

# Hackthebox writeup

K.S Nandakumar

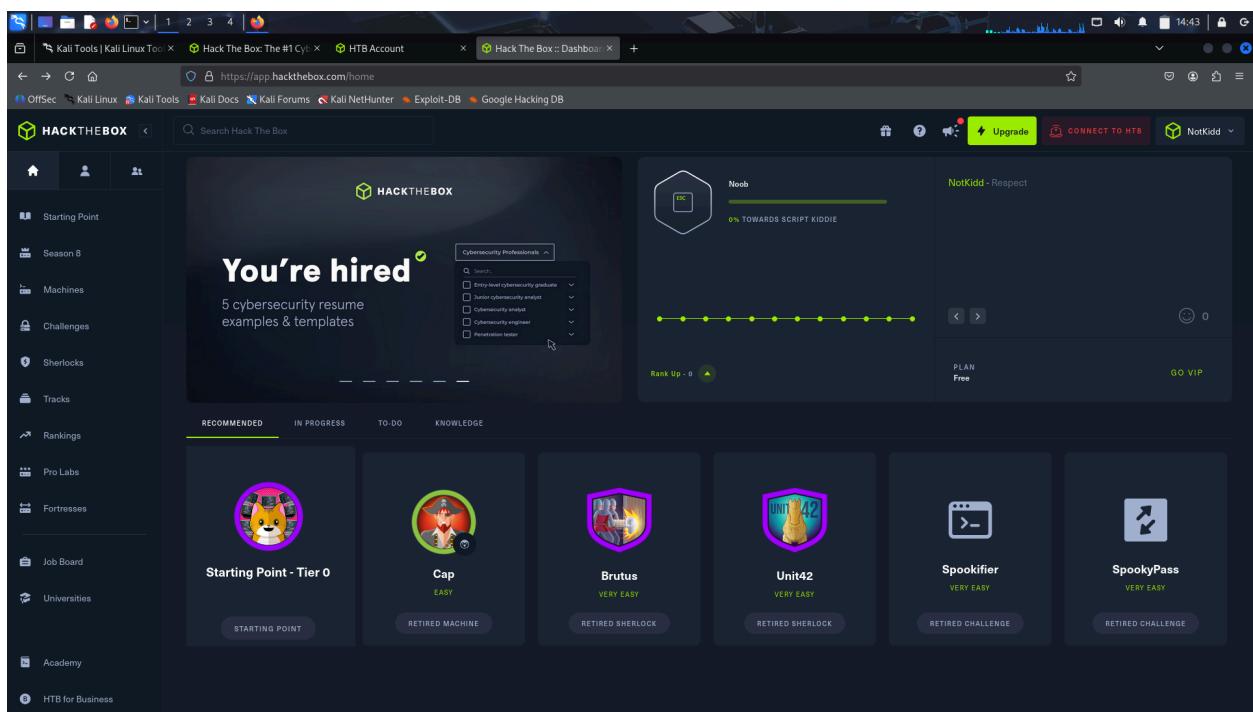
As this is my first CTF, I started with the very easy

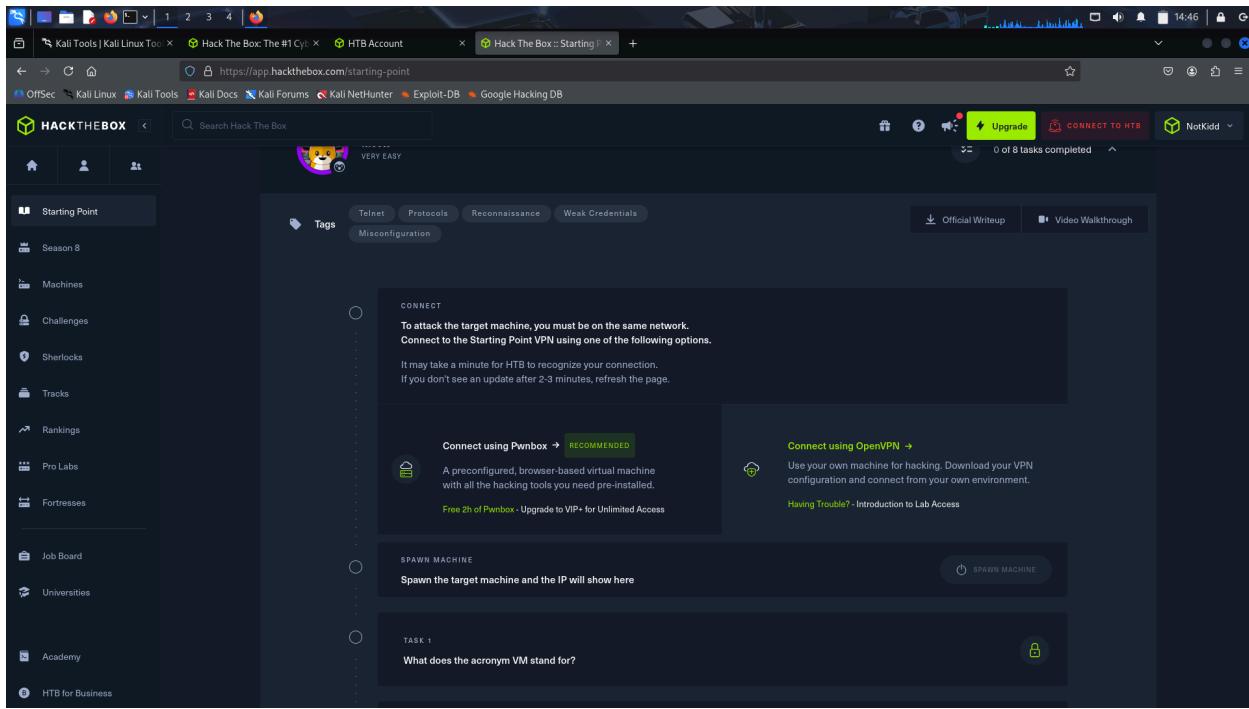
## Tier 0 - The key is a strong foundation

I started by learning how to connect to various services, such as FTP, SMB, Telnet, Rsync, and RDP. Next, I discovered the power of Nmap, a valuable tool for identifying open ports on target systems, allowing me to assess their vulnerabilities.

