Hackthebox writeup

K.S Nandakumar

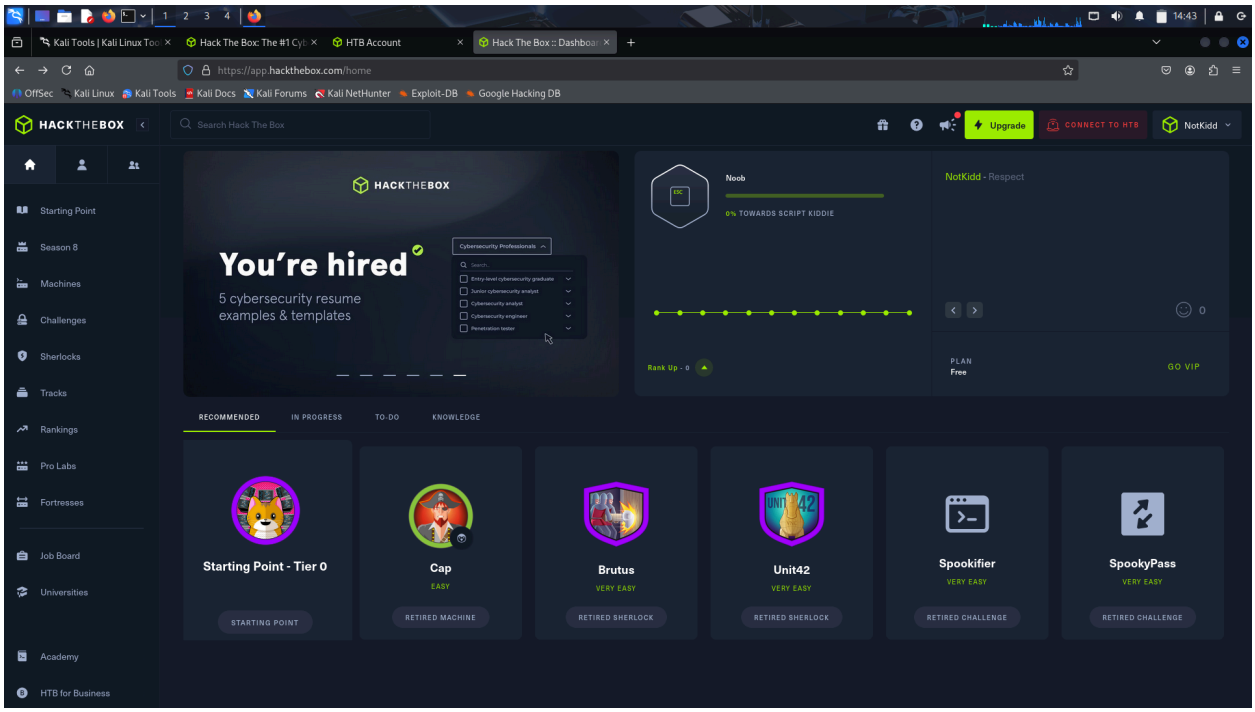
As this is my first CTF, I started with the very easy

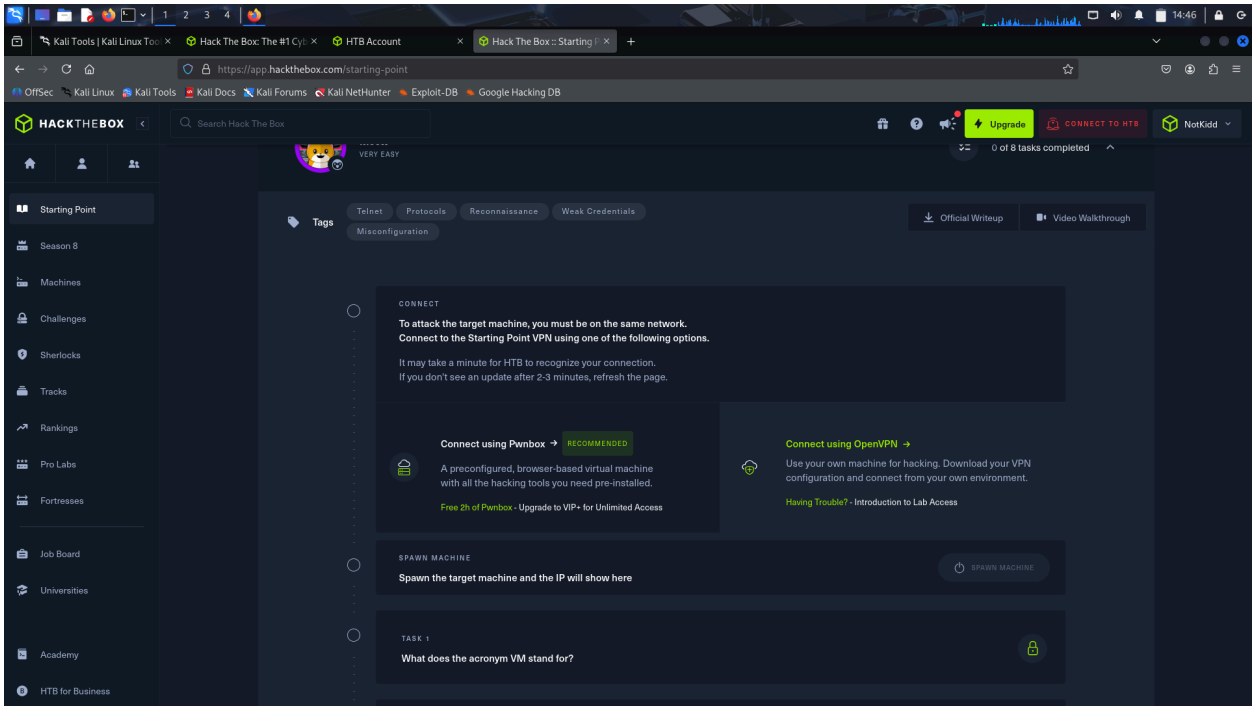
Tier 0 - The key is a strong foundation

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.

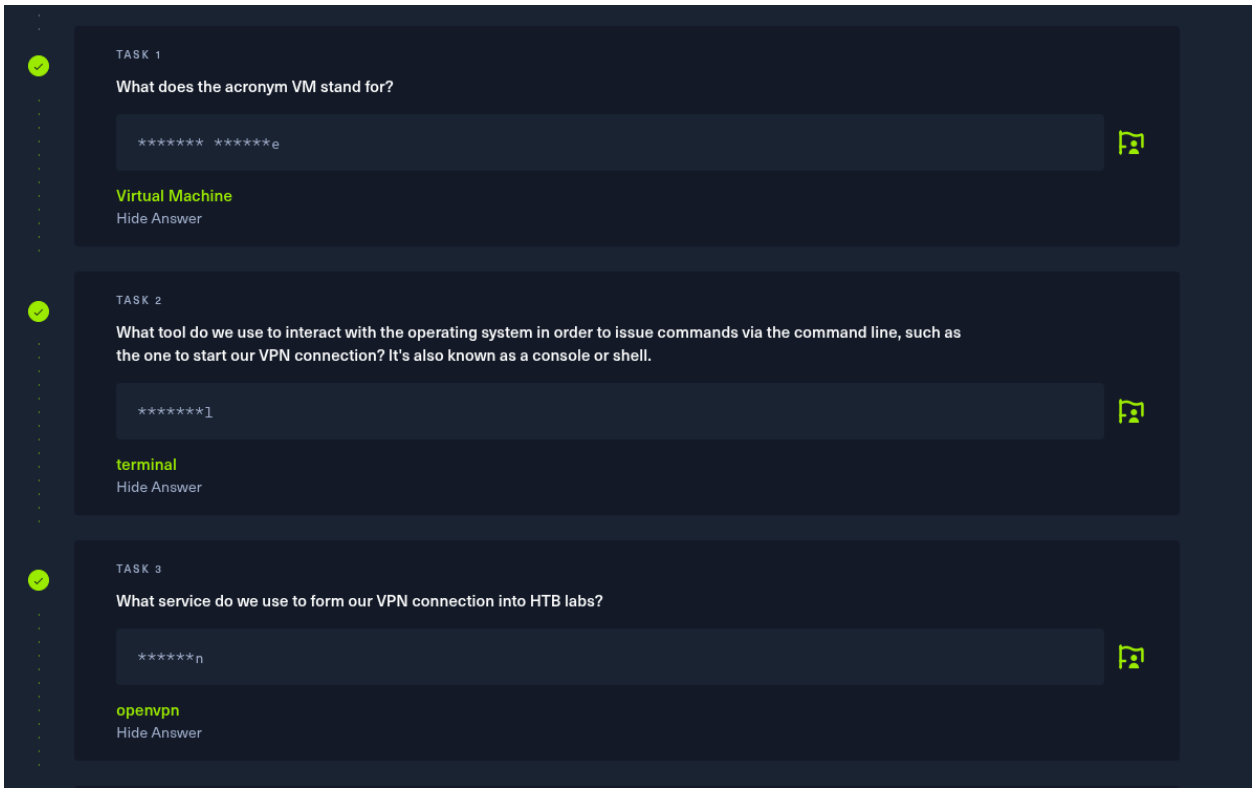
- I learned how to connect FTP, SMB, Telnet, Rsync and RDP anonymously.
- I learned how to use Nmap to identify open ports.

