Nama : Nabil Ulil Albab
Npm : 23670010

1. phising

Phishing adalah teknik hacking dengan cara meng-cloning atau meniru website resmi untuk mendapatkan data sensitif seperti kredensial login, kartu kredit, OTP, dan informasi pribadi lainnya.
Cara mengatasinya Selalu cross-check domain, aktifkan 2FA, gunakan password manager, dan hindari klik link mencurigakan.

2. dns spoofing

DNS spoofing adalah serangan yang memanipulasi sistem DNS dengan cara mengubah hasil resolusi domain sehingga korban diarahkan ke alamat IP palsu.
contoh: user ingin membuka bank.com, tetapi diarahkan ke website tiruan.
Cara mengatasinya

- Gunakan DNSSEC
- Gunakan DoH/DoT (DNS over HTTPS/TLS)
- Flush DNS cache jika mencurigakan
- Hindari jaringan WiFi publik tanpa VPN

3. cookie theft

Cookie theft adalah teknik mencuri cookie sesi pengguna, yang berisi token autentikasi. Jika hacker mendapat cookie ini, mereka bisa login sebagai korban tanpa password.
Metode umum XSS, sniffing di jaringan publik, atau malware.cara mengatasinya

- Gunakan HTTPOnly cookie
- Aktifkan SameSite
- Gunakan HTTPS
- Logout setelah penggunaan
- Jangan akses website sensitif di WiFi publik

4. cross site scripting

XSS adalah serangan yang menyisipkan kode JavaScript berbahaya ke dalam website. Kode tersebut berjalan di browser korban, memungkinkan pencurian cookie, redirect, keylogging, deface, dll.
Jenis XSS:

- Reflected
- Stored
- DOM-based

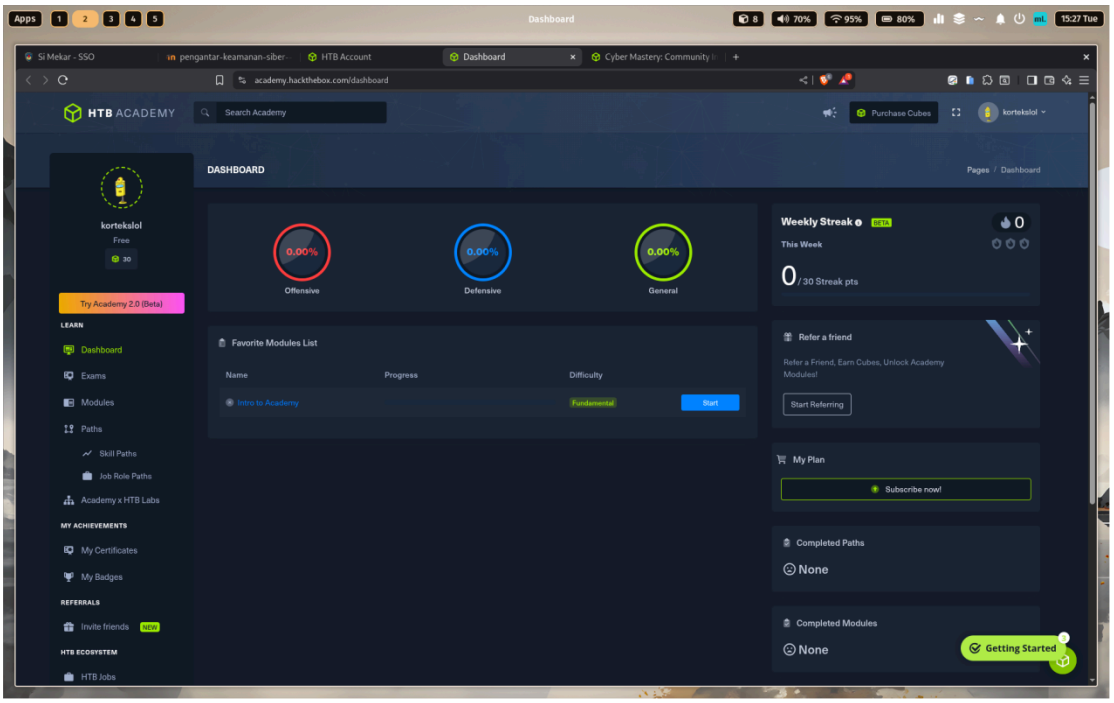
Cara mengatasinya dengan

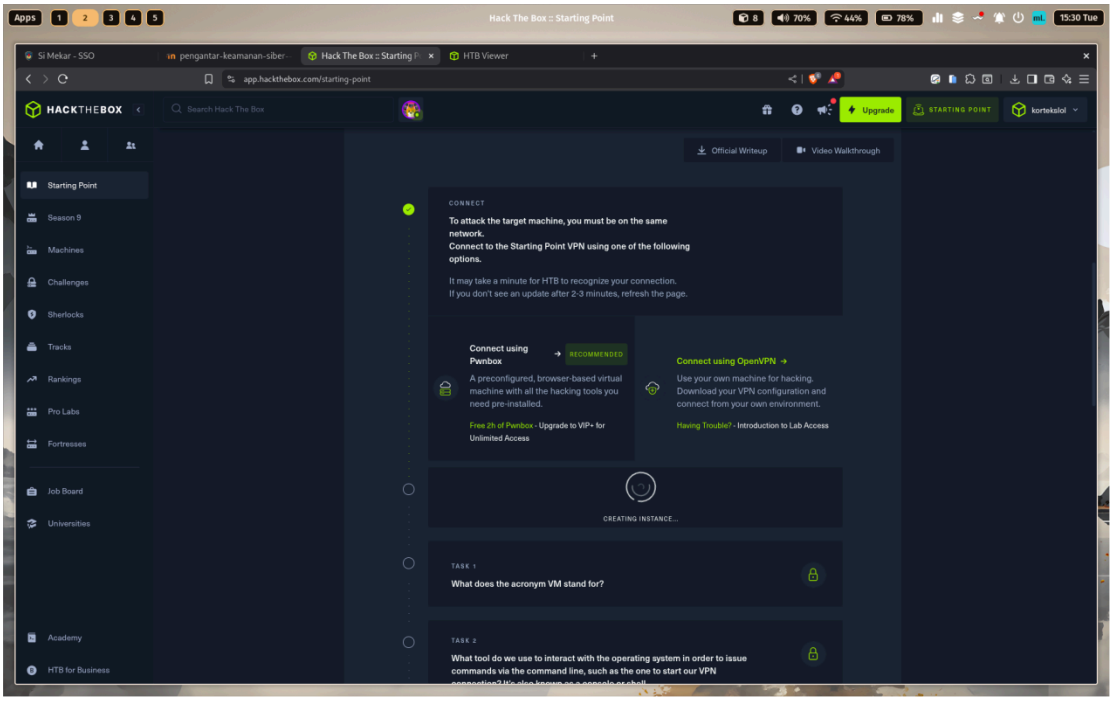
- Gunakan escaping pada input user
- Gunakan Content Security Policy (CSP)
- Validasi input dan sanitasi output
- Jangan pernah langsung menampilkan input user ke halaman