- I learned how to connect FTP, SMB, Telnet, Rsync and RDP anonymously.
- I learned how to use Nmap to identify open ports.

## Meow





the first challenge i faced was to connect my virtual kali linux via openvpn, and for that the documentation really helped and within 20 minutes I figured out how to get connected and did a ping to confirm.

A screenshot showing three completed tasks on the HackTheBox platform. Task 1 asks 'What does the acronym VM stand for?' with the answer '\*\*\*\*\*e' entered. Task 2 asks '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.' with the answer 'terminal' entered. Task 3 asks 'What service do we use to form our VPN connection into HTB labs?' with the answer 'openvpn' entered. Each task has a green checkmark and a 'Hide Answer' link.

**HIDE ANSWER**

**TASK 4**

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

```
***g
```

**ping**  
**HIDE ANSWER**

**TASK 5**

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

```
***p
```

**nmap**  
**HIDE ANSWER**

**TASK 6**

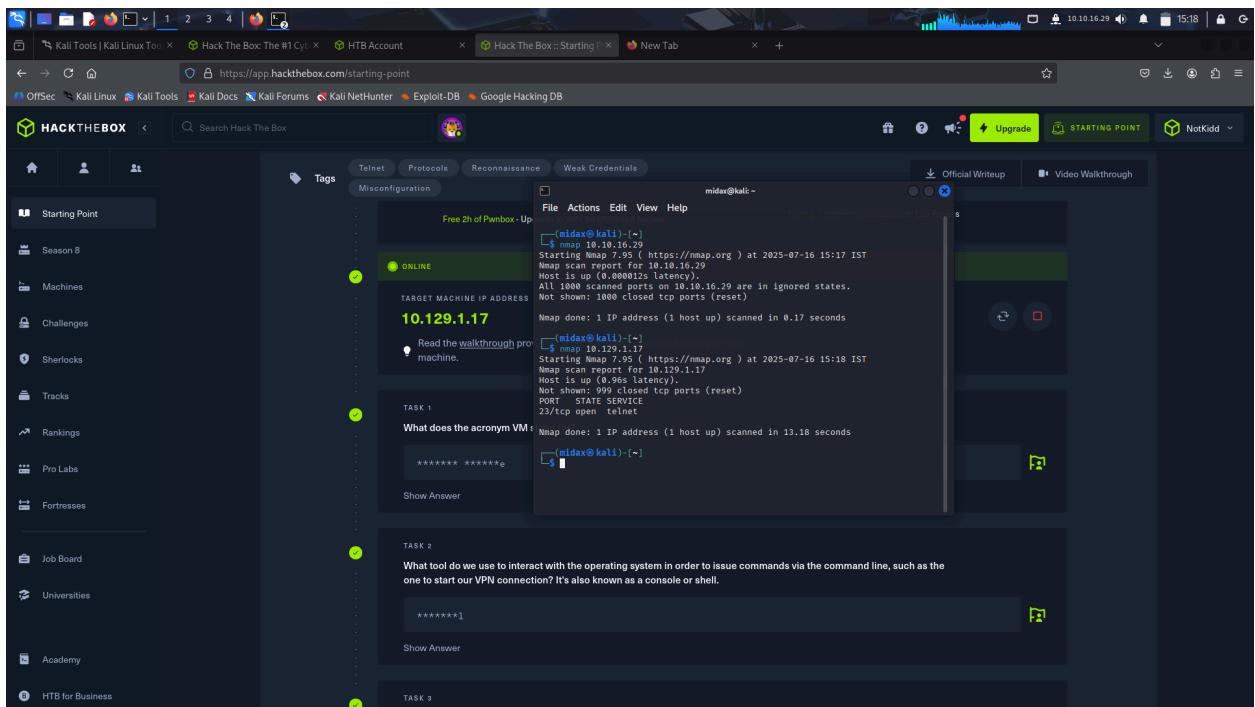
What service do we identify on port 23/tcp during our scans?

```
*****t
```

**telnet**  
**HIDE ANSWER**

The first few tasks were fairly easy as I know it already.