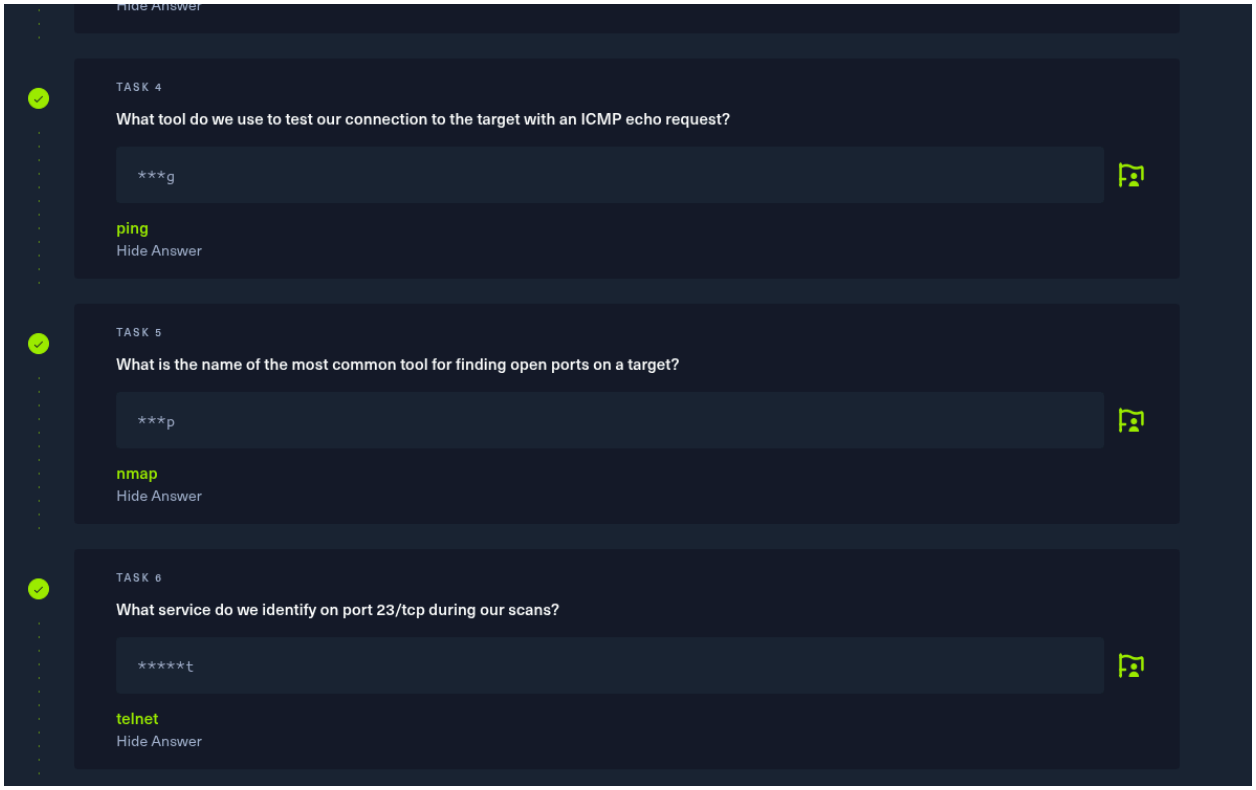
Meow



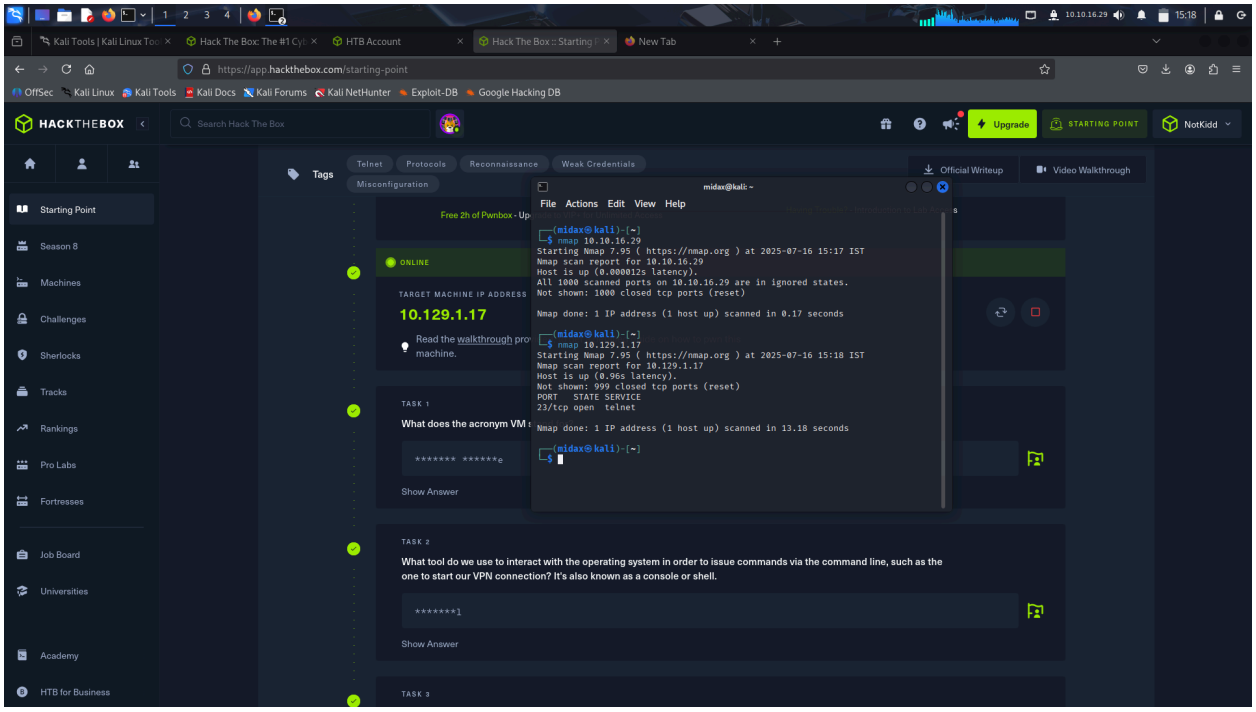


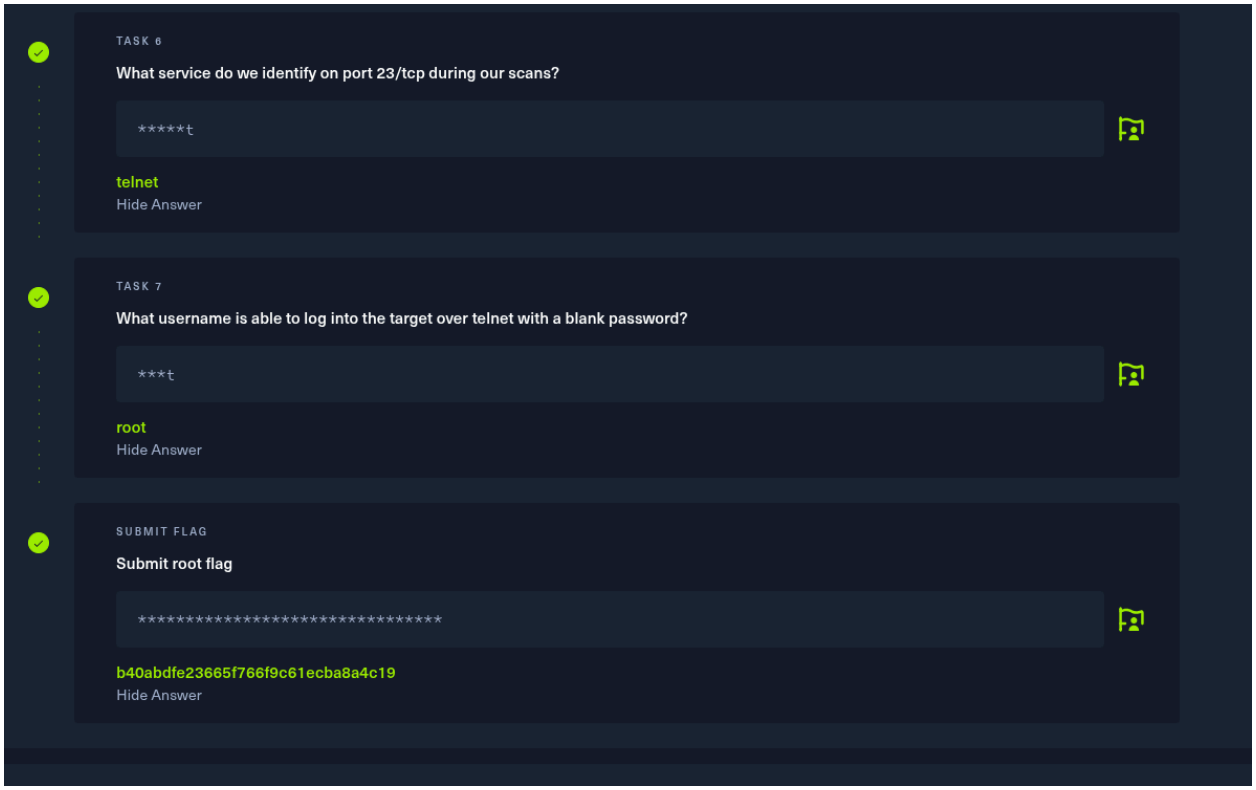
the first challenge i faced was to connect my virtual kali linux via openvpn, and for that the documentation really helped and within 20 minutes I figured out how to get connected and did a ping to confirm.