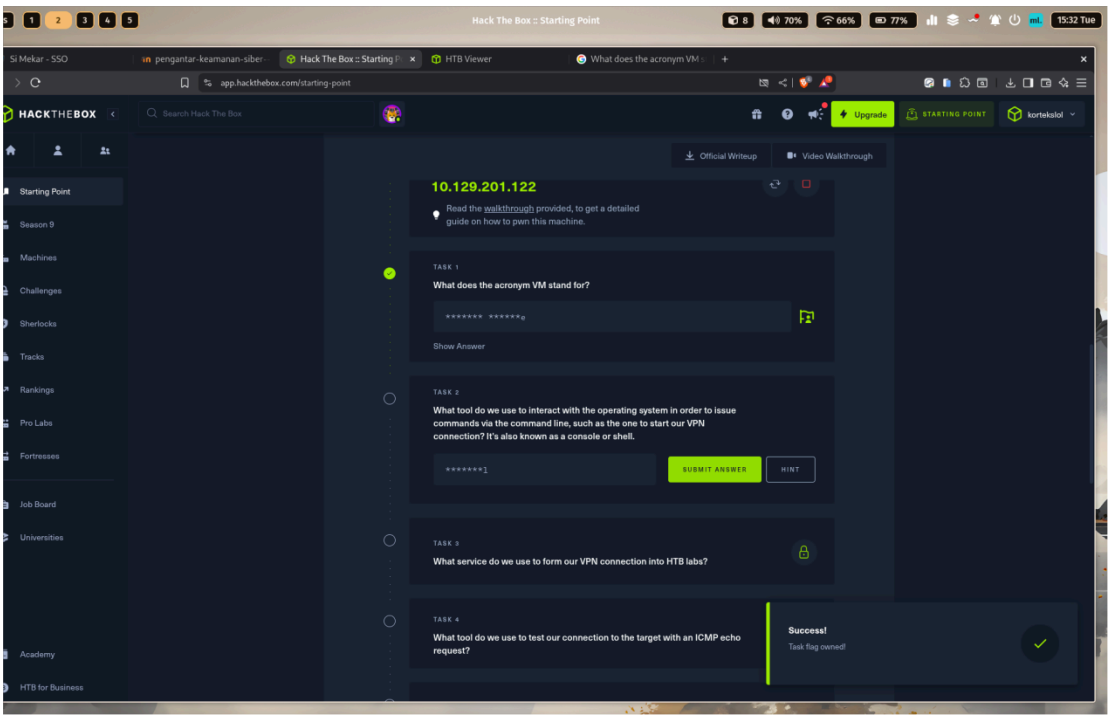
5. sql injection

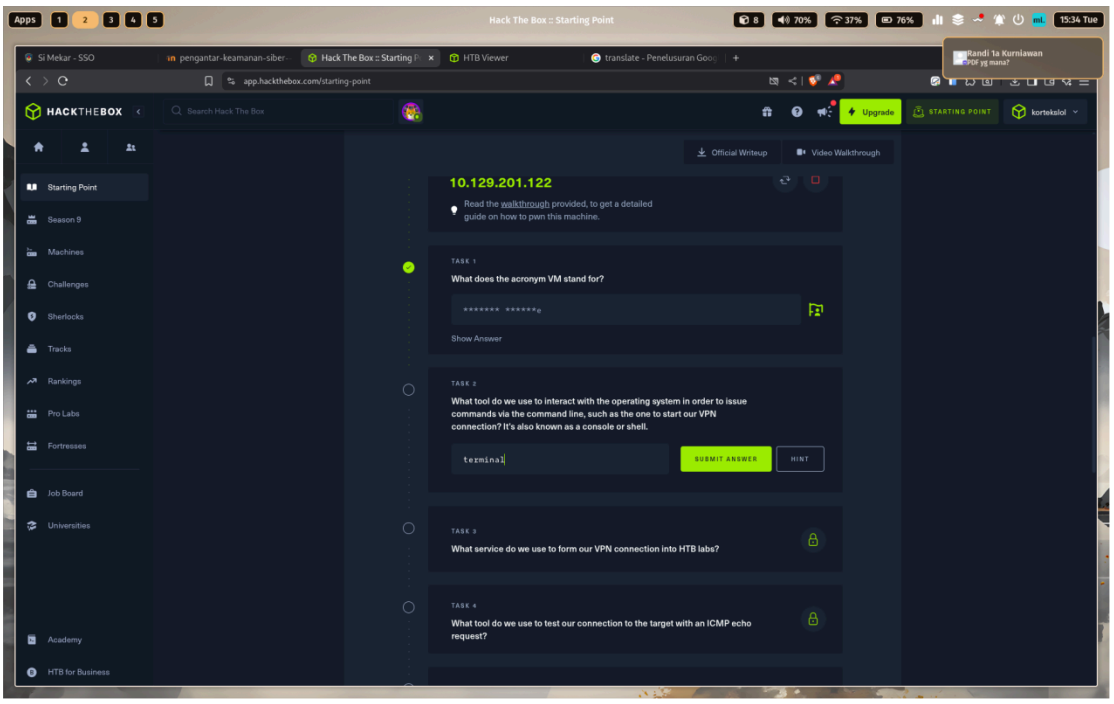
biasanya memannfaatkan form untuk injject query , dan untuk cara amankan dengan cara csrf token

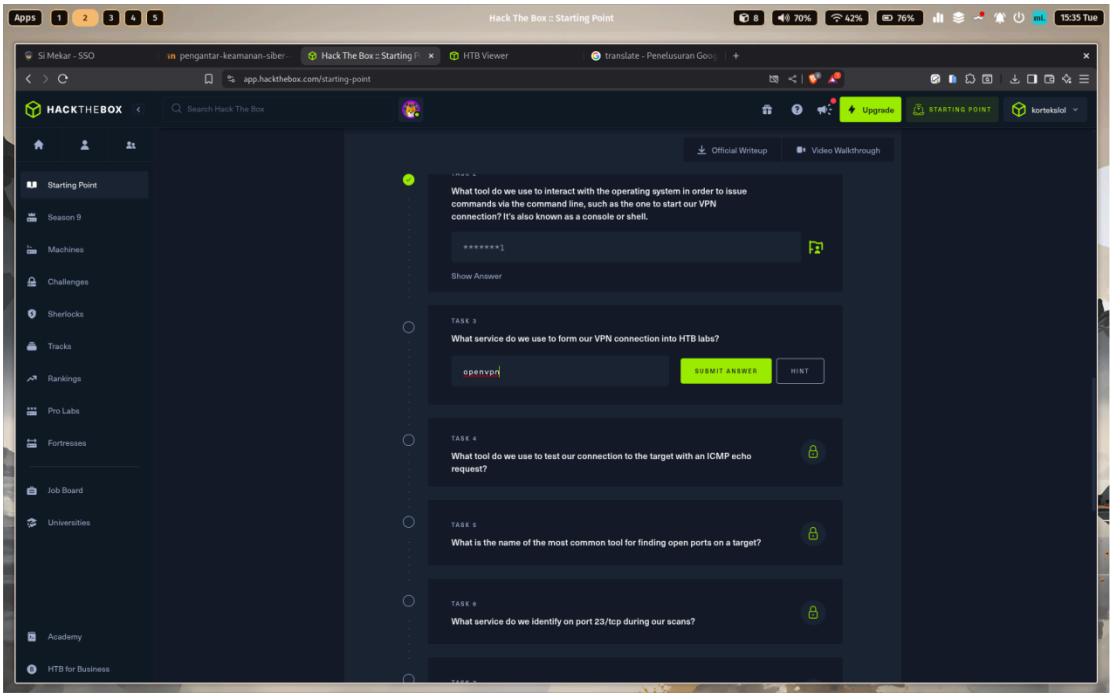
ulasan hackthebock :
untuk sourse 1,2,3 membantu user untuk mengenal perintah2 dasar untuk mengoperasikan os dengan base unix , belum masuk materi hacking, masih dalam tahap pengenalan hal2 fundamental tengtang protocol2 transfer file , dan pengenalan client server