Then to find which service are on port 23/tcp, i ran a simple **nmap <ip addr>**



The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with various navigation links like Season 8, Machines, Challenges, etc. The main area shows a terminal window with the command `nmap 10.10.16.29` and its output. The output shows that port 23/tcp is open and identified as telnet. Below the terminal, there are two tasks:

**TASK 1**  
What does the acronym VM stand for?  
\*\*\*\*\*  
Show Answer

**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.  
\*\*\*\*\*  
Show Answer

 TASK 6

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

\*\*\*\*\*t



**telnet**

[Hide Answer](#)

 TASK 7

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

\*\*\*t



**root**

[Hide Answer](#)

 SUBMIT FLAG

Submit root flag

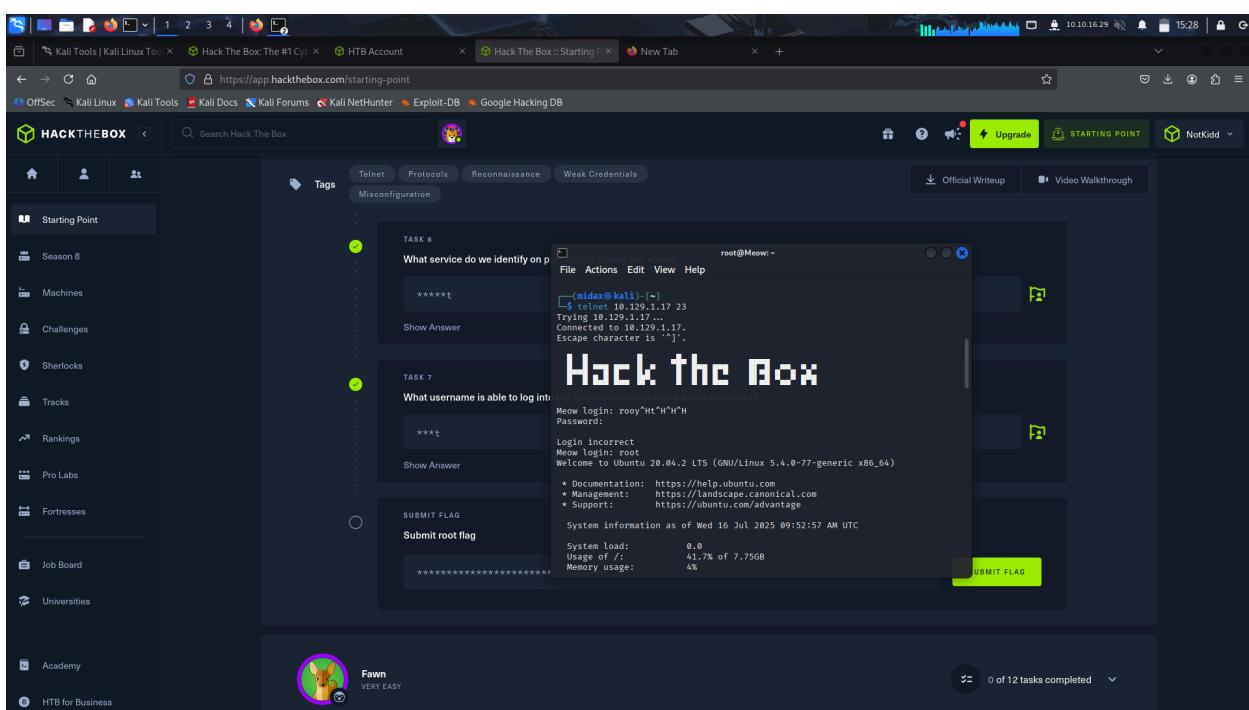
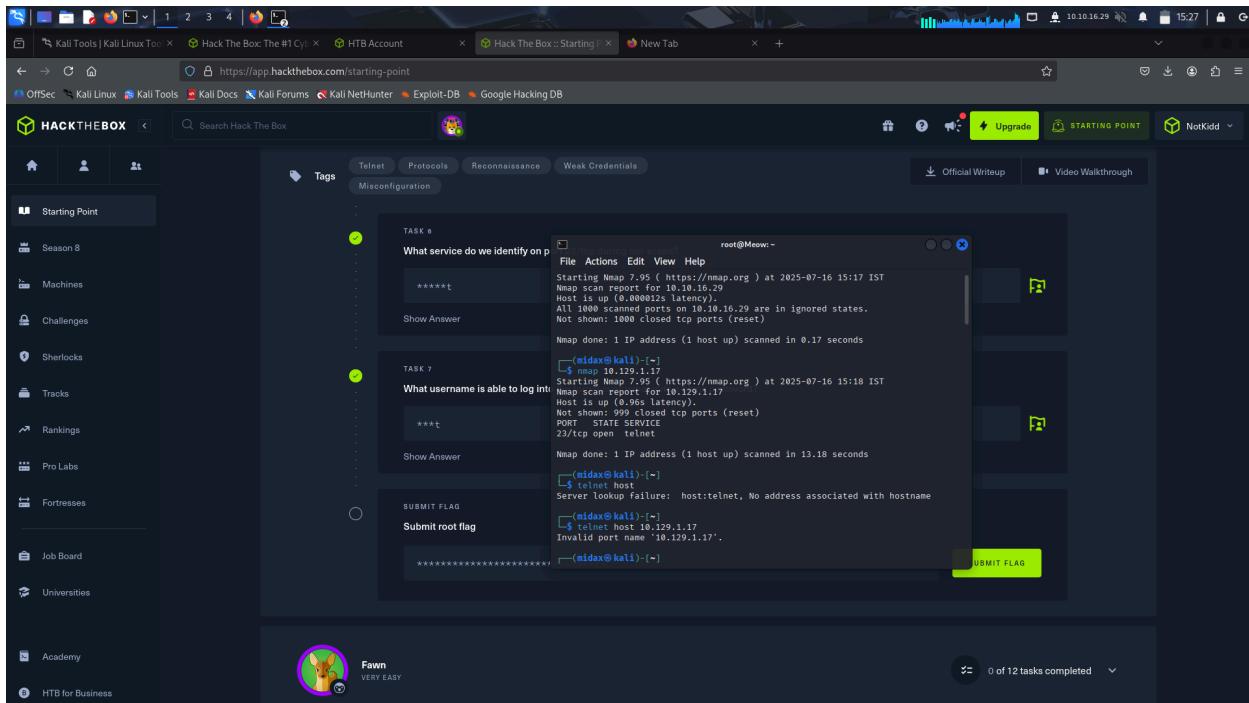
\*\*\*\*\*