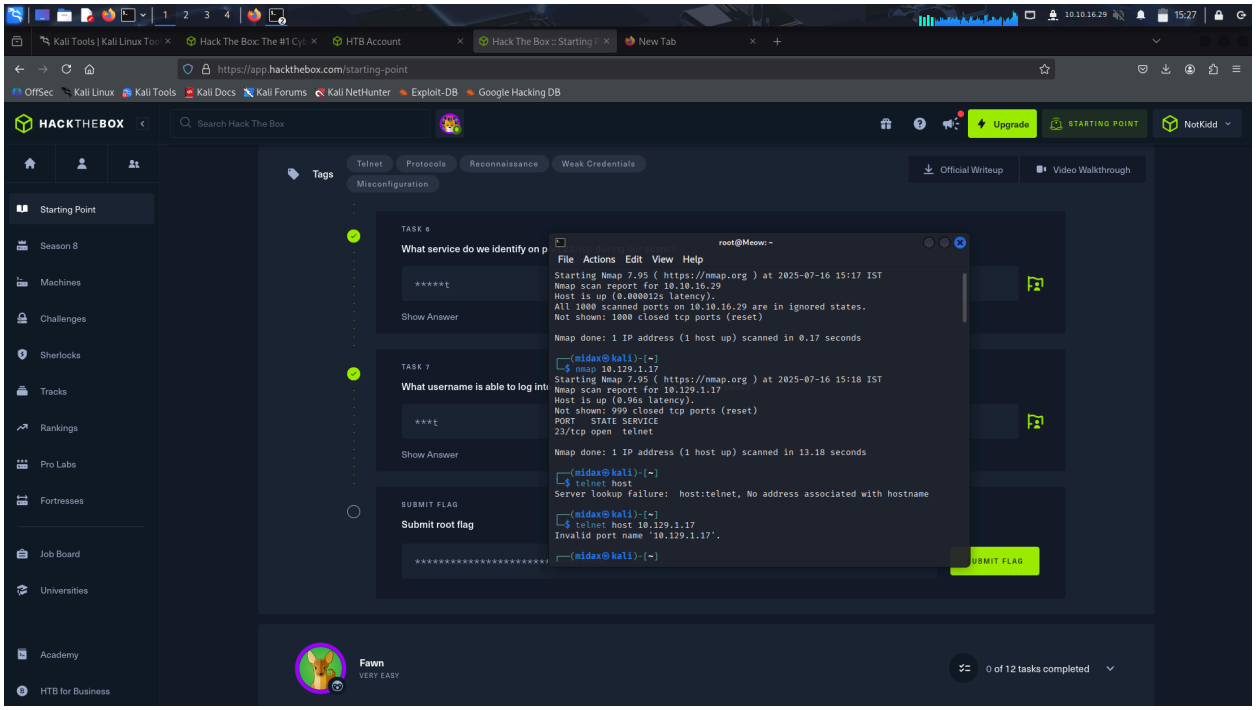


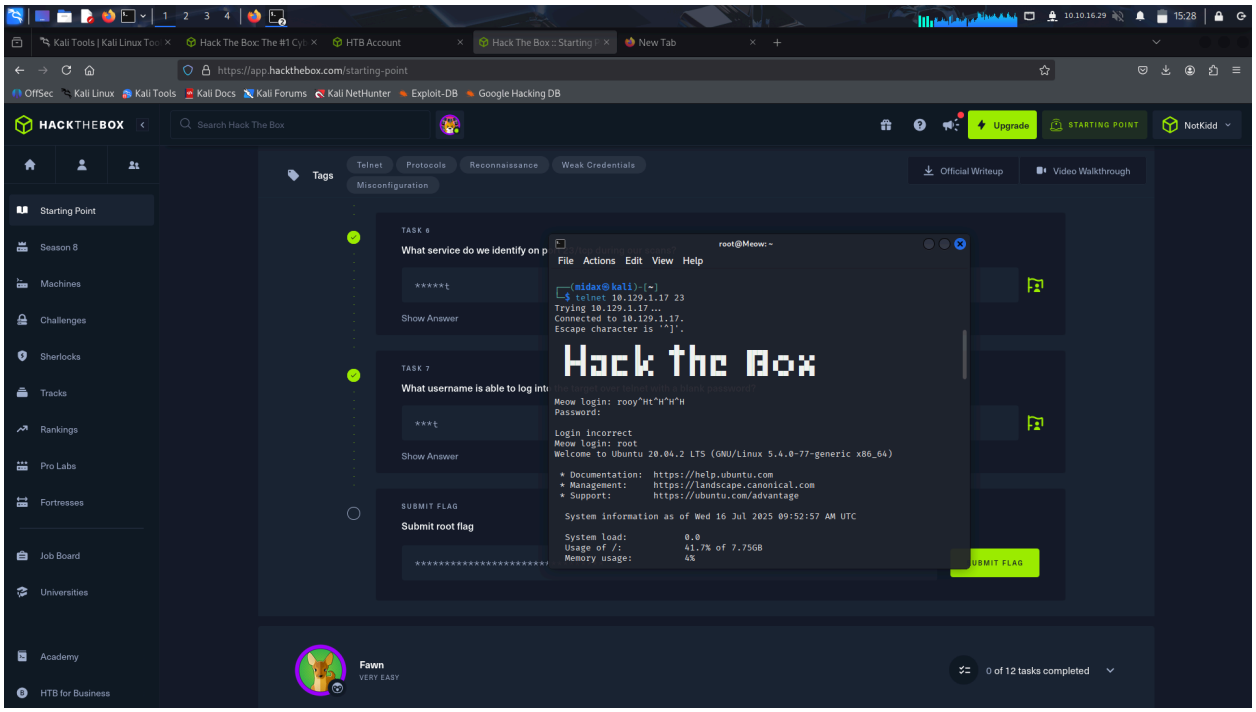
The first few tasks were fairly easy as I know it already.
Then to find which service are on port 23/tcp, i ran a simple **nmap <ip addr>**

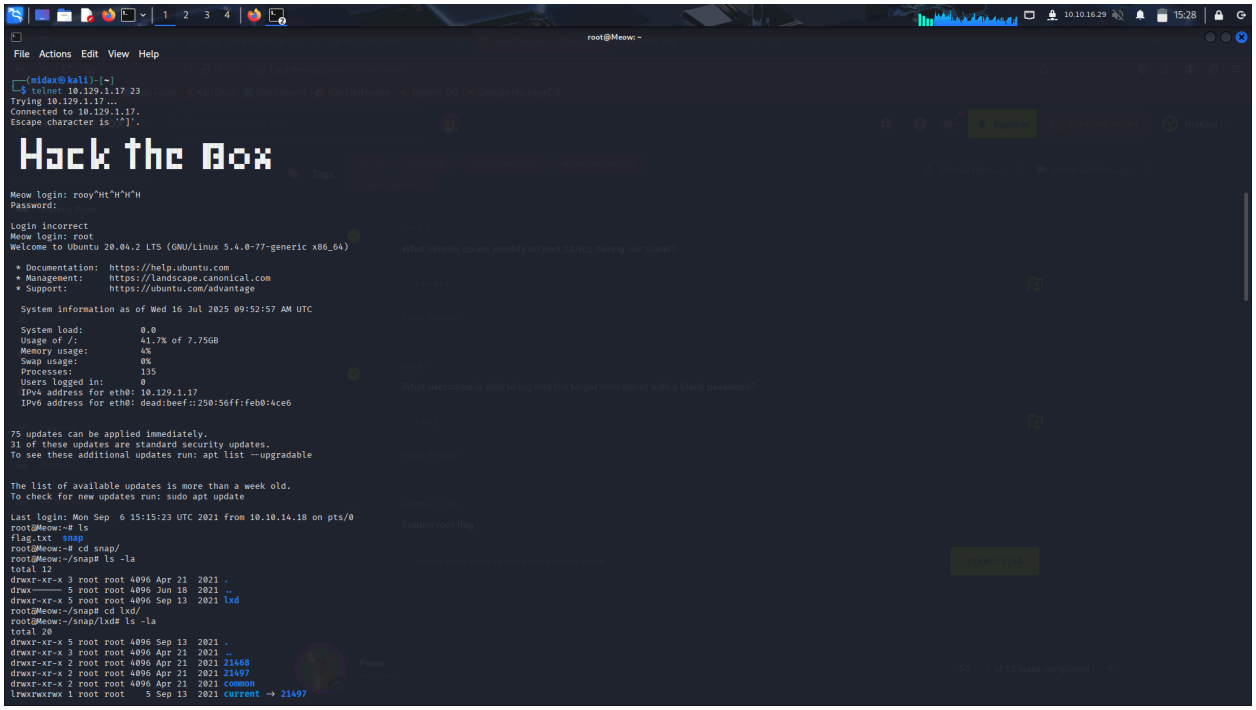


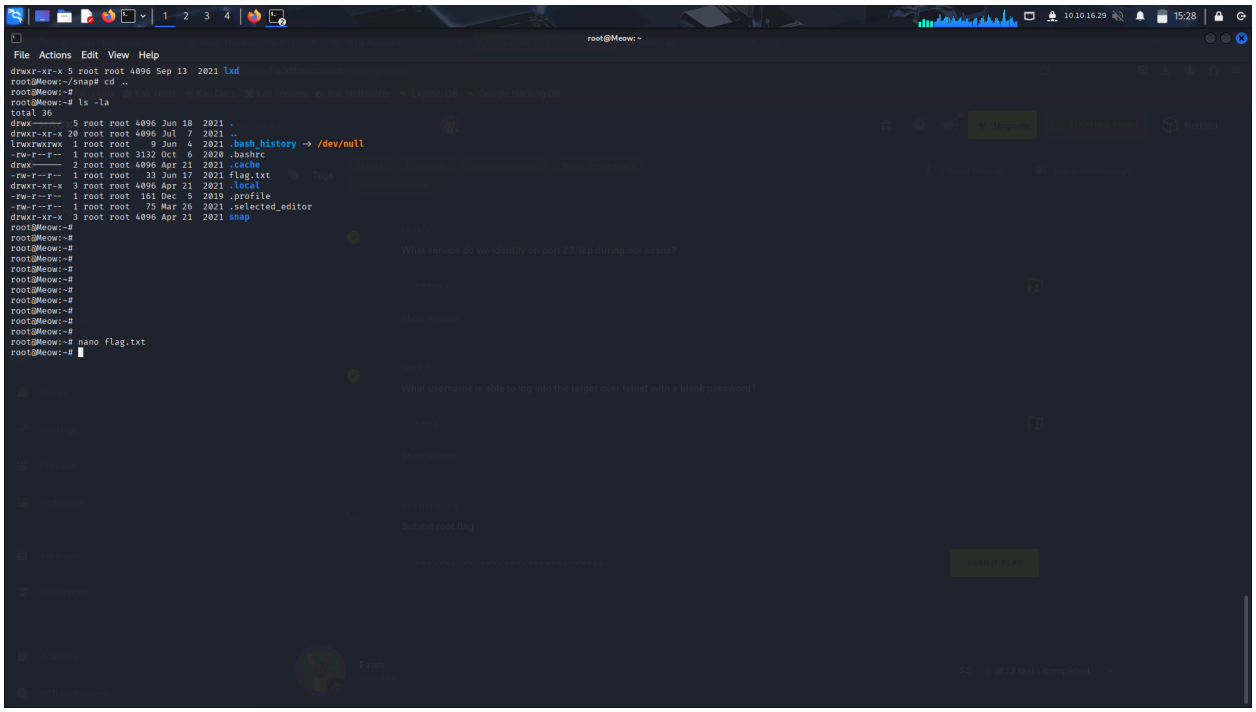


finding the root flag was fun since it is my first time navigating through telnet.