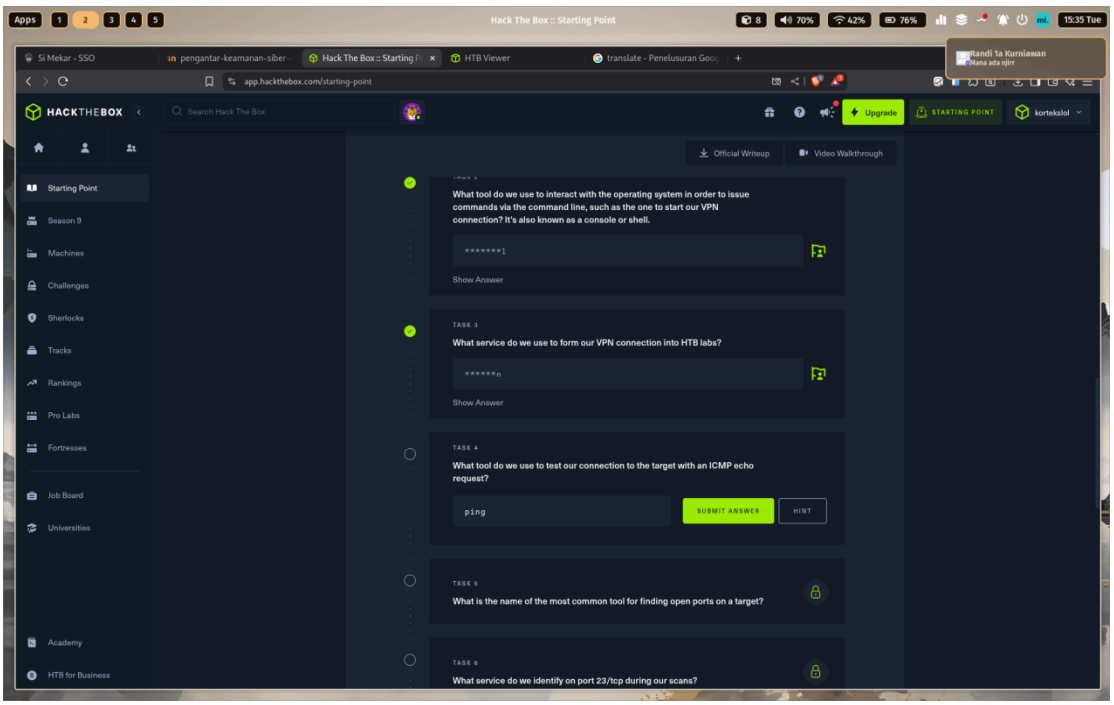


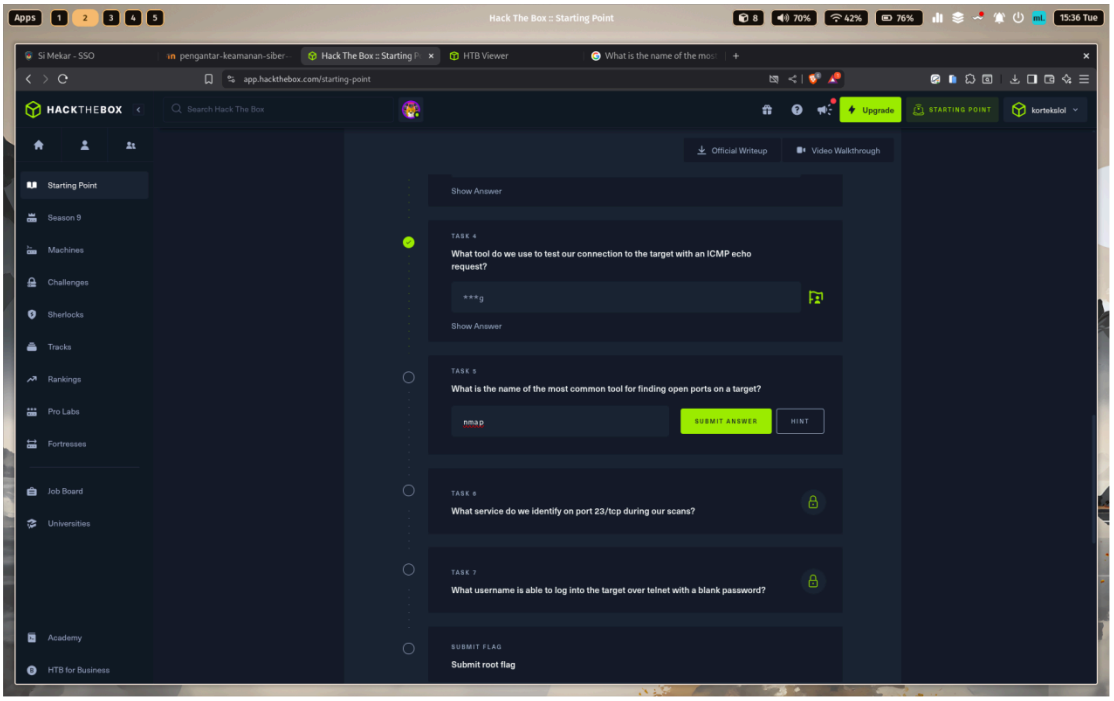


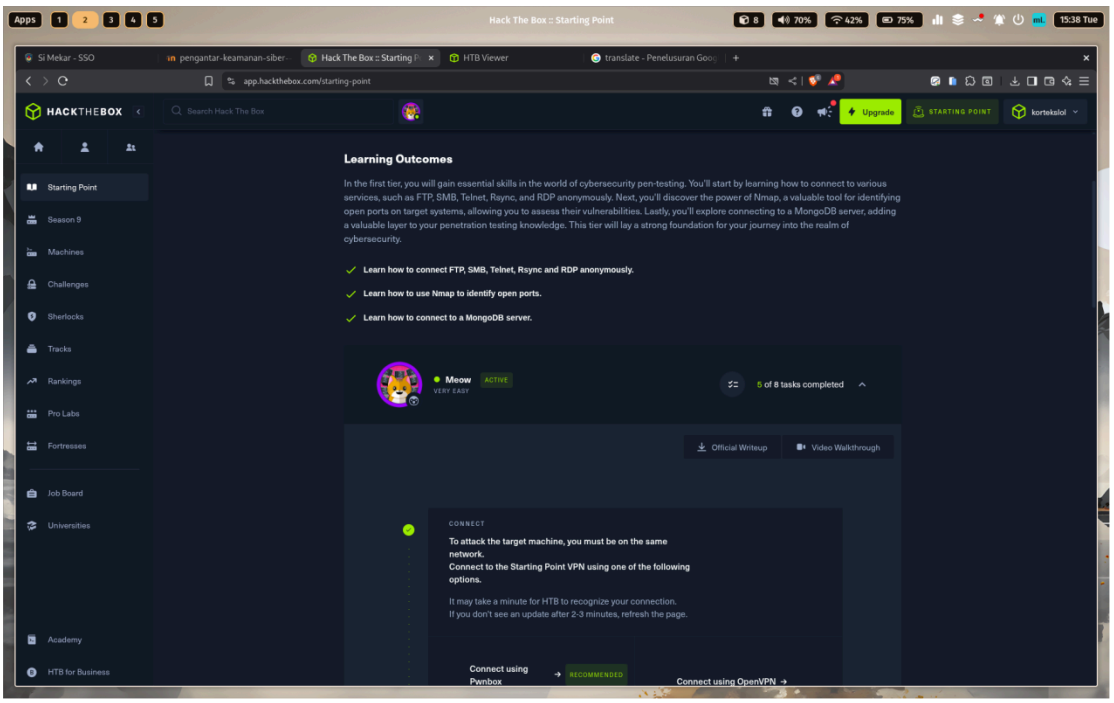

Hack The Box :: Starting Point
HACKTHEBOX
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Official Writeup
Video Walkthrough
10.129.201.122
Read the walkthrough provided, to get a detailed guide on how to pwn this machine.
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.
SUBMIT ANSWER
HINT
TASK 3
What service do we use to form our VPN connection into HTB labs?
TASK 4
What tool do we use to test our connection to the target with an ICMP echo request?
Success!
Task flag owned!

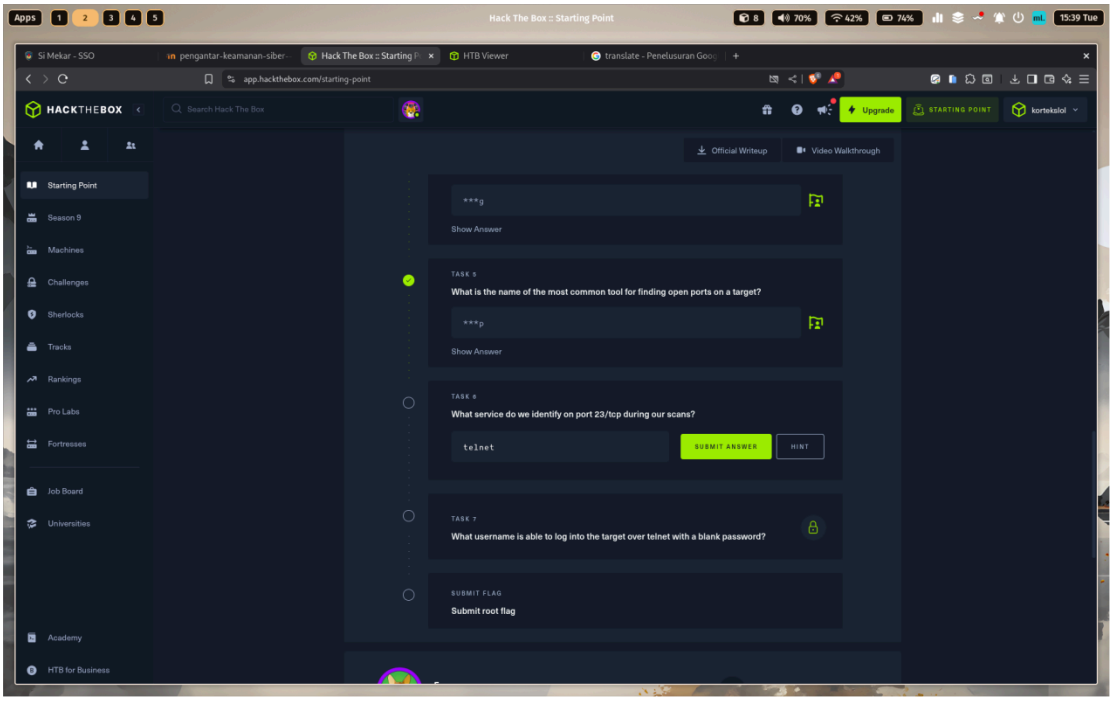

Hack The Box :: Starting Point
HACKTHEBOX
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Official Writeup
Video Walkthrough
10.129.201.122
Read the walkthrough provided, to get a detailed guide on how to pwn this machine.
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.
terminal
SUBMIT ANSWER
HINT
TASK 3
What service do we use to form our VPN connection into HTB labs?
TASK 4
What tool do we use to test our connection to the target with an ICMP echo request?

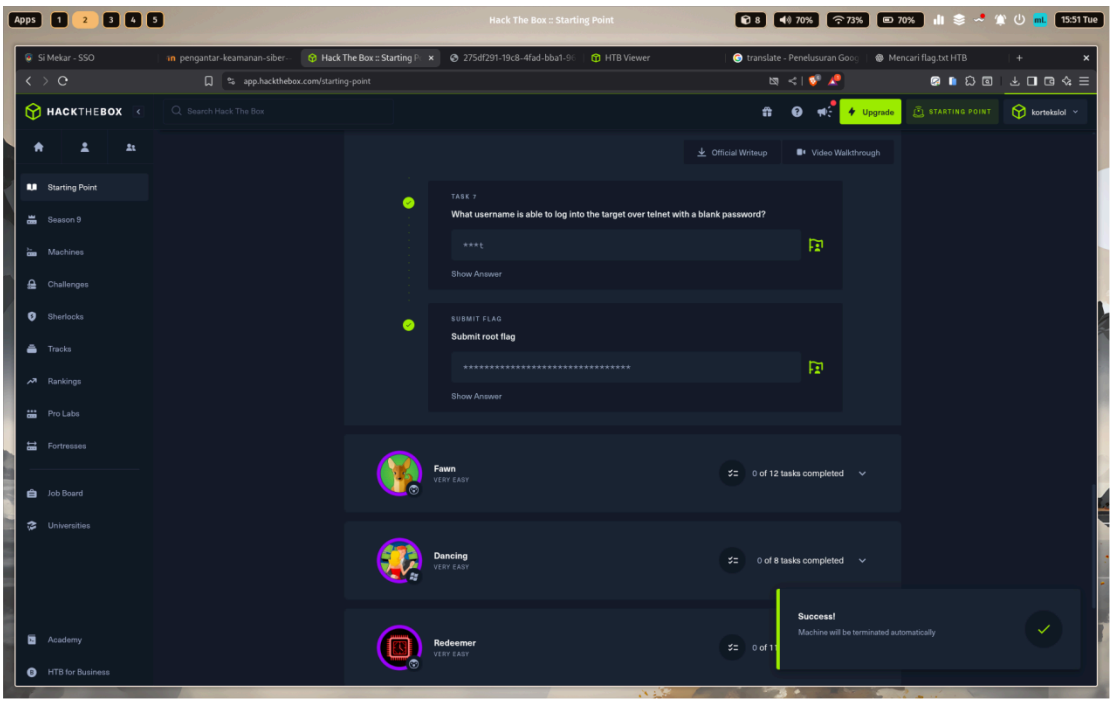

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
korteksiol
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
What tool do we use 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.
*******1
Show Answer
TASK 3
What service do we use to form our VPN connection into HTB labs?
openvpn
SUBMIT ANSWER
HINT
TASK 4
What tool do we use to test our connection to the target with an ICMP echo request?
TASK 5
What is the name of the most common tool for finding open ports on a target?
TASK 6
What service do we identify on port 23/tcp during our scans?

