

Meow

Hack The Box



Writeup by : kkarinzzz

## Daftar Isi

Task 1.....	3
<i>Flag : Virtual Machine</i> .....	3
Task 2.....	3
<i>Flag : terminal</i> .....	3
Task 3.....	4
<i>Flag : openvpn</i> .....	4
Task 4.....	4
<i>Flag : ping</i> .....	4
Task 5.....	5
<i>Flag : nmap</i> .....	5
Task 6.....	5
<i>Flag : telnet</i> .....	5
Task 7.....	6
<i>Flag : root</i> .....	6
Task 8.....	7
<i>Flag : b40abdfc23665f766f9c61ecba8a4c19</i> .....	8

## Task 1:

What does the acronym VM stand for?

*Flag : Virtual Machine*

The screenshot shows a dark-themed interface for a task. On the left, there's a vertical sidebar with a green checkmark icon at the top. The main area is titled "TASK 1". A question is displayed: "What does the acronym VM stand for?". Below the question is a text input field containing "\*\*\*\*\* \*e". To the right of the input field is a small green icon of a person with a speech bubble. At the bottom of the screen, there's a "Show Answer" button.

## 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.

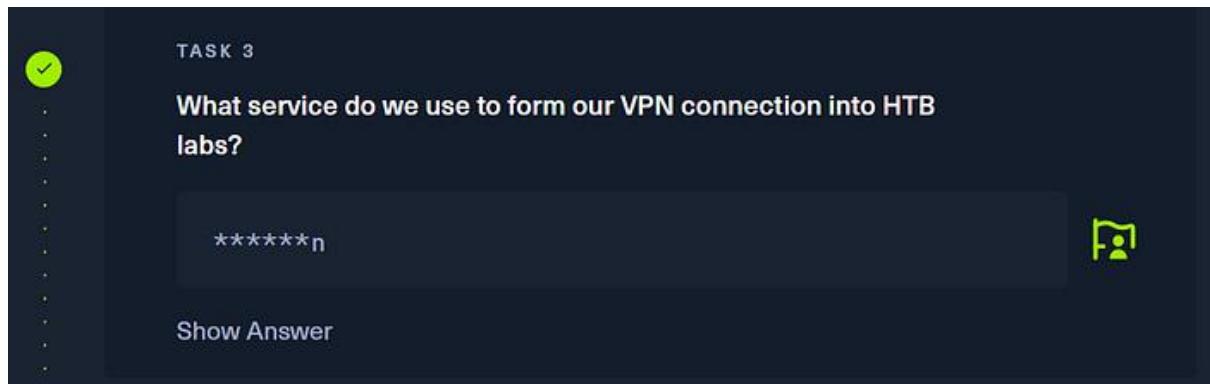
*Flag : terminal*

The screenshot shows a dark-themed interface for a task. On the left, there's a vertical sidebar with a green checkmark icon at the top. The main area is titled "TASK 2". A question is displayed: "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.". Below the question is a text input field containing "\*\*\*\*\*l". To the right of the input field is a small green icon of a person with a speech bubble. At the bottom of the screen, there's a "Show Answer" button.

## Task 3:

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

*Flag: openvpn*

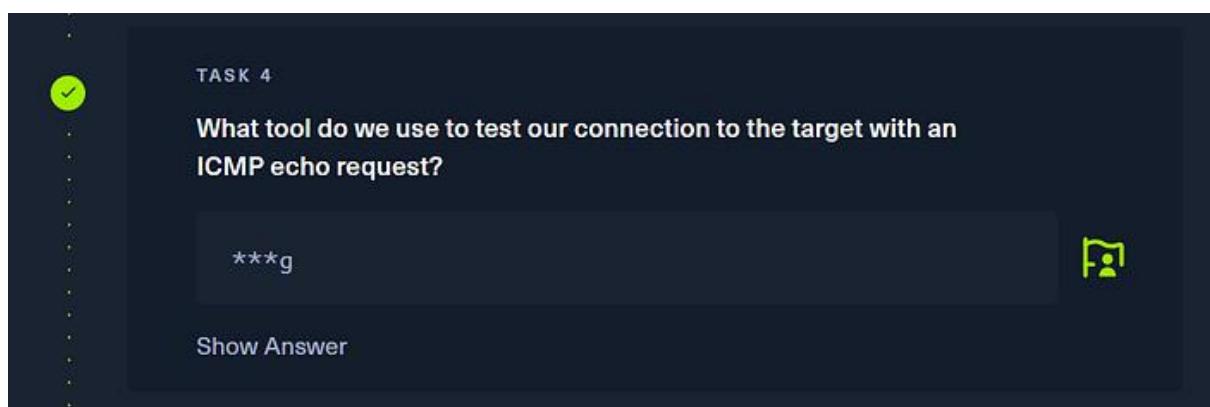


A screenshot of a digital task card titled "TASK 3". The question asks, "What service do we use to form our VPN connection into HTB labs?". A partially obscured answer, "\*\*\*\*\*n", is shown in a text input field. A yellow checkmark icon is visible on the left side of the card.