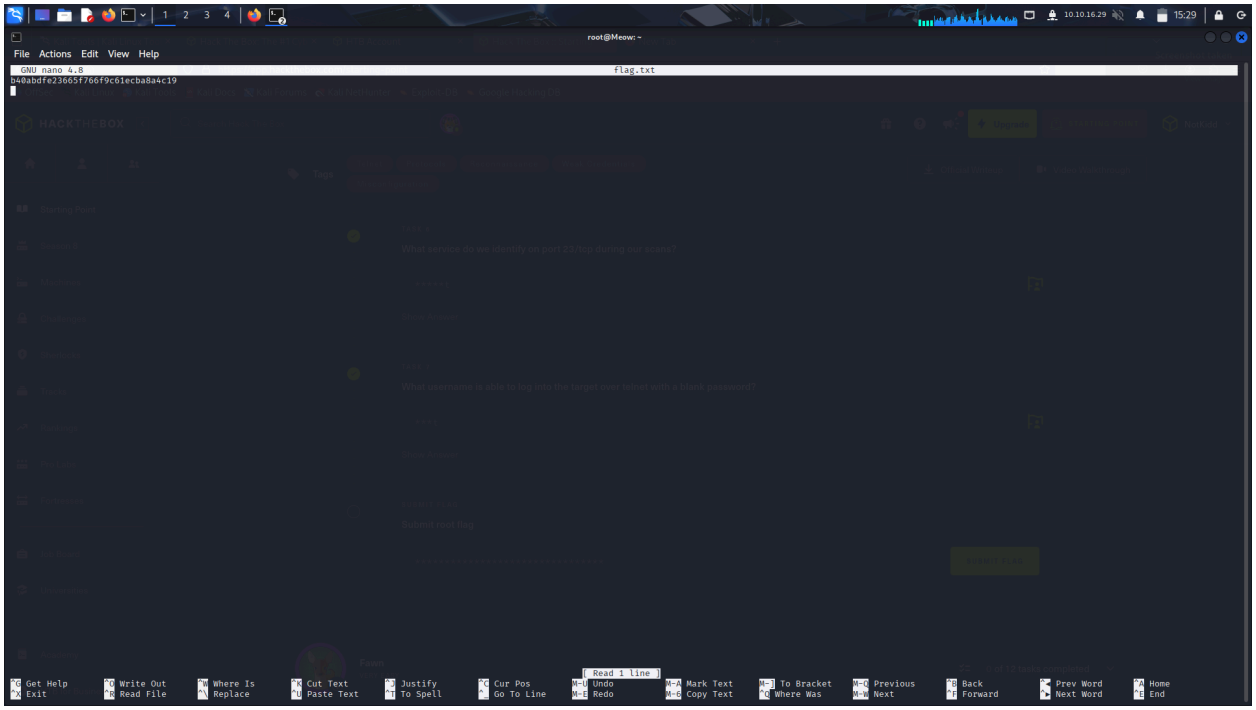

HACKTHEBOX
Starting Point
Season 8
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Tags
Telnet
Protocols
Reconnaissance
Weak Credentials
Misconfiguration
Official Writeup
Video Walkthrough
TASK 6
What service do we identify on p
*****t
Show Answer
TASK 7
What username is able to log int
***t
Show Answer
SUBMIT FLAG
Submit root flag
Fawn
VERY EASY
0 of 12 tasks completed
root@Meow: ~
File Actions Edit View Help
Starting Nmap 7.95 (https://nmap.org) at 2025-07-16 15:17 IST
Nmap scan report for 10.10.16.29
Host is up (0.000012s latency).
All 1000 scanned ports on 10.10.16.29 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
(midax㉿kali)-[~]
$ nmap 10.129.1.17
Starting Nmap 7.95 (https://nmap.org) at 2025-07-16 15:18 IST
Nmap scan report for 10.129.1.17
Host is up (0.96s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE
23/tcp open telnet
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
(midax㉿kali)-[~]
$ telnet host
Server lookup failure: host:telnet, No address associated with hostname
(midax㉿kali)-[~]
$ telnet host 10.129.1.17
Invalid port name '10.129.1.17'.
(midax㉿kali)-[~]

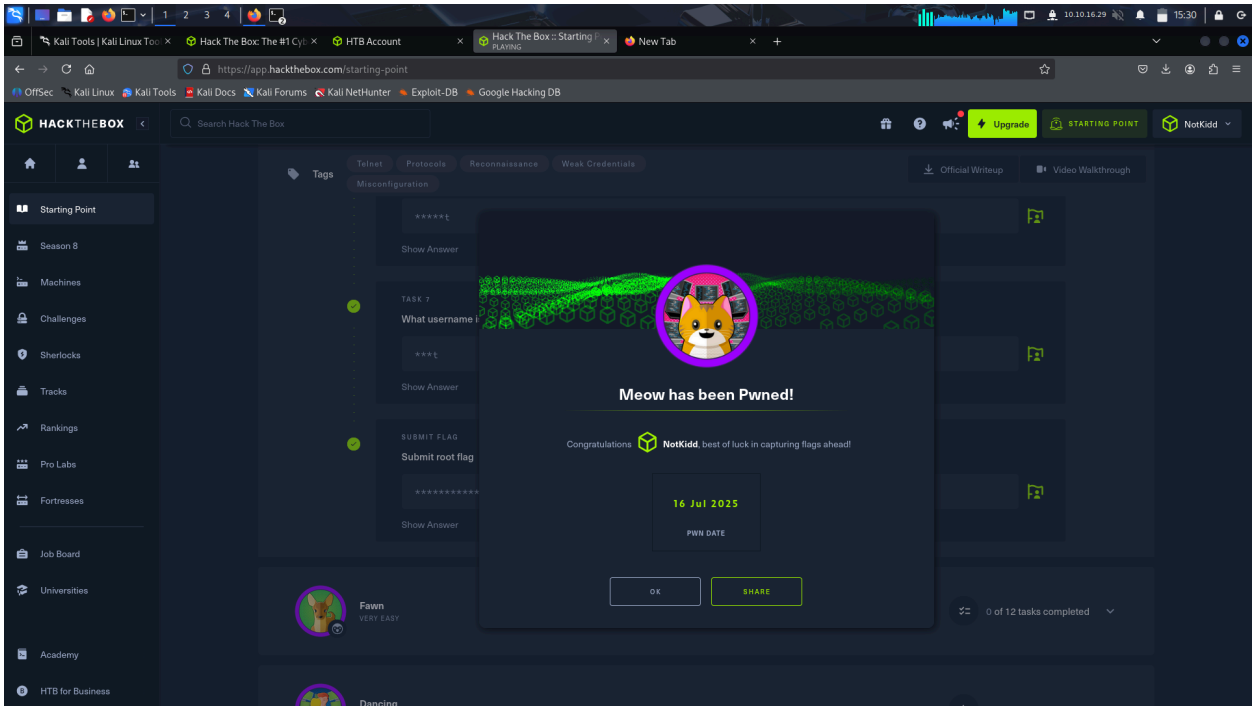

HACKTHEBOX
Starting Point
Season 8
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Tags
Telnet
Protocols
Reconnaissance
Weak Credentials
Misconfiguration
Official Writeup
Video Walkthrough
TASK 6
What service do we identify on p
*****t
Show Answer
TASK 7
What username is able to log int
***t
Show Answer
SUBMIT FLAG
Submit root flag
Fawn
VERY EASY
0 of 12 tasks completed
root@Meow: ~
File Actions Edit View Help
(midax㉿kali)-[~]
$ telnet 10.129.1.17 23
Trying 10.129.1.17...
Connected to 10.129.1.17.
Escape character is '^]'.
Hack the Box
Meow login: rooy^Ht^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/advantage
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%

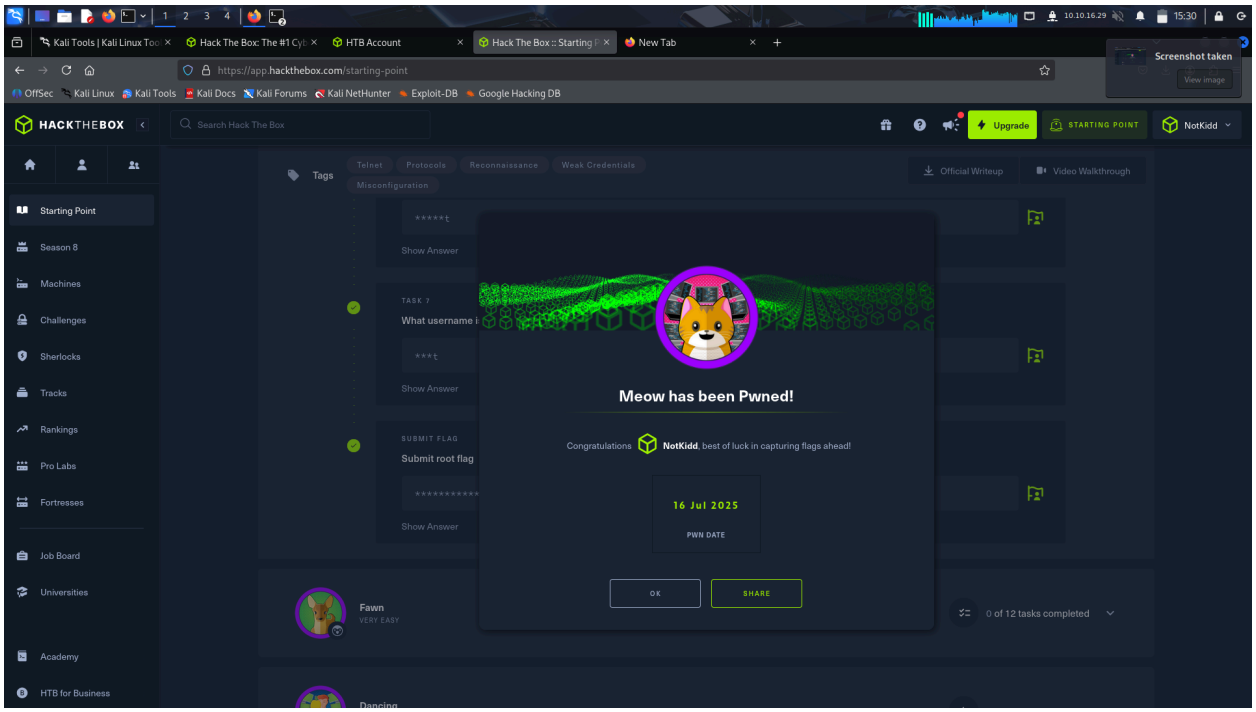




now thinking back.. I should’ve read the flag using cat instead of nano, anyway i found the flag.