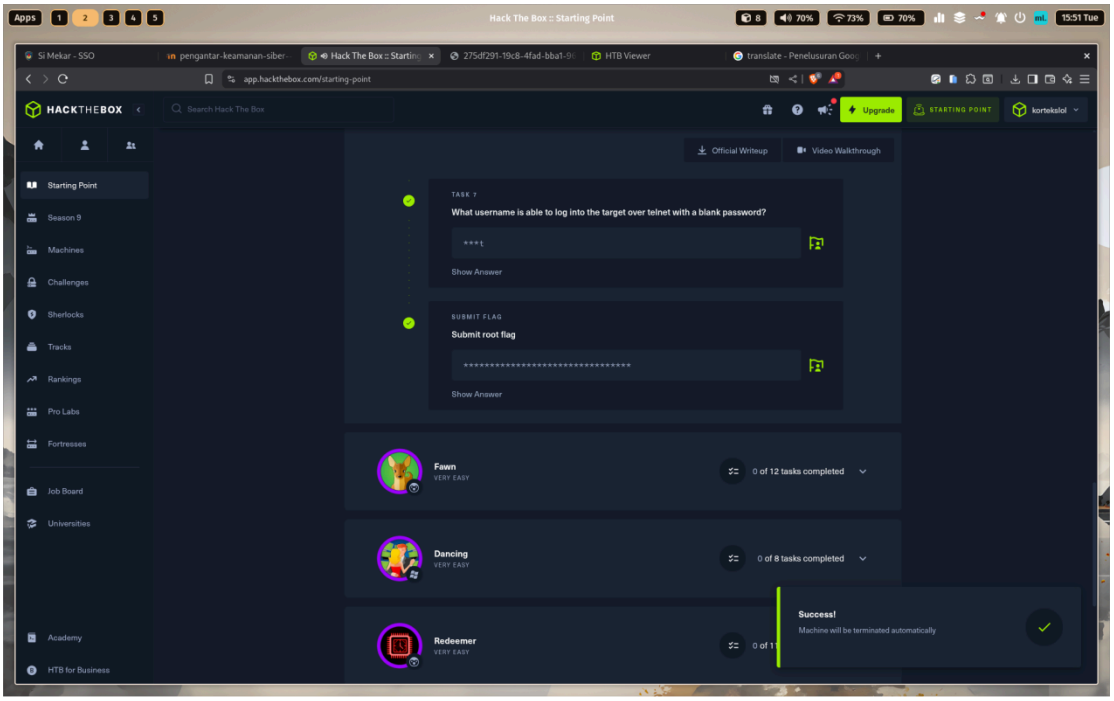

Hack The Box :: Starting Point
Randi Ta Kurniawan
Mana ada njirr
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
korteksiol
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
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.
*******1
Show Answer
TASK 3
What service do we use to form our VPN connection into HTB labs?
******n
Show Answer
TASK 4
What tool do we use to test our connection to the target with an ICMP echo request?
ping
SUBMIT ANSWER
HINT
TASK 5
What is the name of the most common tool for finding open ports on a target?
TASK 6
What service do we identify on port 23/tcp during our scans?

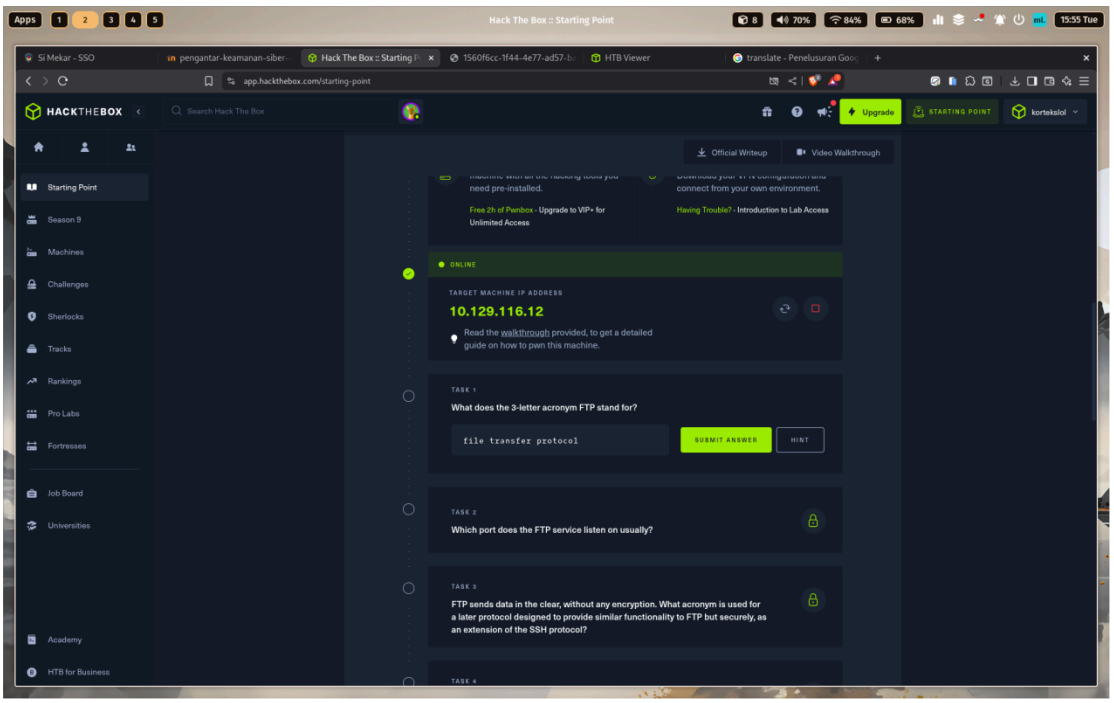

Apps
Hack The Box :: Starting Point
15:36 Tue
Si Mekar - SSO
pengantar-keamanan-siber-...
Hack The Box :: Starting P...
HTB Viewer
What is the name of the mos...
app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
Upgrade
STARTING POINT
korteksilol
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Show Answer
TASK 4
What tool do we use to test our connection to the target with an ICMP echo request?
***g
Show Answer
TASK 5
What is the name of the most common tool for finding open ports on a target?
nmap
SUBMIT ANSWER
HINT
TASK 6
What service do we identify on port 23/tcp during our scans?
TASK 7
What username is able to log into the target over telnet with a blank password?
SUBMIT FLAG
Submit root flag

