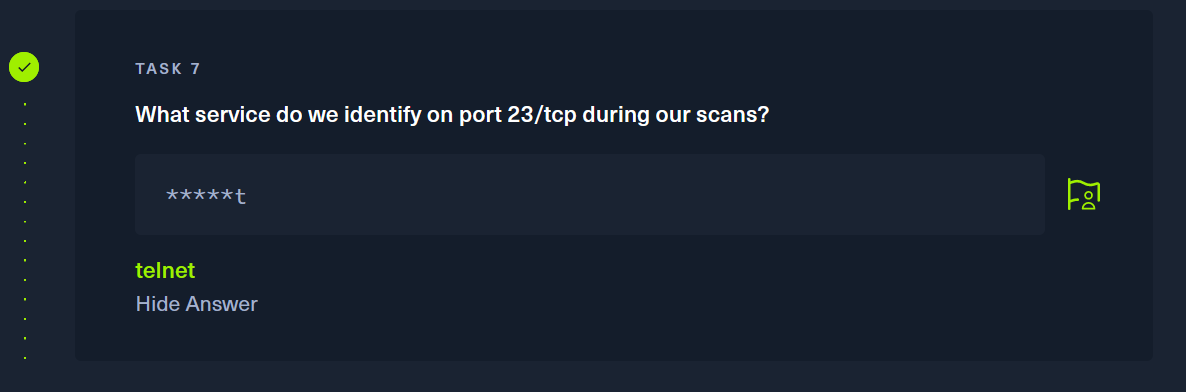
Task 6

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



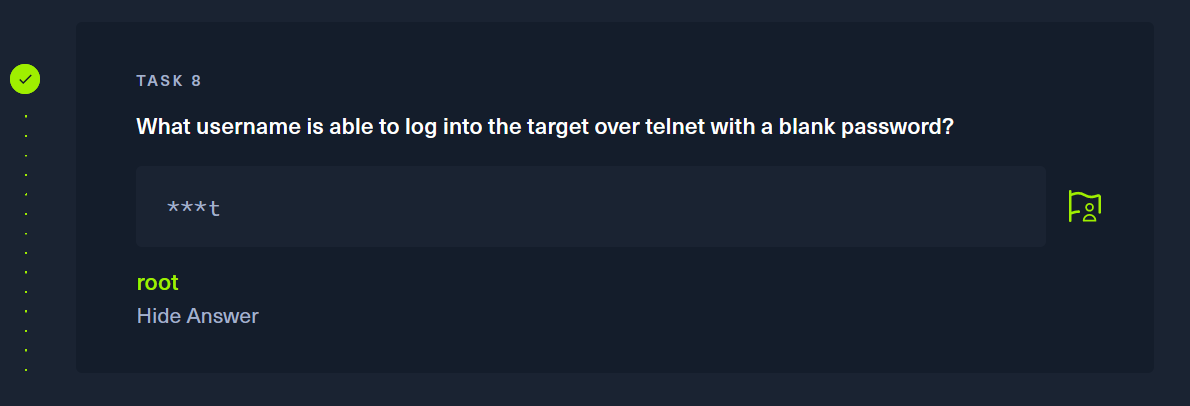
Task 7

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



Task 8

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



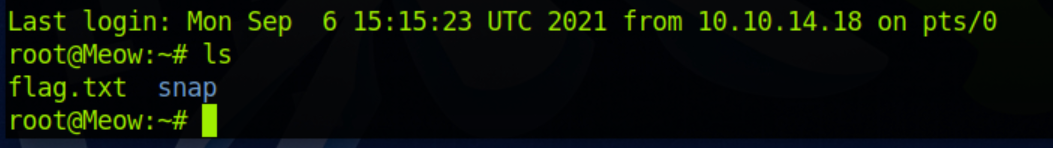
Submit Flag

Submit root flag

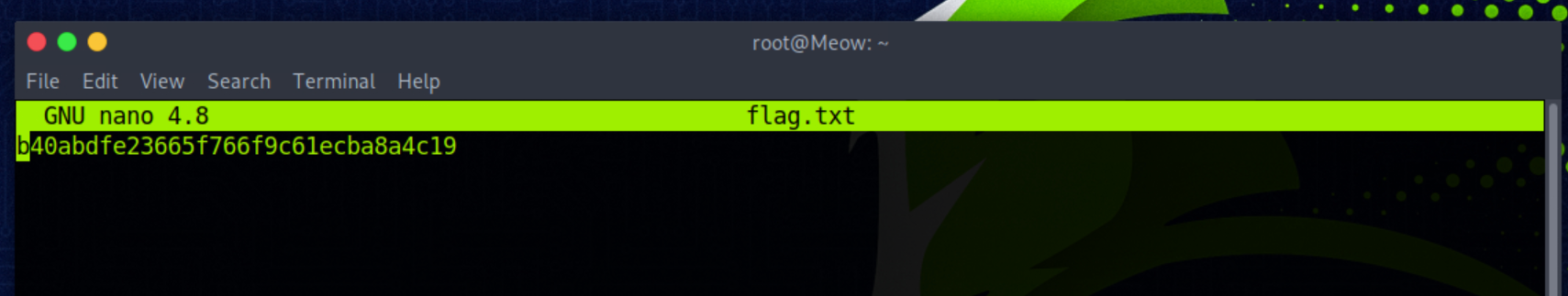
With the answers that we provided in the previous tasks gives us hints to attack the machine. Task 8 says “able to log into the target over telnet with blank password”. So we will attempt to connect to the machine using telnet and assuming the password is root.



The login root allowed us to sign in so lets see if we are able to execute commands and if so lets check the directory.



In the root directory we are able to see a document called flag.txt lets see if we can open that text document using nano.



We have the flag lets go ahead and input that into the submit root flag document.



That flag that we had just submitted was the correct flag to pwn Meow.