root@Meow: ~
File Actions Edit View Help
GNU nano 4.8 flag.txt
b40abdfe23665f766f9c61ecba8a4c19
Read 1 line
Get Help
Write Out
Where Is
Cut Text
Justify
Cur Pos
Undo
Mark Text
To Bracket
Previous
Back
Prev Word
Home
Exit
Read File
Replace
Paste Text
To Spell
Go To Line
Redo
Copy Text
Where Was
Next
Forward
Next Word
End

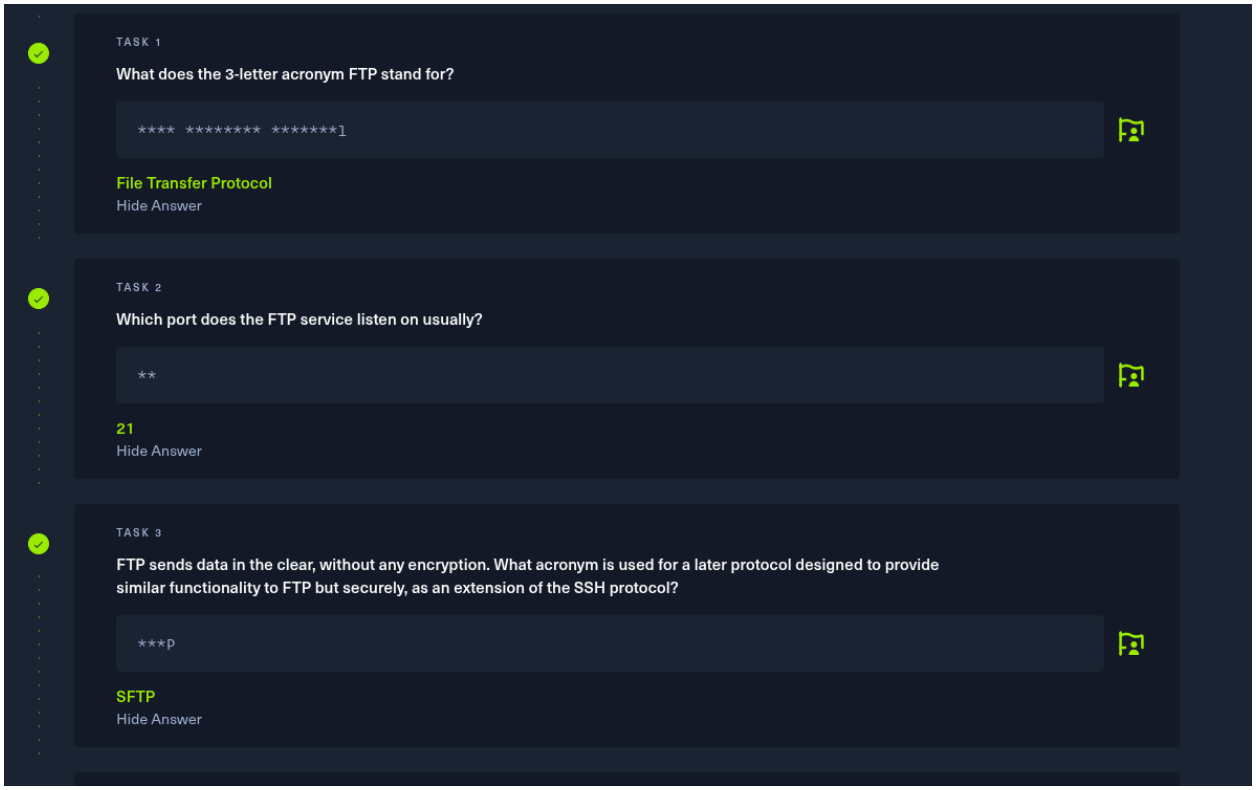


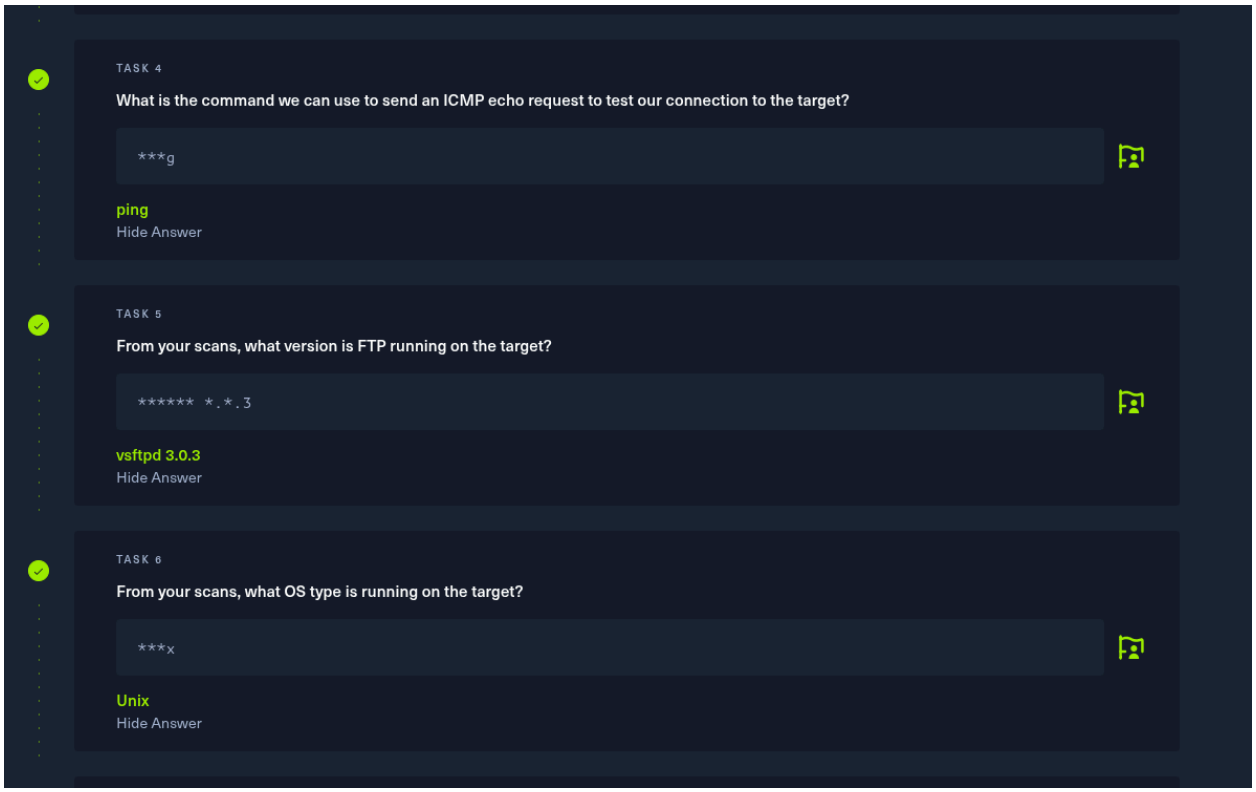


And that's how I completed the meow, it was an easy one, so I kept going..

Fawn

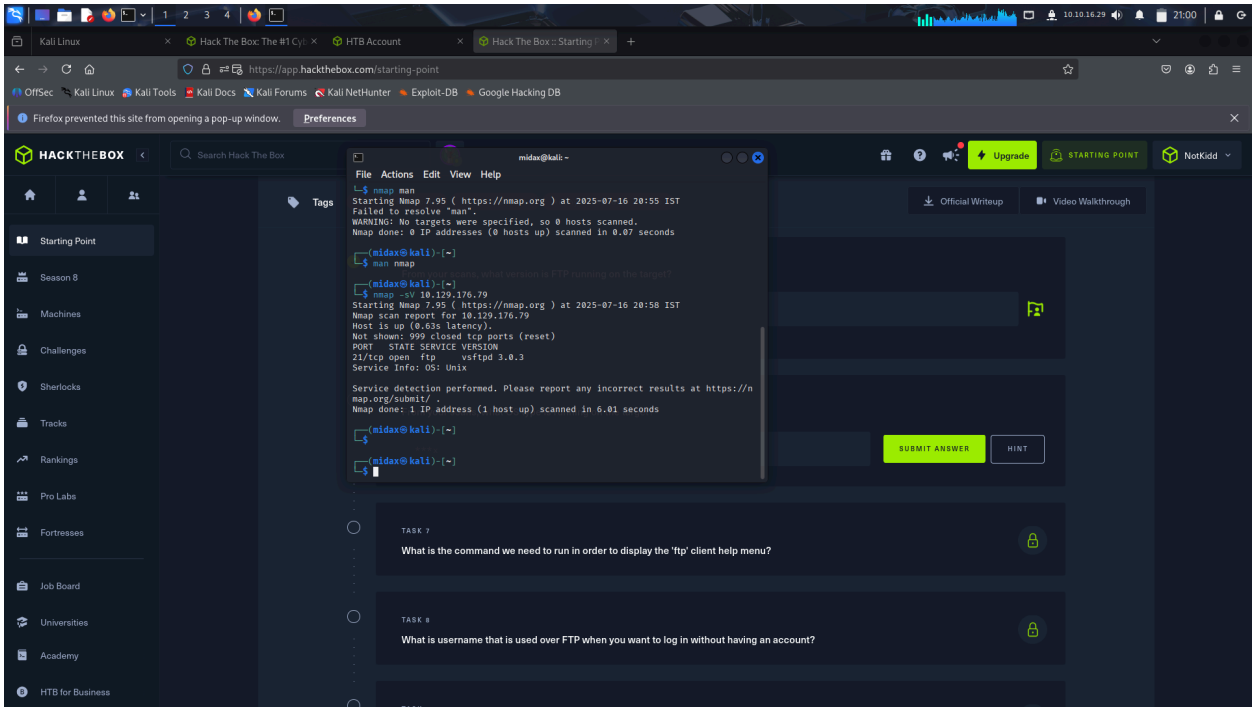
This time connecting to openvpn wasn't a big of a deal, it was a piece of cake.