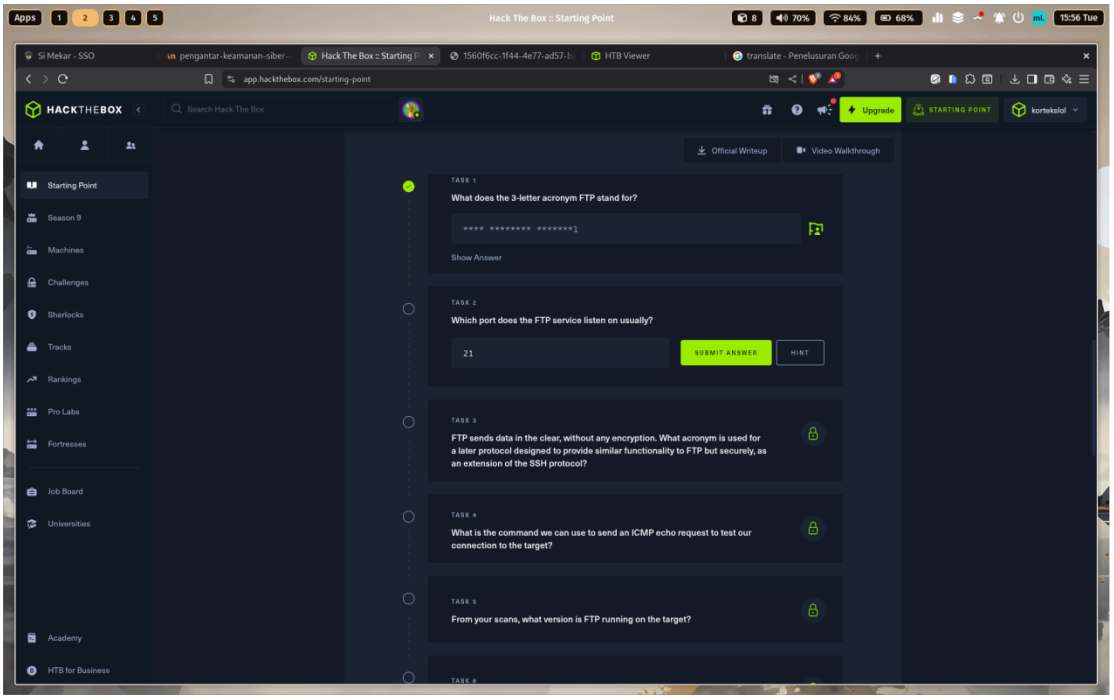

Apps
Hack The Box :: Starting Point
15:38 Tue
Si Mekar - SSO
pengantar-keamanan-siber-...
Hack The Box :: Starting P...
HTB Viewer
translate - Penelusuran Goog...
app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
Upgrade
STARTING POINT
korteksilol
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Learning Outcomes
In the first tier, you will gain essential skills in the world of cybersecurity pen-testing. You'll start by learning how to connect to various services, such as FTP, SMB, Telnet, Rsync, and RDP anonymously. Next, you'll discover the power of Nmap, a valuable tool for identifying open ports on target systems, allowing you to assess their vulnerabilities. Lastly, you'll explore connecting to a MongoDB server, adding a valuable layer to your penetration testing knowledge. This tier will lay a strong foundation for your journey into the realm of cybersecurity.
Learn how to connect FTP, SMB, Telnet, Rsync and RDP anonymously.
Learn how to use Nmap to identify open ports.
Learn how to connect to a MongoDB server.
Meow
VERY EASY
ACTIVE
5 of 8 tasks completed
Official Writeup
Video Walkthrough
CONNECT
To attack the target machine, you must be on the same network.
Connect to the Starting Point VPN using one of the following options.
It may take a minute for HTB to recognize your connection.
If you don't see an update after 2-3 minutes, refresh the page.
Connect using Pwnbox
RECOMMENDED
Connect using OpenVPN

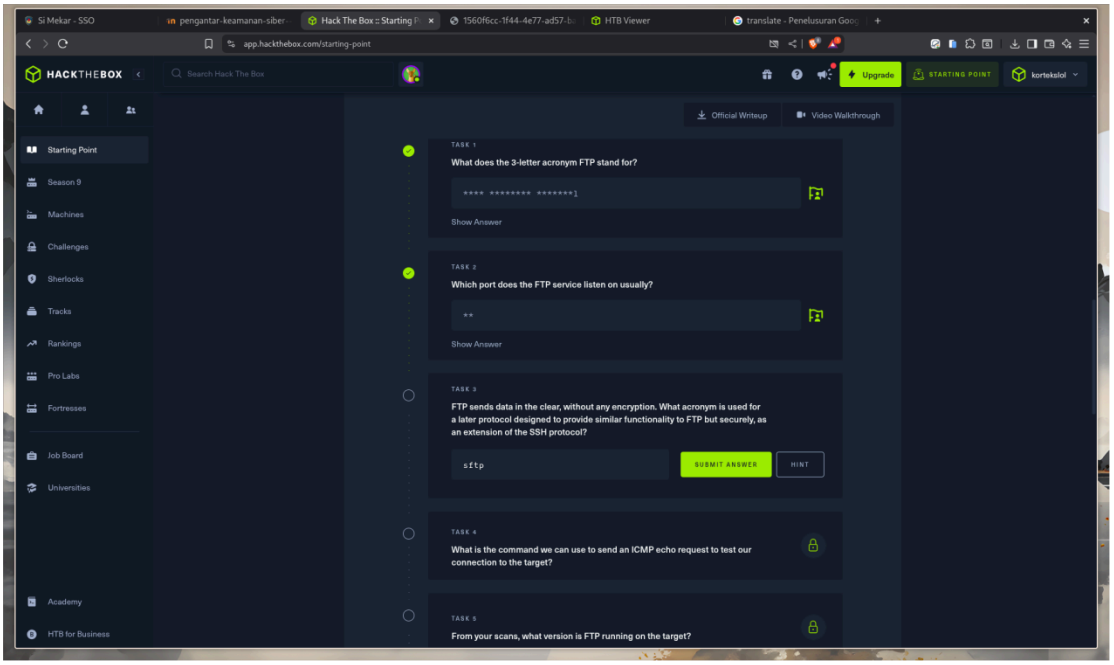

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Starting Point
Official Writeup
Video Walkthrough
Show Answer
TASK 5
What is the name of the most common tool for finding open ports on a target?
Show Answer
TASK 6
What service do we identify on port 23/tcp during our scans?
telnet
SUBMIT ANSWER
HINT
TASK 7
What username is able to log into the target over telnet with a blank password?
SUBMIT FLAG
Submit root flag

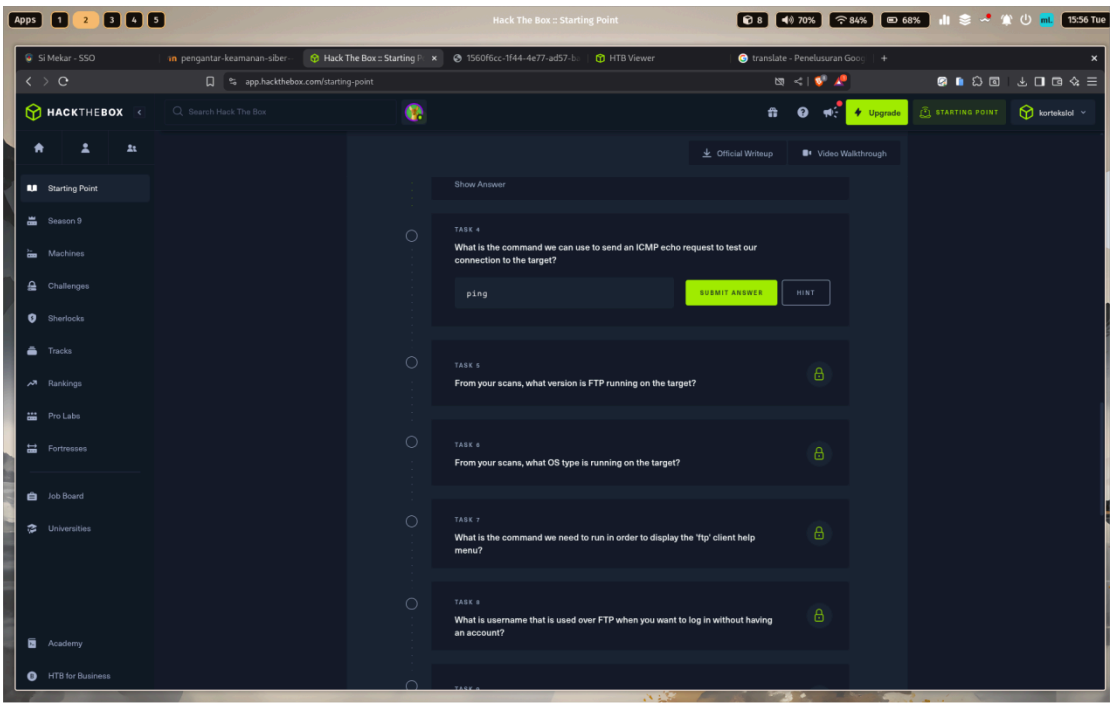

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Starting Point
Official Writeup
Video Walkthrough
TASK 7
What username is able to log into the target over telnet with a blank password?
Show Answer
SUBMIT FLAG
Submit root flag
Show Answer
Fawn
VERY EASY
0 of 12 tasks completed
Dancing
VERY EASY
0 of 8 tasks completed
Redeemer
VERY EASY
Success!
Machine will be terminated automatically

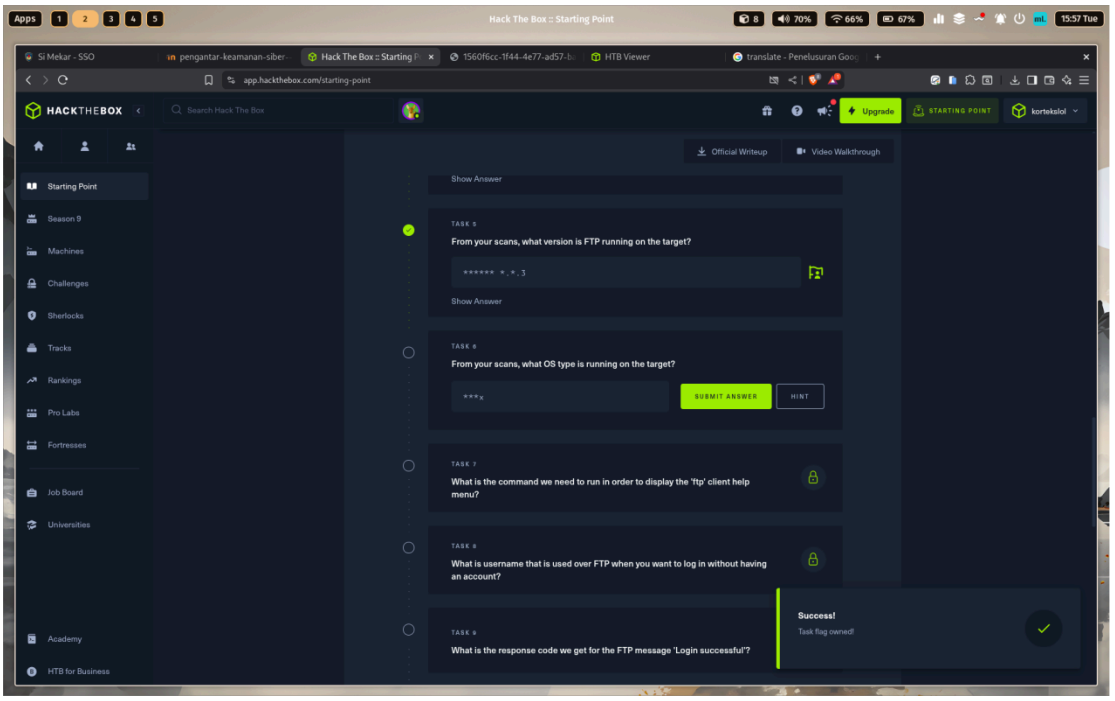

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
TASK 7
What username is able to log into the target over telnet with a blank password?
Show Answer
SUBMIT FLAG
Submit root flag
Show Answer
Fawn
VERY EASY
0 of 12 tasks completed
Dancing
VERY EASY
0 of 8 tasks completed
Redeemer
VERY EASY
Success!
Machine will be terminated automatically