**b40abdf23665f766f9c61ecba8a4c19**

[Hide Answer](#)

finding the root flag was fun since it is my first time navigating through telnet.



```
(Metasploit) -> $ telnet 10.129.1.17 23
Trying 10.129.1.17...
Connected to 10.129.1.17.
Escape character is '^}'.

[Hack the Box] -> Meow:~
```

Hack the Box

Meow login: rooYHt^H^H^H  
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/adantage.com

System information as of Wed 16 Jul 2025 09:52:57 AM UTC

```
System load: 0.0
Usage of /: 41.7% of 7.75GB
Memory usage: 4%
Swap usage: 0%
Processes: 153
Users logged in: 0
IPv4 address for eth0: 10.129.1.17
IPv6 address for eth0: dead:beef::250:56ff:feb0:4ce6
```

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

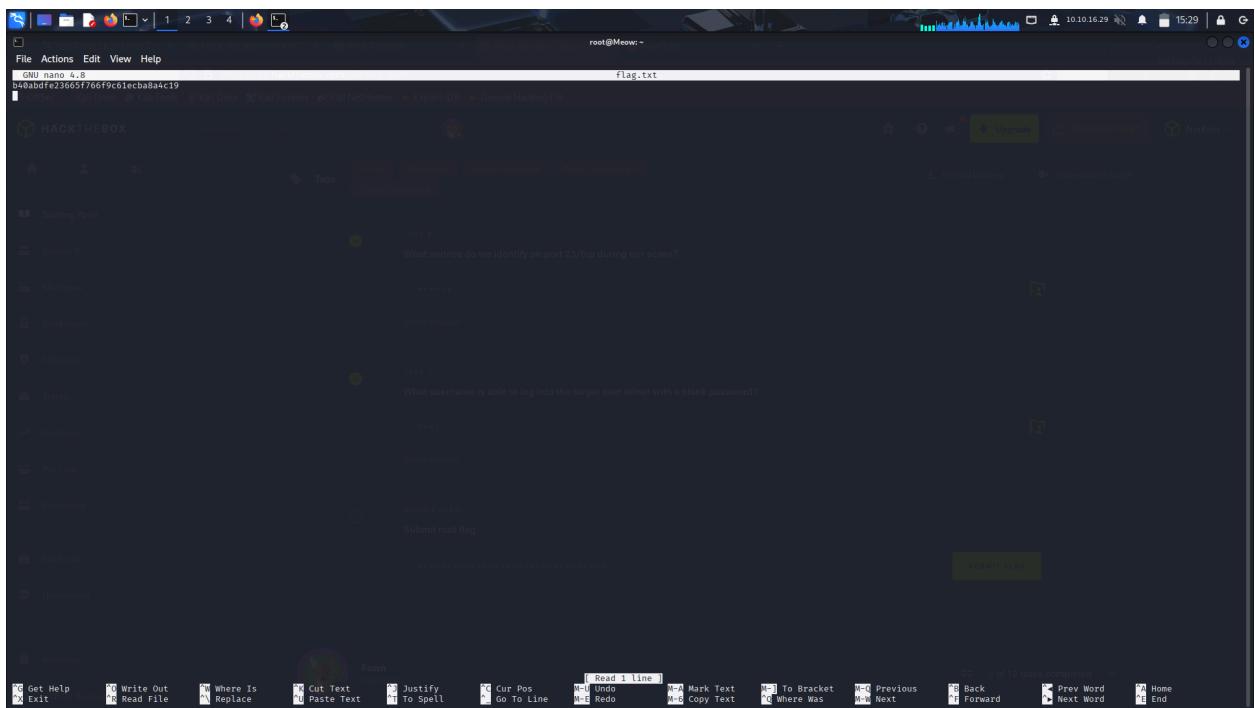
```
Last login: Mon Sep 6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~$ ls
flag.txt  snap
root@Meow:~# cd snap/
root@Meow:~/snap# ls -la
total 12
drwxr-xr-x 3 root root 4096 Apr 21 2021 .
drwxr-xr-x 5 root root 4096 Jun 18 2021 ..
drwxr-xr-x 5 root root 4096 Sep 13 2021 lxd
root@Meow:~/snap# ls -la
total 20
drwxr-xr-x 5 root root 4096 Sep 13 2021 .
drwxr-xr-x 3 root root 4096 Apr 21 2021 ..
drwxr-xr-x 2 root root 4096 Apr 21 2021 21468
drwxr-xr-x 2 root root 4096 Apr 21 2021 common
drwxrwxr-x 1 root root 5 Sep 13 2021 current -> 21497
```