## Task 4:

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

*Flag: ping*

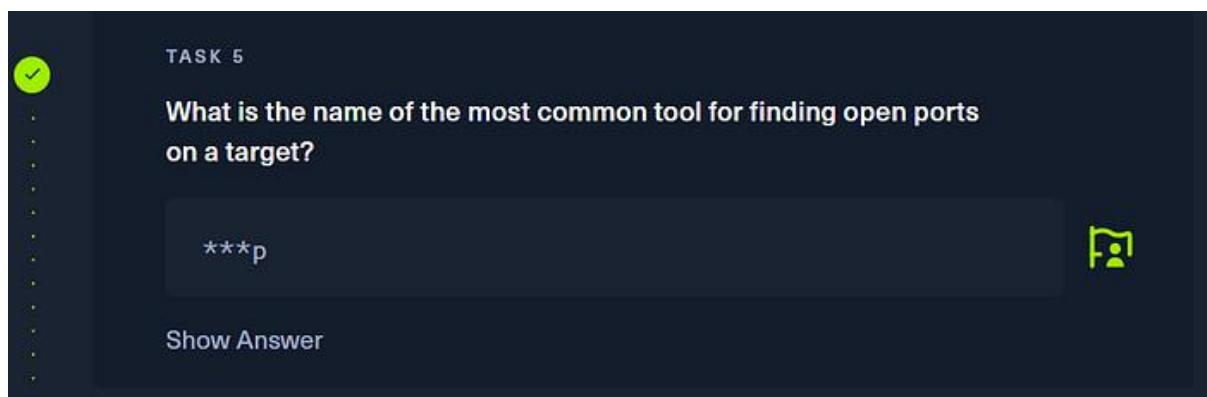


A screenshot of a digital task card titled "TASK 4". The question asks, "What tool do we use to test our connection to the target with an ICMP echo request?". A partially obscured answer, "\*\*\*g", is shown in a text input field. A yellow checkmark icon is visible on the left side of the card.

## Task 5:

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

*Flag : nmap*

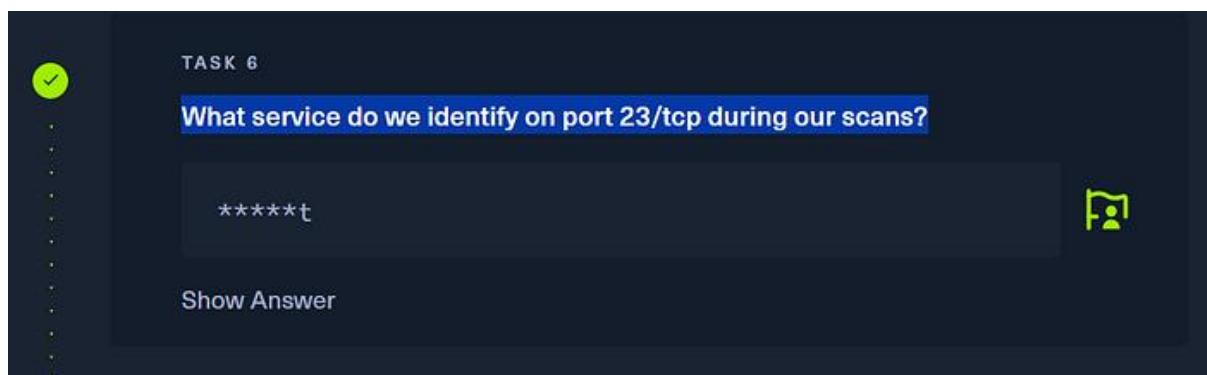


A screenshot of a digital task interface titled "TASK 5". On the left, there is a vertical list of dots. In the center, the question "What is the name of the most common tool for finding open ports on a target?" is displayed. Below the question, a text input field contains the partially typed answer "\*\*\*p". To the right of the input field is a green checkmark icon. At the bottom of the interface, there is a "Show Answer" button.

## Task 6:

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

*Flag : telnet*



A screenshot of a digital task interface titled "TASK 6". On the left, there is a vertical list of dots. In the center, the question "What service do we identify on port 23/tcp during our scans?" is displayed in a blue highlighted box. Below the question, a text input field contains the partially typed answer "\*\*\*\*\*t". To the right of the input field is a green checkmark icon. At the bottom of the interface, there is a "Show Answer" button.

## Task 7:

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

*Flag: root*

The screenshot shows a dark-themed user interface for a task. On the left, there is a vertical sidebar with a green circular icon containing a white checkmark. To its right, the text "TASK 7" is displayed in a small, light-colored font. Below this, a question is presented in a larger, bold, black font: "What username is able to log into the target over telnet with a blank password?". Underneath the question, there is a text input field containing the characters "\*\*\*\*". To the right of this field is a small, light-blue rectangular button featuring a white silhouette of a person's head and shoulders. At the bottom of the interface, there is a light-colored button labeled "Show Answer".

## Task 8:

Submit root flag

Steps:

1. Run nmap to scan ports

*nmap -sC -sV (IP Target)*

```
(kkarinzzz㉿kkarinzzz)~]$ nmap -sC -sV 10.129.76.202
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-12 20:55 +0700
Nmap scan report for 10.129.76.202
Host is up (0.38s 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 746.94 seconds

(kkarinzzz㉿kkarinzzz)~]$
```

There is an open port 23 (telnet)

2. Connect to telnet

*telnet (IP Target)*

Log in using root

```
(kkarinzzz㉿kkarinzzz)-[~]
└─$ telnet 10.129.76.202
Trying 10.129.76.202 ...
Connected to 10.129.76.202.
Escape character is '^]'.
ls

Hack the Box

Meow login: ls
Password:

Login incorrect
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 Mon 12 Jan 2026 02:19:07 PM UTC
```

After logging in, just search for the flag

3. Obtain the flag

*ls*

*cat flag.txt*

```
Last login: Mon Jan 12 13:11:42 UTC 2026 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfc23665f766f9c61ecba8a4c19
root@Meow:~#
```

*Flag: b40abdfc23665f766f9c61ecba8a4c19*