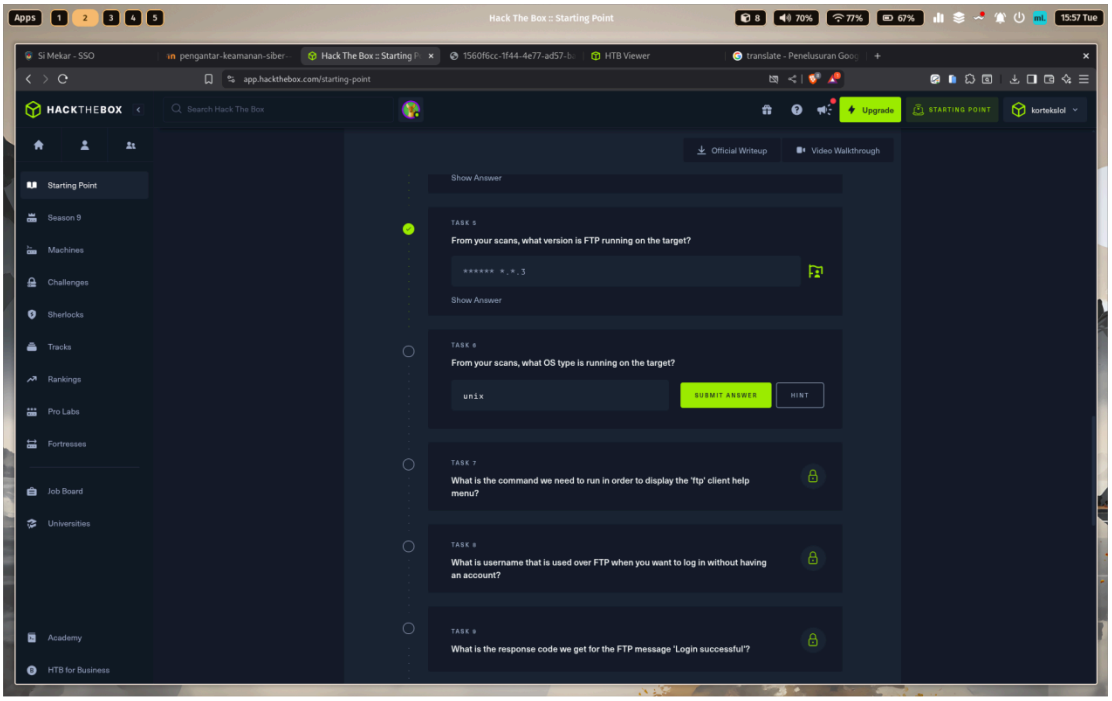

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access
Having Trouble? - Introduction to Lab Access
ONLINE
TARGET MACHINE IP ADDRESS
10.129.116.12
Read the walkthrough provided, to get a detailed guide on how to pwn this machine.
TASK 1
What does the 3-letter acronym FTP stand for?
file transfer protocol
SUBMIT ANSWER
HINT
TASK 2
Which port does the FTP service listen on usually?
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?
TASK 4

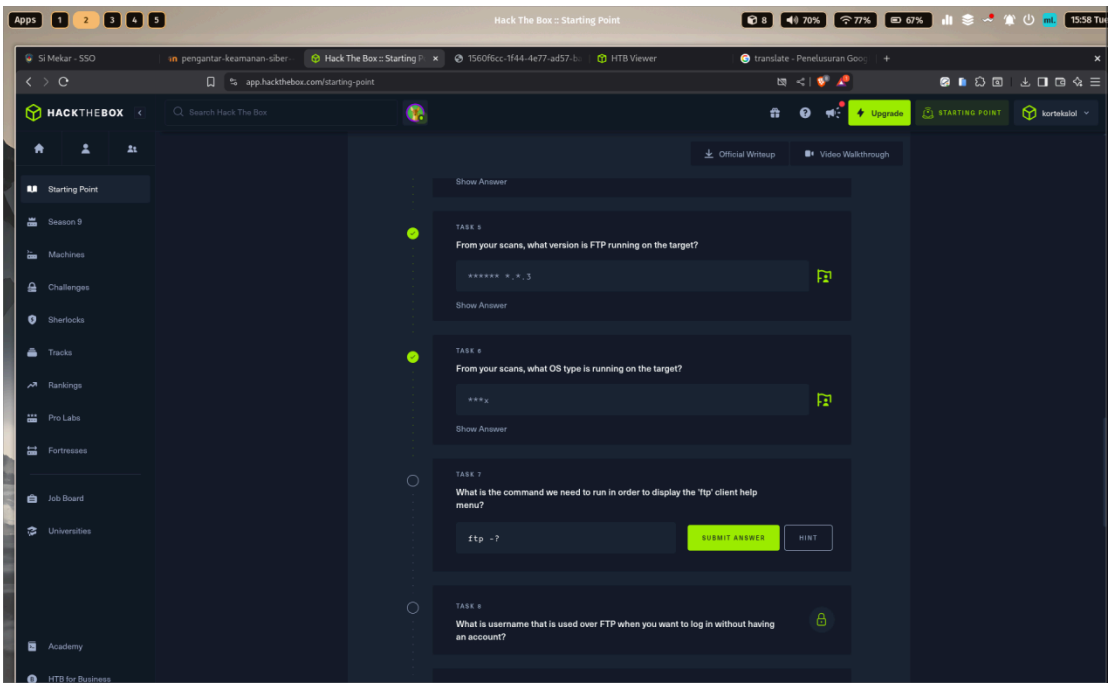

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
Upgrade
STARTING POINT
kortekslol
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
TASK 1
What does the 3-letter acronym FTP stand for?
**** ******** *******1
Show Answer
TASK 2
Which port does the FTP service listen on usually?
21
SUBMIT ANSWER
HINT
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?
TASK 4
What is the command we can use to send an ICMP echo request to test our connection to the target?
TASK 5
From your scans, what version is FTP running on the target?

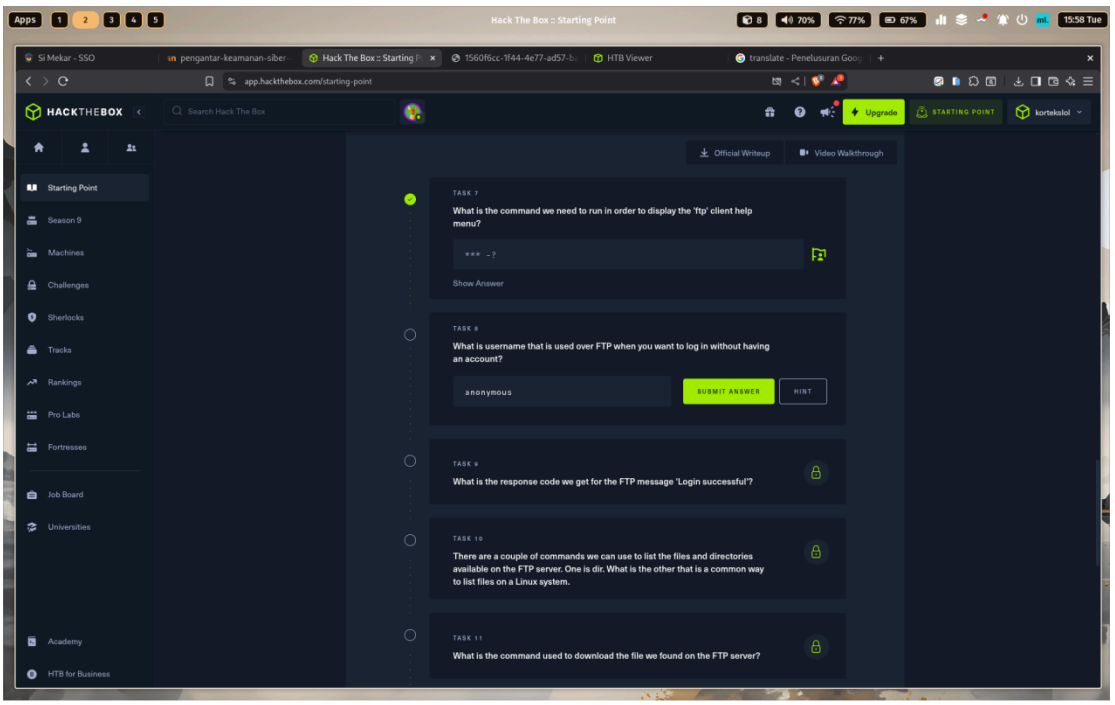

app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
Upgrade
STARTING POINT
kortekslol
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
TASK 1
What does the 3-letter acronym FTP stand for?
**** ******** *******1
Show Answer
TASK 2
Which port does the FTP service listen on usually?
**
Show Answer
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?
sftp
SUBMIT ANSWER
HINT
TASK 4
What is the command we can use to send an ICMP echo request to test our connection to the target?
TASK 5
From your scans, what version is FTP running on the target?