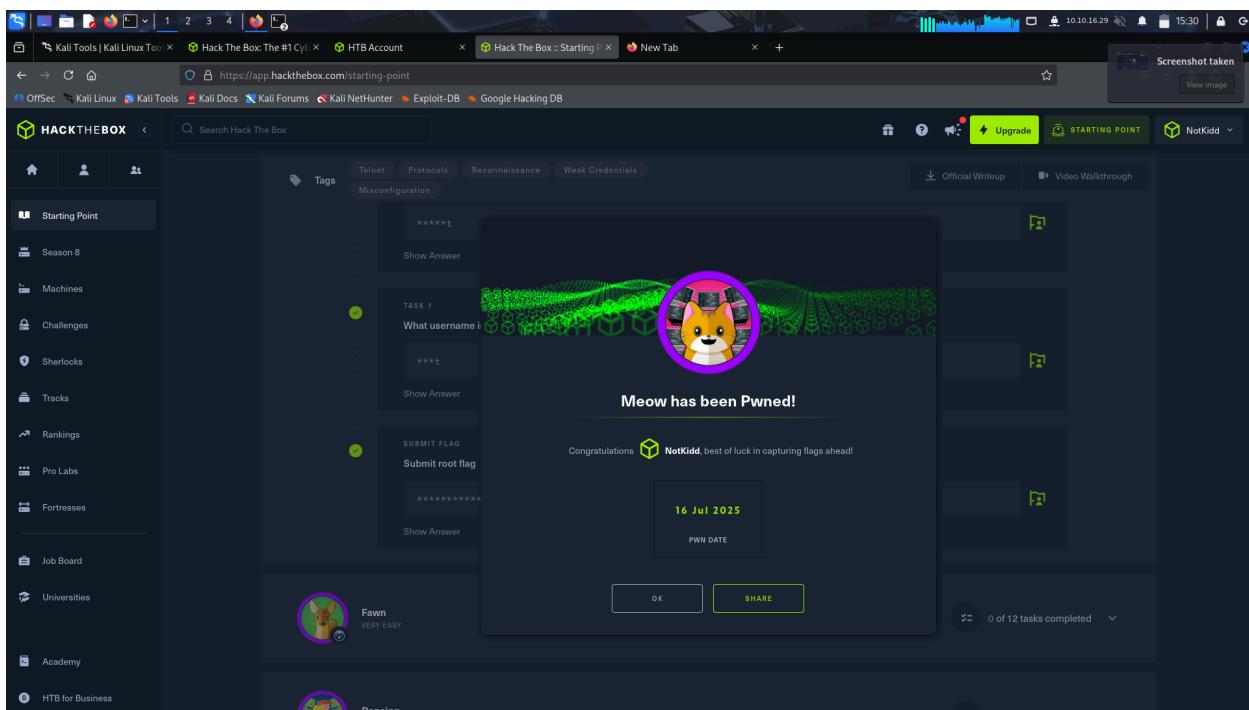
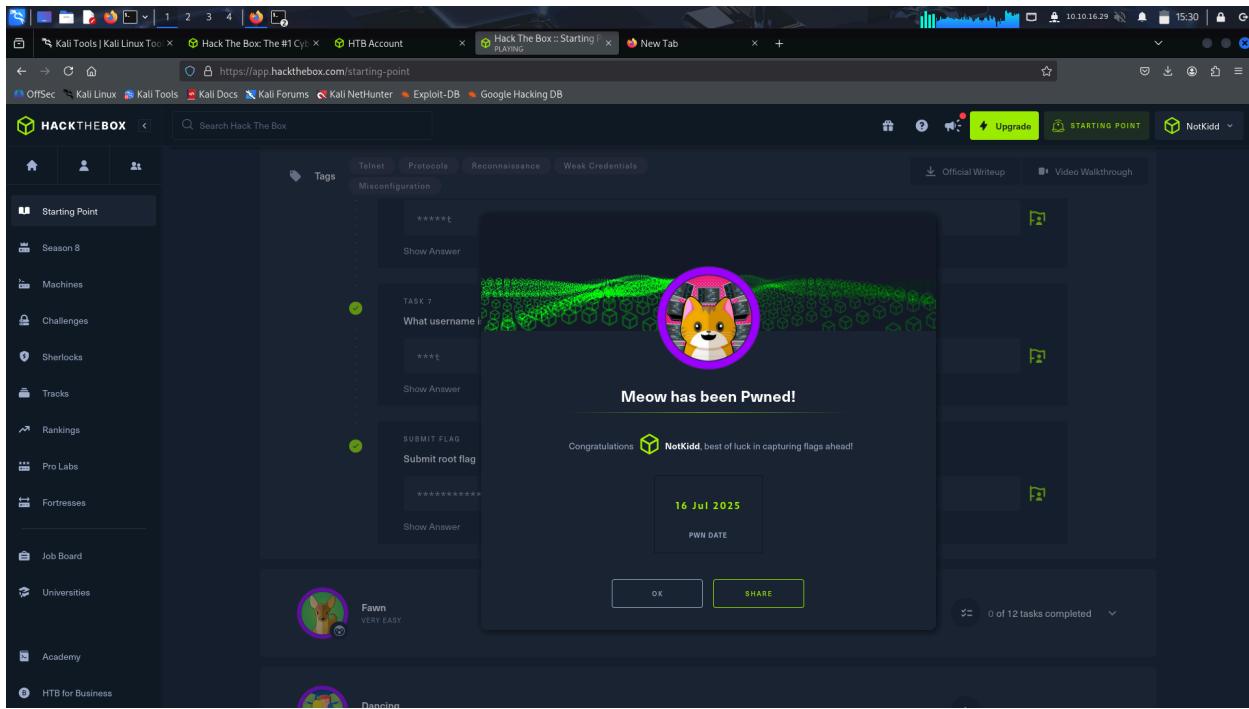
```
[Hack the Box] -> Meow:~
```

```
File Actions Edit View Help
drwxr-xr-x 5 root root 4096 Sep 13 2021 lxd
root@Meow:~/snap# cd ..
root@Meow:~# cd ..
root@Meow:~# ls -la
total 1
drwxr-xr-x 5 root root 4096 Jun 18 2021 .
drwxr-xr-x 20 root root 4096 Jul 7 2021 .
lrwxrwxrwx 1 root root 9 Jun 4 2021 bash_history -> /dev/null
-rw-r--r-- 1 root root 3132 Oct 6 2020 .bashrc
drwxr-xr-x 2 root root 4096 Apr 21 2021 .cache
-rw-r--r-- 1 root root 177212147 2021 .config
drwxr-xr-x 3 root root 4096 Apr 21 2021 .local
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
-rw-r--r-- 1 root root 205 Mar 20 2021 .selected_editor
drwxr-xr-x 1 root root 4096 Apr 21 2021 snap
root@Meow:~# 
root@Meow:~# nano flag.txt
root@Meow:~#
```