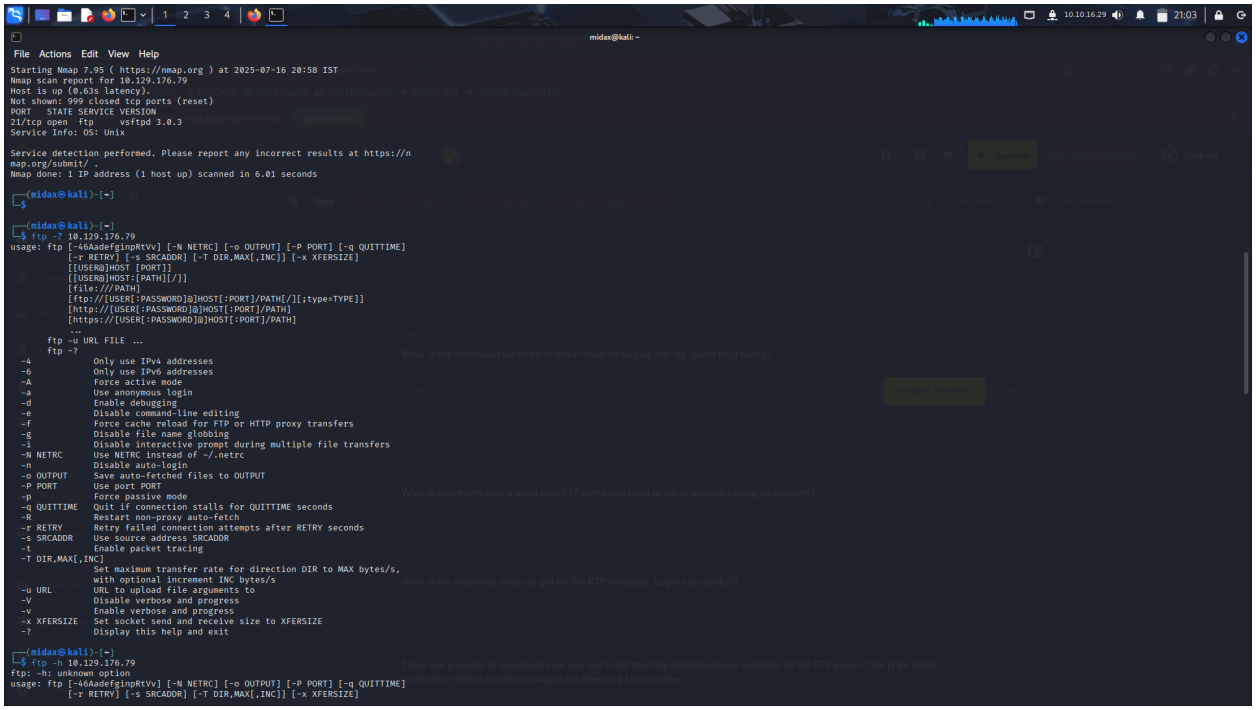


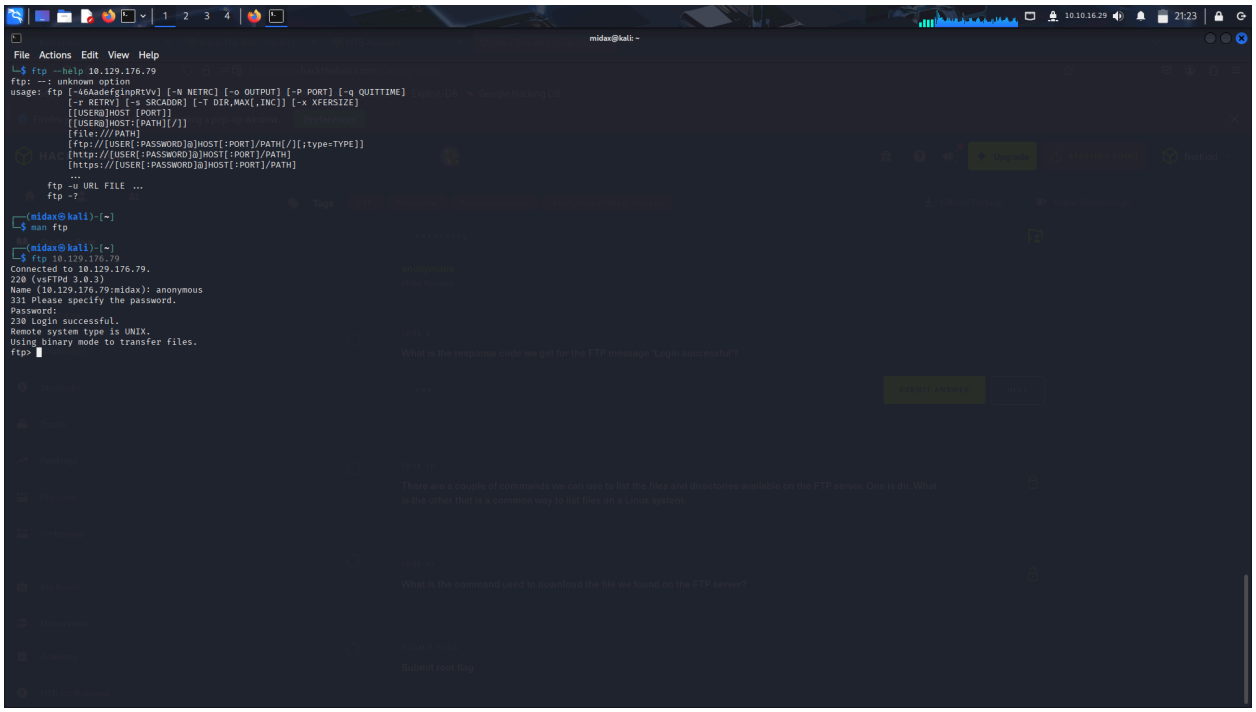


till now the questions were theoretical and i get to complete all of it with ease. Until when they ask which version is FTP running on
To find the version **man nmap** helped a lot

nmap -sV <ip addr>




midax@kali: ~
File Actions Edit View Help
Starting Nmap 7.95 (https://nmap.org) at 2025-07-16 20:58 IST
Nmap scan report for 10.129.176.79
Host is up (0.63s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.01 seconds
(midax㉿kali)-[~]
$
(midax㉿kali)-[~]
$ ftp -? 10.129.176.79
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
[-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
[[USER@]HOST [PORT]]
[[USER@]HOST:[PATH][/]]
[file:///PATH]
[ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
[http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
[https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
...
ftp -u URL FILE ...
ftp -?
-4 Only use IPv4 addresses
-6 Only use IPv6 addresses
-A Force active mode
-a Use anonymous login
-d Enable debugging
-e Disable command-line editing
-f Force cache reload for FTP or HTTP proxy transfers
-g Disable file name globbing
-i Disable interactive prompt during multiple file transfers
-N NETRC Use NETRC instead of ~/.netrc
-n Disable auto-login
-o OUTPUT Save auto-fetched files to OUTPUT
-P PORT Use port PORT
-p Force passive mode
-q QUITTIME Quit if connection stalls for QUITTIME seconds
-R Restart non-proxy auto-fetch
-r RETRY Retry failed connection attempts after RETRY seconds
-s SRCADDR Use source address SRCADDR
-t Enable packet tracing
-T DIR,MAX[,INC]
Set maximum transfer rate for direction DIR to MAX bytes/s,
with optional increment INC bytes/s
-u URL URL to upload file arguments to
-V Disable verbose and progress
-v Enable verbose and progress
-x XFERSIZE Set socket send and receive size to XFERSIZE
-? Display this help and exit
(midax㉿kali)-[~]
$ ftp -h 10.129.176.79
ftp: -h: unknown option
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
[-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]


midax@kali: ~
File Actions Edit View Help
$ ftp --help 10.129.176.79
ftp: --: unknown option
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
[-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
[[USER@]HOST [PORT]]
[[USER@]HOST:[PATH][/]]
[file:///PATH]
[ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
[http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
[https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
...
ftp -u URL FILE ...
ftp -?
(midax㉿kali)-[~]
$ man ftp
(midax㉿kali)-[~]
$ ftp 10.129.176.79
Connected to 10.129.176.79.
220 (vsFTPd 3.0.3)
Name (10.129.176.79:midax): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