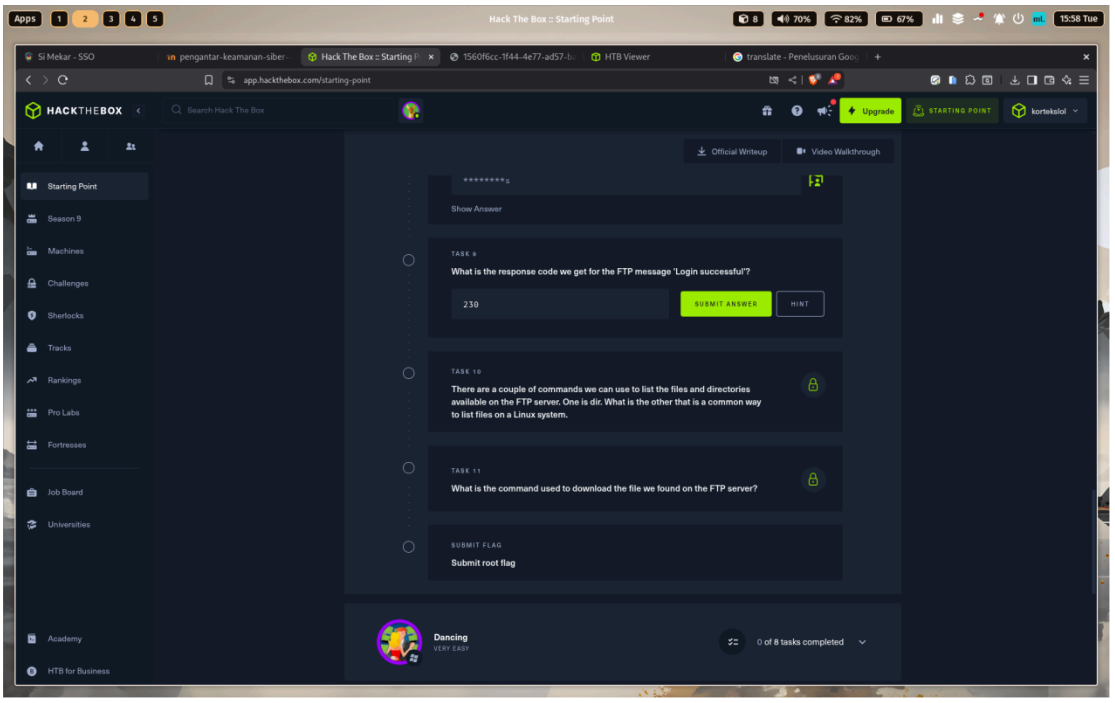

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
korteksiol
Official Writeup
Video Walkthrough
Show Answer
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
TASK 4
What is the command we can use to send an ICMP echo request to test our connection to the target?
ping
SUBMIT ANSWER
HINT
TASK 5
From your scans, what version is FTP running on the target?
TASK 6
From your scans, what OS type is running on the target?
TASK 7
What is the command we need to run in order to display the 'ftp' client help menu?
TASK 8
What is username that is used over FTP when you want to log in without having an account?

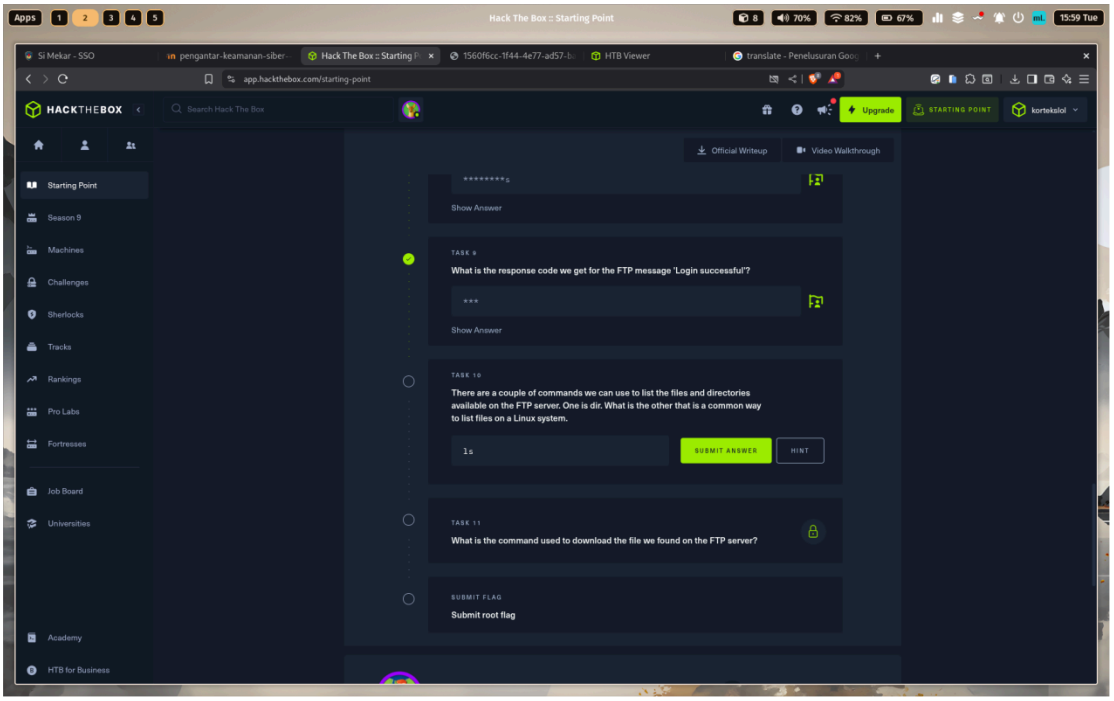

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
korteksiol
Official Writeup
Video Walkthrough
Show Answer
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
TASK 5
From your scans, what version is FTP running on the target?
Show Answer
TASK 6
From your scans, what OS type is running on the target?
SUBMIT ANSWER
HINT
TASK 7
What is the command we need to run in order to display the 'ftp' client help menu?
TASK 8
What is username that is used over FTP when you want to log in without having an account?
TASK 9
What is the response code we get for the FTP message 'Login successful'?
Success!
Task flag owned!

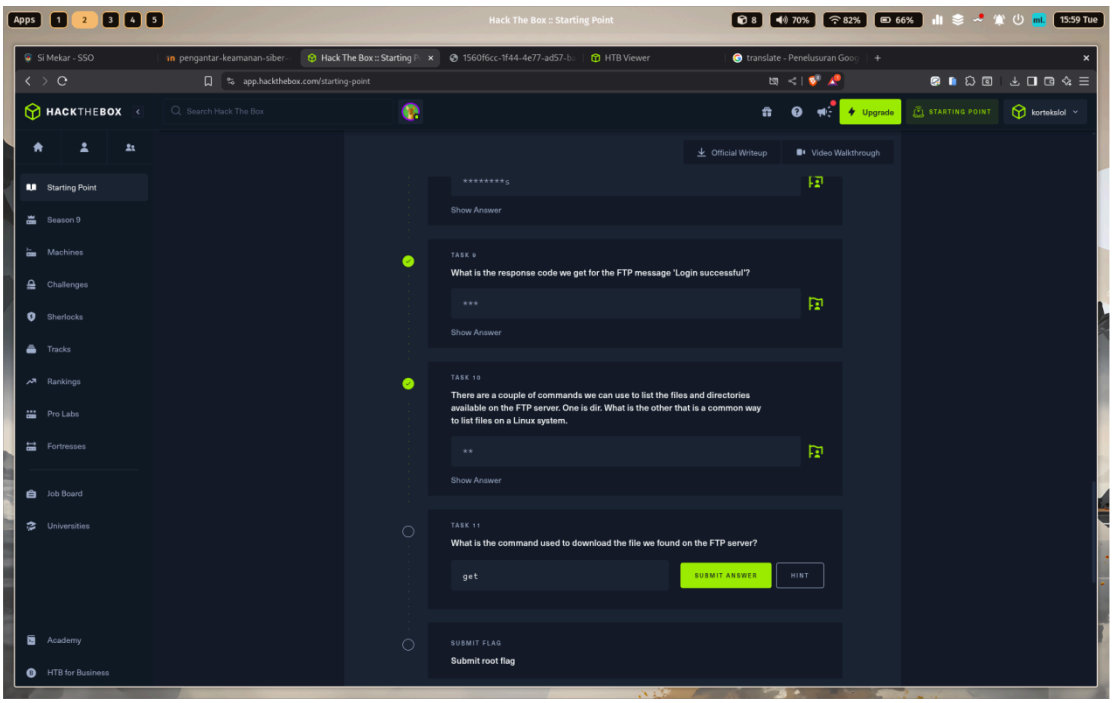

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Video Walkthrough
Show Answer
TASK 5
From your scans, what version is FTP running on the target?
****** *.*.3
Show Answer
TASK 6
From your scans, what OS type is running on the target?
unix
SUBMIT ANSWER
HINT
TASK 7
What is the command we need to run in order to display the 'ftp' client help menu?
TASK 8
What is username that is used over FTP when you want to log in without having an account?
TASK 9
What is the response code we get for the FTP message 'Login successful'?
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business