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

now thinking back.. I should've read the flag using cat instead of nano, anyway i found the flag.





And that's how I completed the meow, it was an easy one, so I kept going..

## Fawn

This time connecting to openvpn wasn't a big of a deal, it was a piece of cake.

**TASK 1**  
What does the 3-letter acronym FTP stand for?

\*\*\*\*\* \*\*\*\*\*  
**File Transfer Protocol**

**TASK 2**  
Which port does the FTP service listen on usually?

\*\*  
**21**

**TASK 3**  
FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

\*\*\*p  
**SFTP**

**TASK 4**  
What is the command we can use to send an ICMP echo request to test our connection to the target?

\*\*\*g  
**ping**

**TASK 5**  
From your scans, what version is FTP running on the target?

\*\*\*\*\* \*.\*.3  
**vsftpd 3.0.3**

**TASK 6**  
From your scans, what OS type is running on the target?

\*\*\*x  
**Unix**

till now the questions were theoretical and i get to complete all of it with ease. Until when they ask which version is FTP running on

To find the version **man nmap** helped a lot

```

File Actions Edit View Help
--sniff Scan and disable port scan
--open Try all hosts as online -- skip host discovery
--PS/PA/PU/PV[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
--PE/RP/PM: ICMP echo, timestamp, and netmask request discovery probes
--PO[protocol list]: IP Protocol Ping
--NMAP[script list]: Run Nmap scripts to resolve [default: sometimes]
--dns-servers <server1,server2,...> Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN METHODS:
--S/T/A/W/M: TCP SYN/Connect() /ACK/Window/Maimon scans
--S/U: UDP Scan
--S/F: TCP Null, FIN, and Xmas scans
--S/A/F: TCP ACK, RST, and SYN-ACK flags
--script-args: Customize TCP scan flags
--S-I: zombie host[:probeport]: Idle scan
--S/Z: SCTP INIT/COOKIE-ECHO scans
--S-PR: probe random hosts: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges> Only scan specified ports
--excl-port <port ranges> Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-R: Scan ports sequentially - don't randomize
--max-retries <n> Maximum number of common ports
--port-ratio <ratio> Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
--S-V: Probe open ports to determine service/version info
--version-intensity <n> Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--script-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
--SC: equivalent to --script=<default>
--script=<lua scripts> <Lua script(s)> is a comma separated list of
  directories, script-files or script-categories
--script-args=<args> Provide arguments to scripts
--script-args-file=<filename> provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updates: Update the script database
--script-help=<Lua script> Show help about scripts.
  <Lua script(s)> is a comma-separated list of script-files or
  script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMEOUTS:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<n>: Set timing template (higher is faster)
--min-hostgroup <n> Set the minimum number of host scan group sizes
--min-parallelism/max-parallelism <n> Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time> Specifies
  probe round trip time.
--max-retries <n> Number of port scan probe retransmissions.
--host-timeout <time> Give up on target after this long
--scan-delay/-max-scan-delay <time> Adjust delay between probes
--max-rate <numbers> Send packets no slower than <numbers> per second
--max-parallel <numbers> Send packets in parallel <numbers> per second
  What is the command that is used over FTP when you want to log in without having an account?

```

Manual page nmap(1) line 107 (press h for help or q to quit)

**nmap -sV <ip addr>**

```

File Actions Edit View Help
midax@kali: ~
$ nmap -sV
Starting Nmap 7.05 ( https://nmap.org ) at 2025-07-16 20:55 IST
Nmap scan report for 10.129.176.79
Host is up (0.000s latency).
Nmap done: 1 IP addresses (0 hosts up) scanned in 0.07 seconds

```

```

(midax㉿kali)-[~]
$ nmap -sV
Starting Nmap 7.05 ( https://nmap.org ) at 2025-07-16 20:58 IST
Nmap scan report for 10.129.176.79
Host is up (0.000s latency).
Nmap done: 1 IP addresses (1 host up) scanned in 6.01 seconds

```

What is the command we need to run in order to display the 'ftp' client help menu?



TASK 10

There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system?

\*\*

ls

[Hide Answer](#)



TASK 11

What is the command used to download the file we found on the FTP server?