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

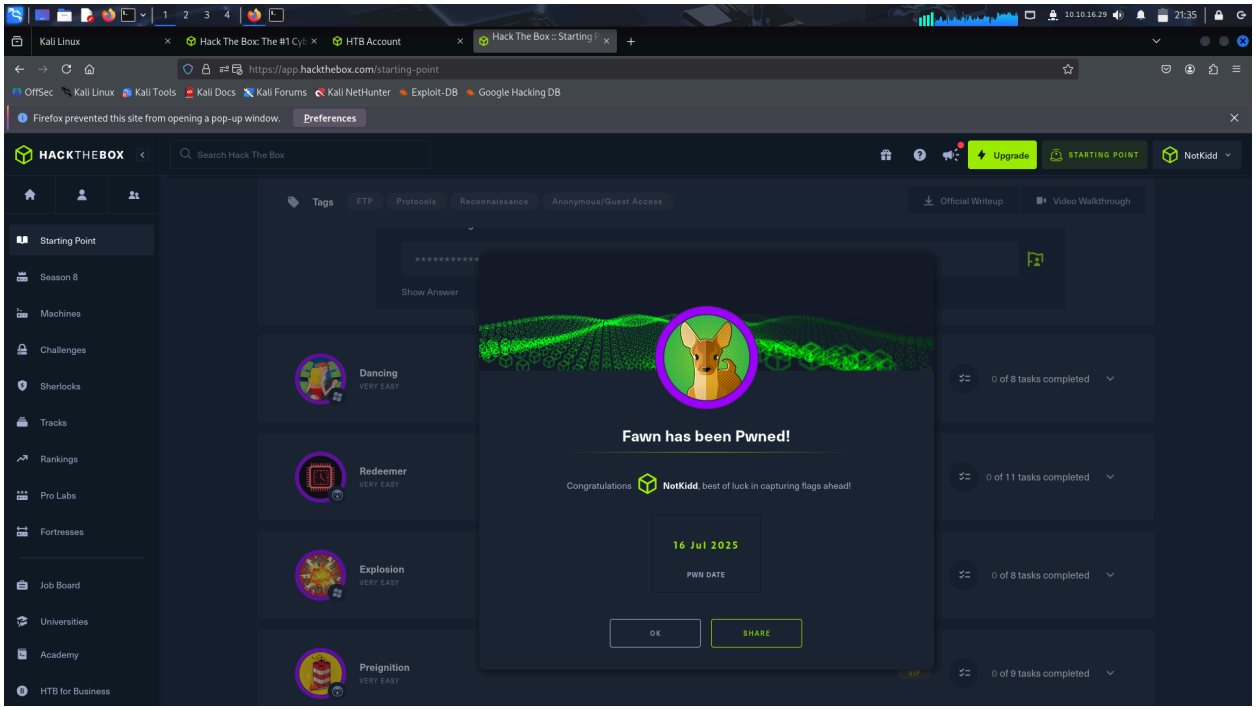
SUBMIT FLAG

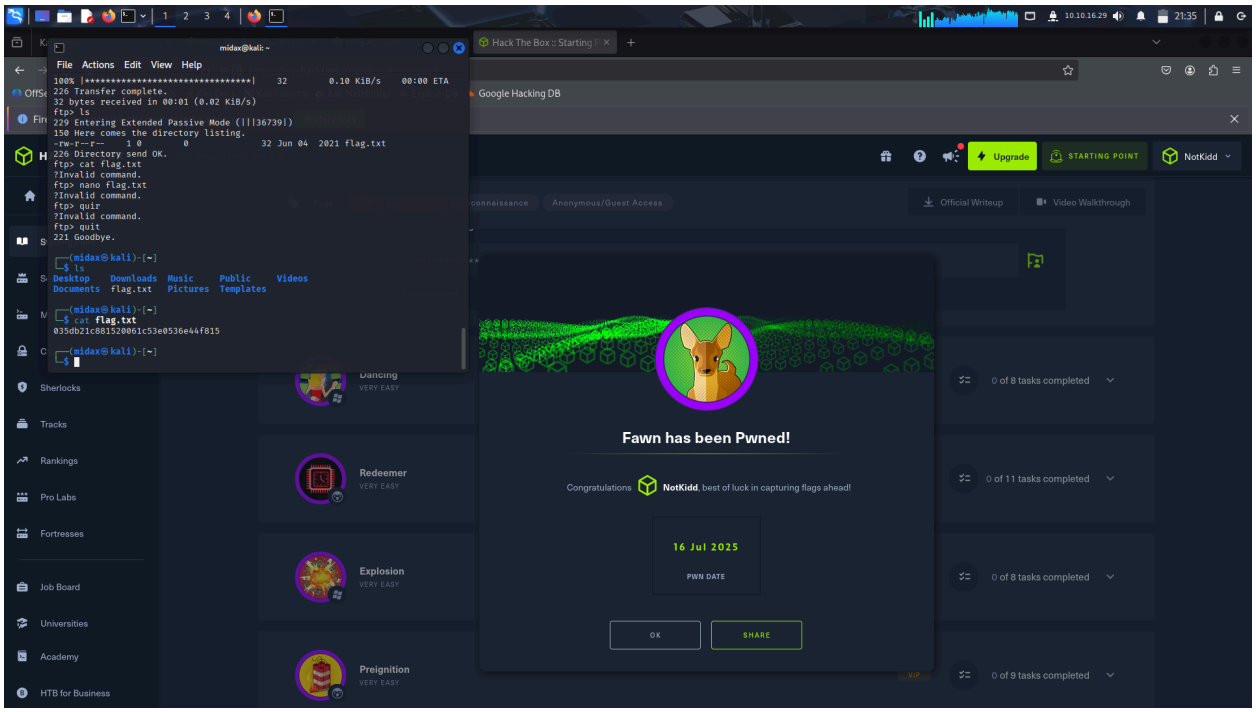
Submit root flag

****

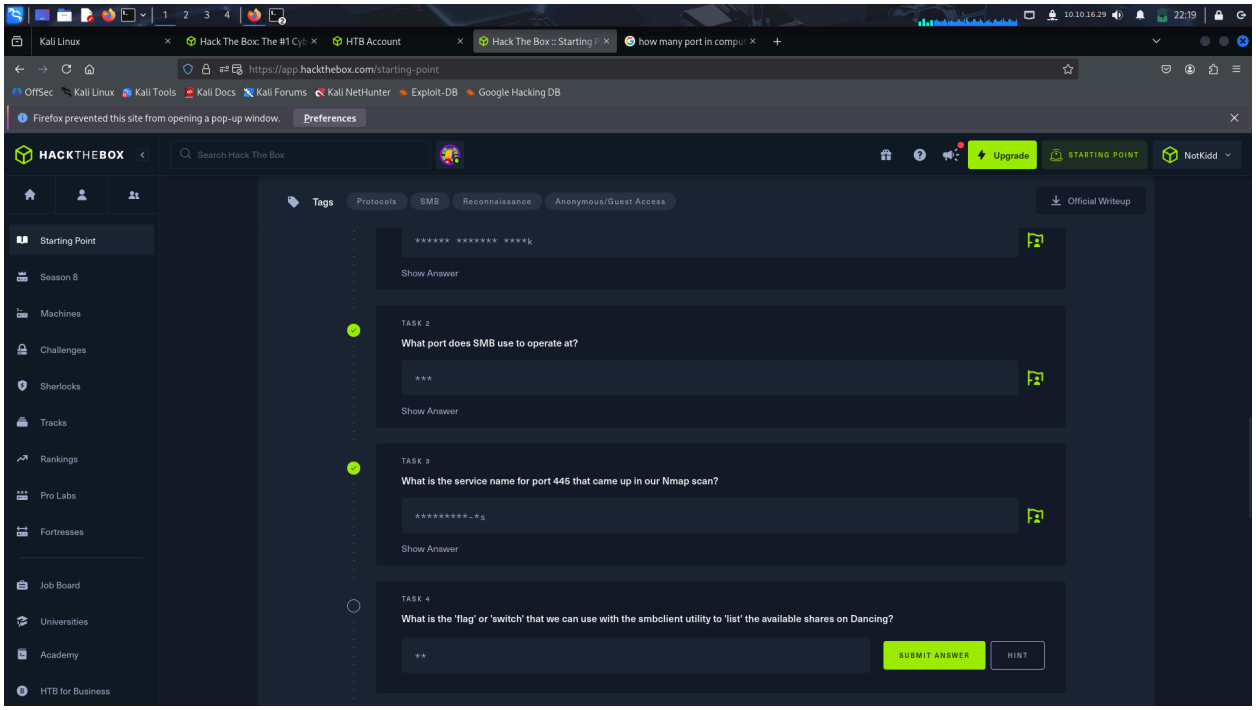
035db21c881520061c53e0536e44f815

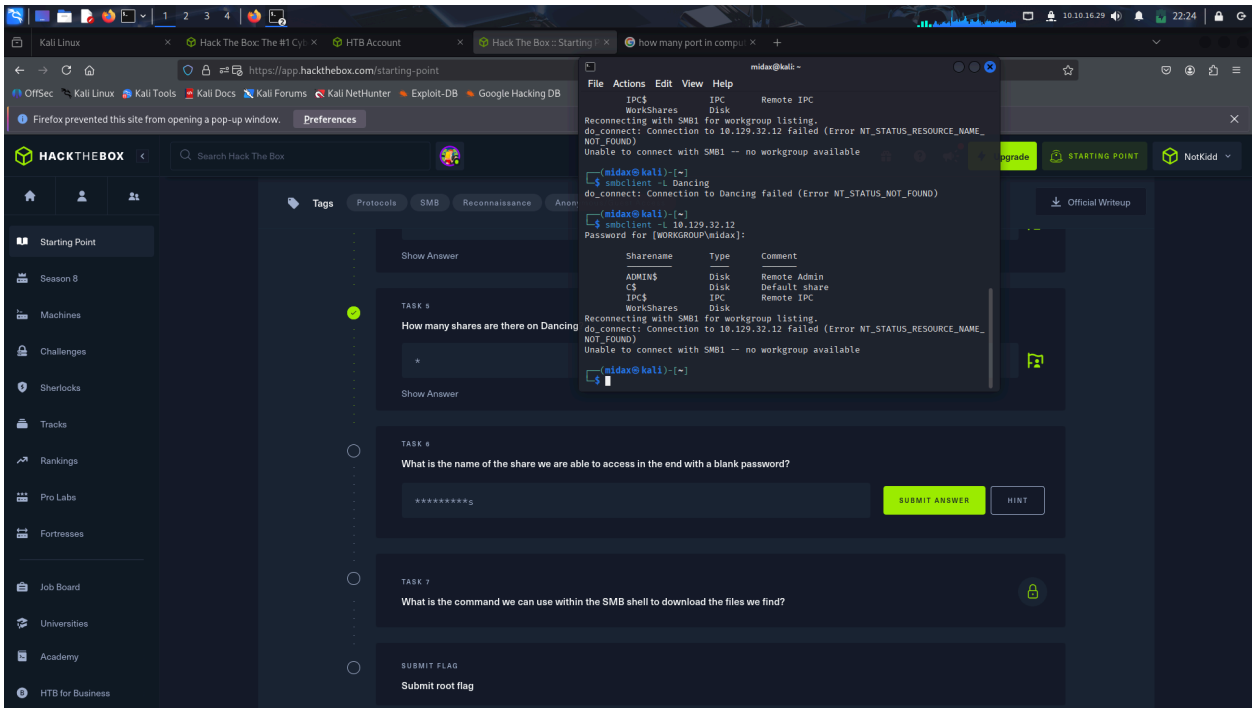
Hide Answer

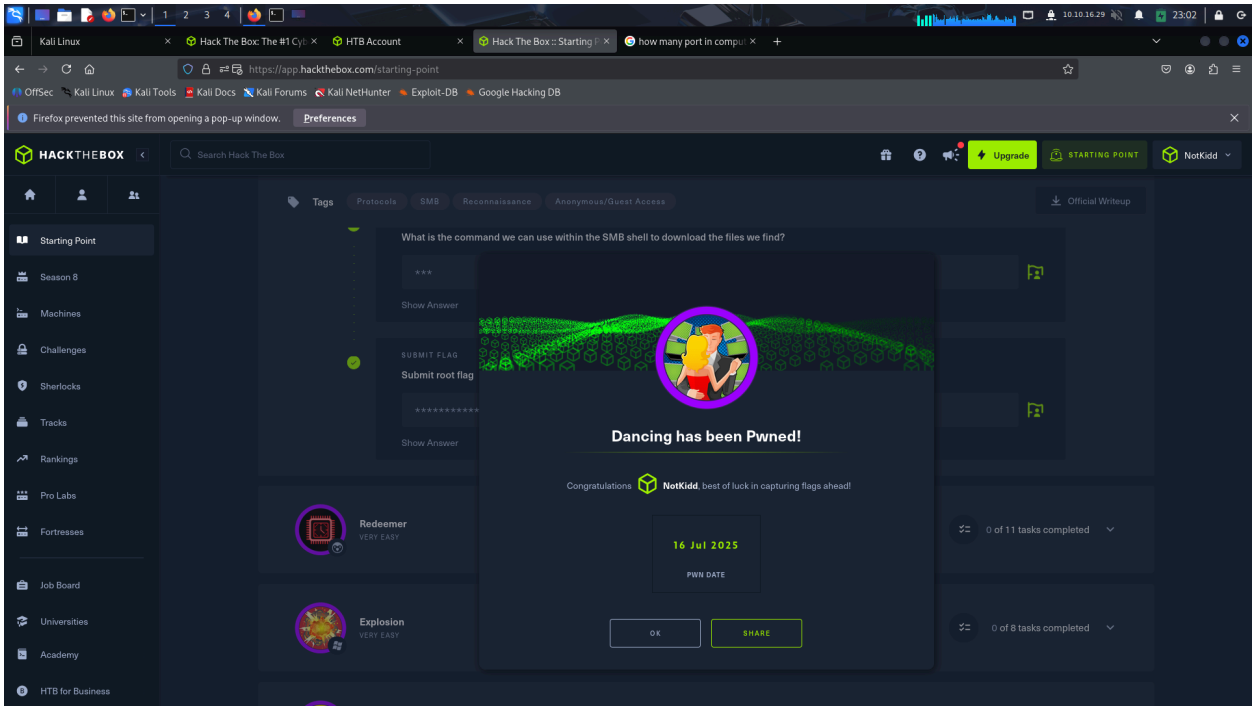

HACKTHEBOX
Starting Point
Season 8
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Fawn has been Pwned!
Congratulations NotKidd, best of luck in capturing flags ahead!
16 Jul 2025
PWN DATE
OK
SHARE
Dancing
Redeemer
Explosion
Preignition

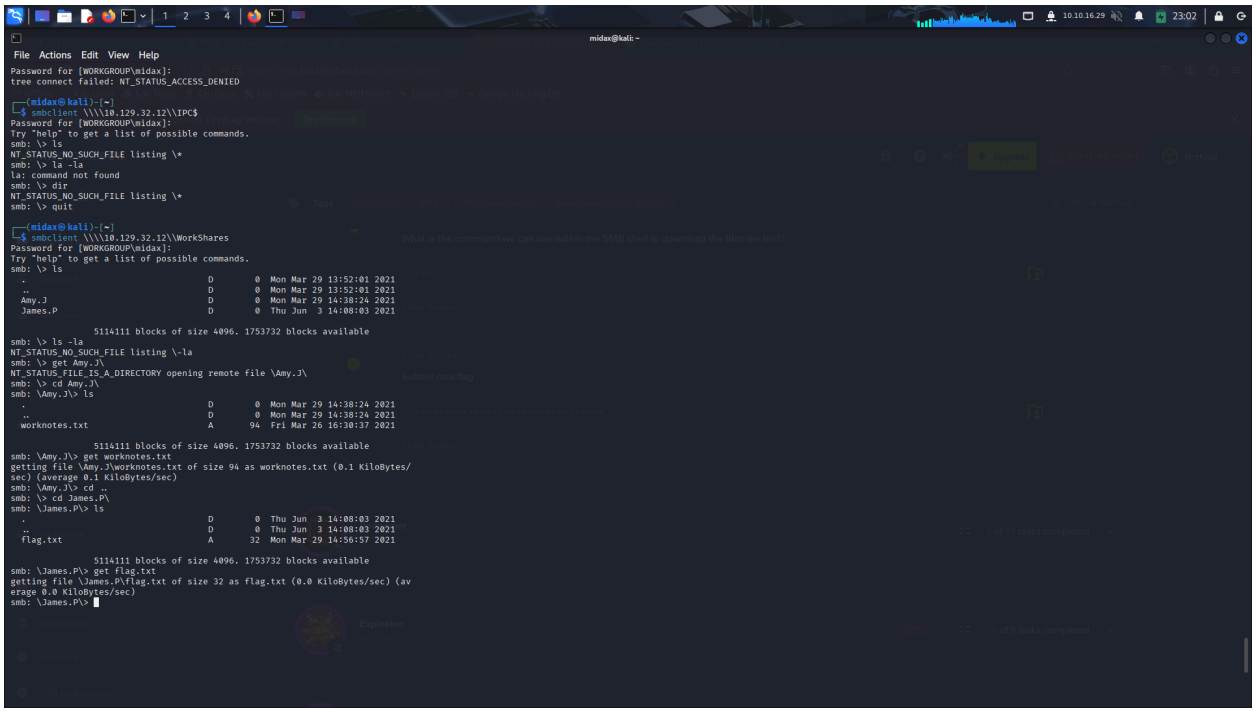

midax@kali: ~
File Actions Edit View Help
100% |*****| 32 0.10 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:01 (0.02 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||36739|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> cat flag.txt
?Invalid command.
ftp> nano flag.txt
?Invalid command.
ftp> quir
?Invalid command.
ftp> quit
221 Goodbye.
Desktop Downloads Music Public Videos
Documents flag.txt Pictures Templates
cat flag.txt
035db21c881520061c53e0536e44f815
Fawn has been Pwned!
Congratulations NotKidd, best of luck in capturing flags ahead!
16 Jul 2025
PWN DATE
OK
SHARE

Dancing


HACKTHEBOX
Starting Point
Season 8
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Tags
Protocols
SMB
Reconnaissance
Anonymous/Guest Access
Official Writeup
Show Answer
TASK 2
What port does SMB use to operate at?
Show Answer
TASK 3
What is the service name for port 445 that came up in our Nmap scan?
Show Answer
TASK 4
What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?
SUBMIT ANSWER
HINT


midax@kali: ~
File Actions Edit View Help
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.32.12 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
$ smbclient -L Dancing
do_connect: Connection to Dancing failed (Error NT_STATUS_NOT_FOUND)