\*\*\*

get

[Hide Answer](#)



SUBMIT FLAG

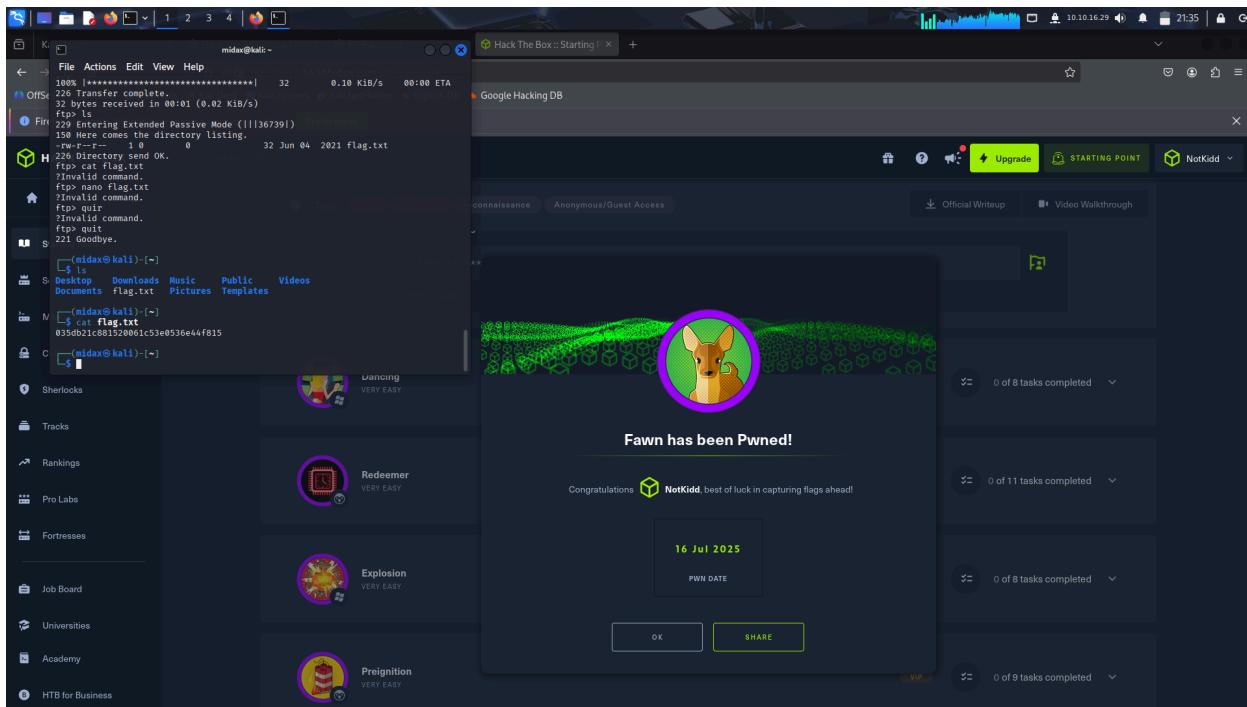
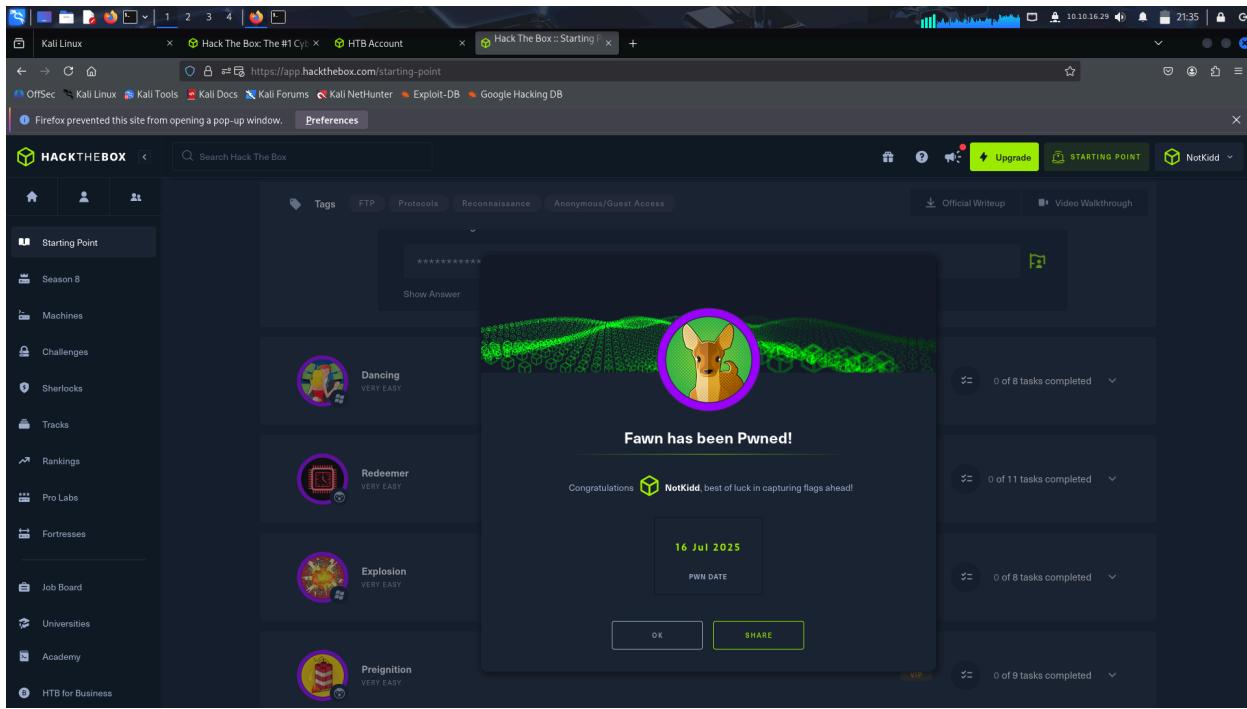
Submit root flag

\*\*\*\*\*

035db21c881520061c53e0536e44f815

[Hide Answer](#)





## Dancing

The screenshot shows a web browser with multiple tabs open. The main tab displays the HackTheBox starting point page. On the left, there's a sidebar with various navigation links like Starting Point, Season 8, Machines, Challenges, etc. The main content area shows several tasks:

- TASK 2**: What port does SMB use to operate at?  
Answer: \*\*\*
- TASK 3**: What is the service name for port 445 that came up in our Nmap scan?  
Answer: \*\*\*\*\*.g
- TASK 4**: What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?  
Answer: \*\*

At the bottom right of the task area, there are "SUBMIT ANSWER" and "HINT" buttons. A terminal window is visible in the background, showing smbclient session logs:

```
(midax㉿kali)-[~] $ smbclient -L Dancing
do_connect: Connection to 10.129.32.12 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
[...]
(midax㉿kali)-[~] $ smbclient -L 10.129.32.12
Password for [WORKGROUP]midax]:
[...]
```

This screenshot shows the same HackTheBox starting point page as the previous one, but with different task content. The terminal window in the background is identical to the previous one.

The tasks listed are:

- TASK 5**: How many shares are there on Dancing?  
Answer: \*
- TASK 6**: What is the name of the share we are able to access in the end with a blank password?  
Answer: \*\*\*\*\*
- TASK 7**: What is the command we can use within the SMB shell to download the files we find?  
Answer: [REDACTED]

At the bottom right of the task area, there are "SUBMIT ANSWER" and "HINT" buttons. A terminal window is visible in the background, showing smbclient session logs:

```
(midax㉿kali)-[~] $ smbclient -L Dancing
do_connect: Connection to 10.129.32.12 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
[...]
(midax㉿kali)-[~] $ smbclient -L 10.129.32.12
Password for [WORKGROUP]midax]:
[...]
```

The screenshot shows the HackTheBox platform interface. On the left sidebar, there's a navigation menu with items like Starting Point, Season 8, Machines, Challenges, Sherlocks, Tracks, Rankings, Pro Labs, Fortresses, Job Board, Universities, Academy, and HTB for Business. The main content area displays a challenge titled "Dancing has been Pwned!". The challenge details ask: "What is the command we can use within the SMB shell to download the files we find?". It includes a "SUBMIT FLAG" button and a "Submit root flag" button. Below the challenge, there's a congratulatory message: "Congratulations  **NotKidd**, best of luck in capturing flags ahead!". A timestamp "16 Jul 2025" is shown under the date "PWN DATE". At the bottom of the challenge card are "OK" and "SHARE" buttons. The top of the screen shows a browser window with multiple tabs open, including "Kali Linux", "Hack The Box: The #1 Cy...", "HTB Account", "Hack The Box :: Starting point", and "how many port in compu...". The status bar at the bottom right shows the IP address 10.10.16.29 and the time 23:02.

```
File Actions Edit View Help
Password for [WORKGROUP\weida]: 
tree connect failed: NT_STATUS_ACCESS_DENIED

(midea@kali) ~: 
└─$ smbclient //10.129.32.12\\IPC$ 
Password for [WORKGROUP\weida]: 
Try "help" to get a list of possible commands.
smb: > ls 
smb: > la -la 
la: command not found
smb: > 
NT_STATUS_NO_SUCH_FILE listing \* 
smb: > 

(midea@kali) ~: 
└─$ smbclient //10.129.32.12\\WorkShares 
Password for [WORKGROUP\weida]: 
Try "help" to get a list of possible commands.
smb: > ls 
          D      0 Mon Mar 29 13:52:01 2021 
..           D      0 Mon Mar 29 13:52:01 2021 
Amy.J        D      0 Mon Mar 29 14:38:24 2021 
James.P      D      0 Thu Jun  3 14:08:03 2021 
smb: > 
5114111 blocks of size 4096. 1753732 blocks available

smb: > ls . 
..           D      0 Mon Mar 29 13:52:01 2021 
Amy.J        D      0 Mon Mar 29 14:38:24 2021 
James.P      D      0 Thu Jun  3 14:08:03 2021 
smb: > 
NT_STATUS_NO_SUCH_FILE listing \-la 
smb: > get Amy.J\ 
smb: > 
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \Amy.J\ 
smb: > cd Amy.J\ 
smb: > 
Submit root flag
smb: > Amy.J\> ls 
          D      0 Mon Mar 29 14:38:24 2021 
..           D      0 Mon Mar 29 14:38:24 2021 
worknotes.txt  A     94 Fri Mar 26 16:30:37 2021 
smb: > 
5114111 blocks of size 4096. 1753732 blocks available 
smb: > Amy.J\> get worknotes.txt 
getfile file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.1 KiloBytes/sec) 
(sec) (average 0.1 KiloBytes/sec) 
smb: > Amy.J\> cd .. 
smb: > cd James.P\ 
smb: > James.P\> ls 
          D      0 Thu Jun  3 14:08:03 2021 
..           D      0 Thu Jun  3 14:08:03 2021 
flag.txt      A     32 Mon Mar 29 14:56:57 2021 
smb: > 
5114111 blocks of size 4096. 1753732 blocks available 
smb: > James.P\> get flag.txt 
getfile file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (av 
average 0.0 KiloBytes/sec) 
smb: > James.P\> 
```

## Redeemer