$ smbclient -L 10.129.32.12
Password for [WORKGROUP\midax]:
Sharename Type Comment
ADMIN$ Disk Remote Admin
C$ Disk Default share
IPC$ IPC Remote IPC
WorkShares Disk
TASK 5
How many shares are there on Dancing
TASK 6
What is the name of the share we are able to access in the end with a blank password?
SUBMIT ANSWER
HINT
TASK 7
What is the command we can use within the SMB shell to download the files we find?
SUBMIT FLAG
Submit root flag


HACKTHEBOX
Starting Point
Season 8
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
What is the command we can use within the SMB shell to download the files we find?
Show Answer
Submit root flag
Show Answer
Dancing has been Pwned!
Congratulations NotKidd, best of luck in capturing flags ahead!
16 Jul 2025
PWN DATE
OK
SHARE
Redeemer
VERY EASY
Explosion
VERY EASY
0 of 11 tasks completed
0 of 8 tasks completed


File Actions Edit View Help
Password for [WORKGROUP\midax]:
tree connect failed: NT_STATUS_ACCESS_DENIED
smbclient \\\\10.129.32.12\\IPC$
Password for [WORKGROUP\midax]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NO_SUCH_FILE listing *
smb: \> la -la
la: command not found
smb: \> dir
NT_STATUS_NO_SUCH_FILE listing *
smb: \> quit
smbclient \\\\10.129.32.12\\WorkShares
Password for [WORKGROUP\midax]:
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
5114111 blocks of size 4096. 1753732 blocks available
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> get Amy.J\
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \Amy.J\
smb: \> cd Amy.J\
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
5114111 blocks of size 4096. 1753732 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.1 KiloBytes/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
5114111 blocks of size 4096. 1753732 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.P\>

Redeemer