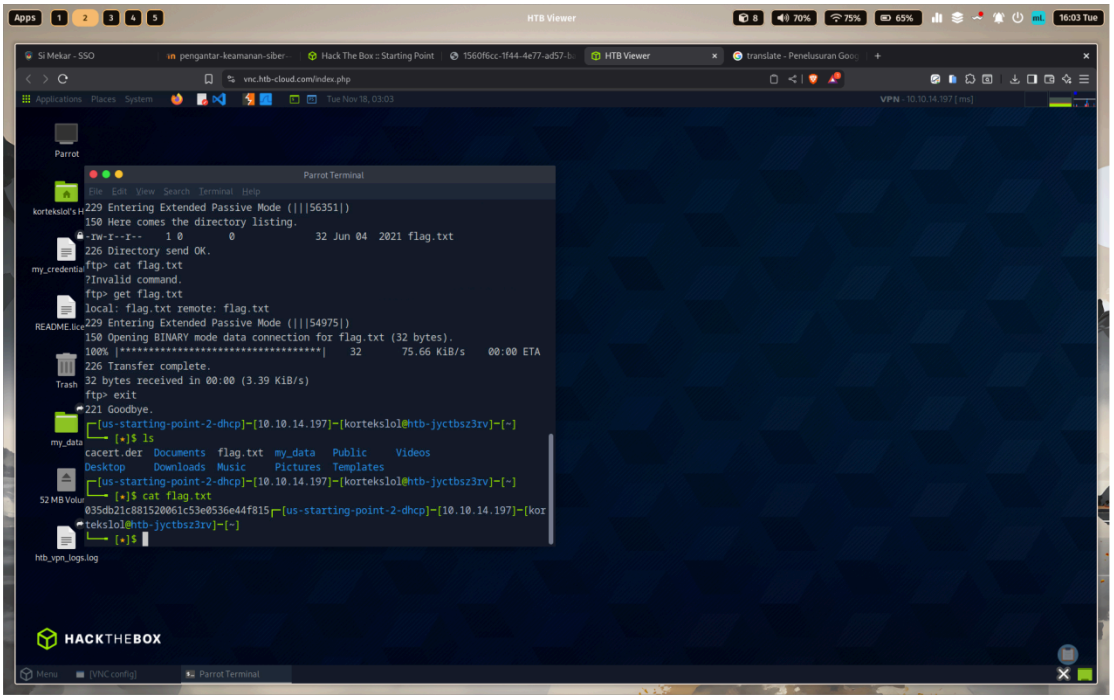

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Video Walkthrough
Show Answer
TASK 5
From your scans, what version is FTP running on the target?
****** *.*.3
Show Answer
TASK 6
From your scans, what OS type is running on the target?
***x
Show Answer
TASK 7
What is the command we need to run in order to display the 'ftp' client help menu?
ftp -?
SUBMIT ANSWER
HINT
TASK 8
What is username that is used over FTP when you want to log in without having an account?
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business

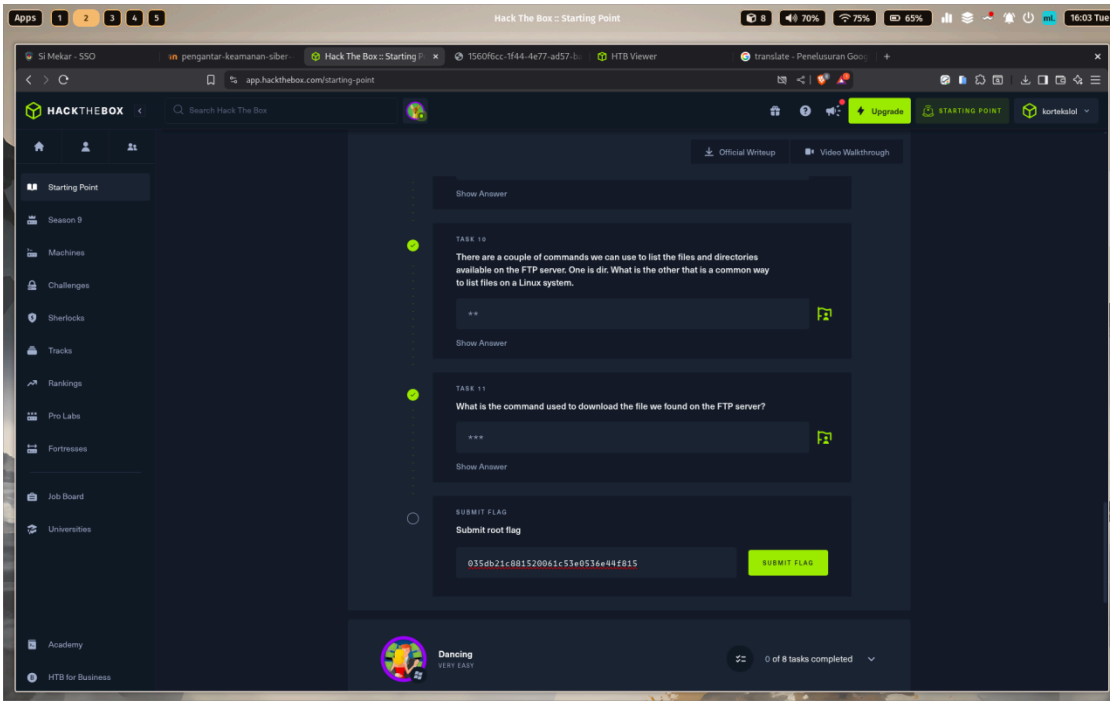

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
TASK 7
What is the command we need to run in order to display the 'ftp' client help menu?
*** -?
Show Answer
TASK 8
What is username that is used over FTP when you want to log in without having an account?
anonymous
SUBMIT ANSWER
HINT
TASK 9
What is the response code we get for the FTP message 'Login successful'?
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.
TASK 11
What is the command used to download the file we found on the FTP server?

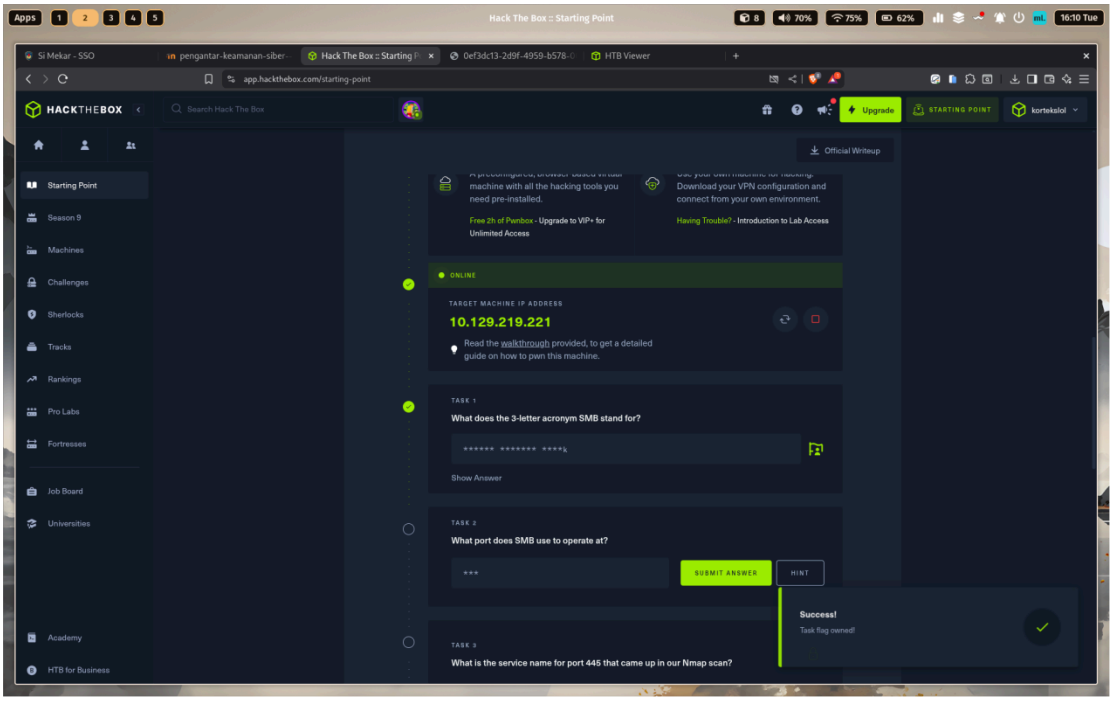

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Video Walkthrough
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Show Answer
TASK 9
What is the response code we get for the FTP message 'Login successful'?
230
SUBMIT ANSWER
HINT
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.
TASK 11
What is the command used to download the file we found on the FTP server?
SUBMIT FLAG
Submit root flag
Dancing
VERY EASY
0 of 8 tasks completed

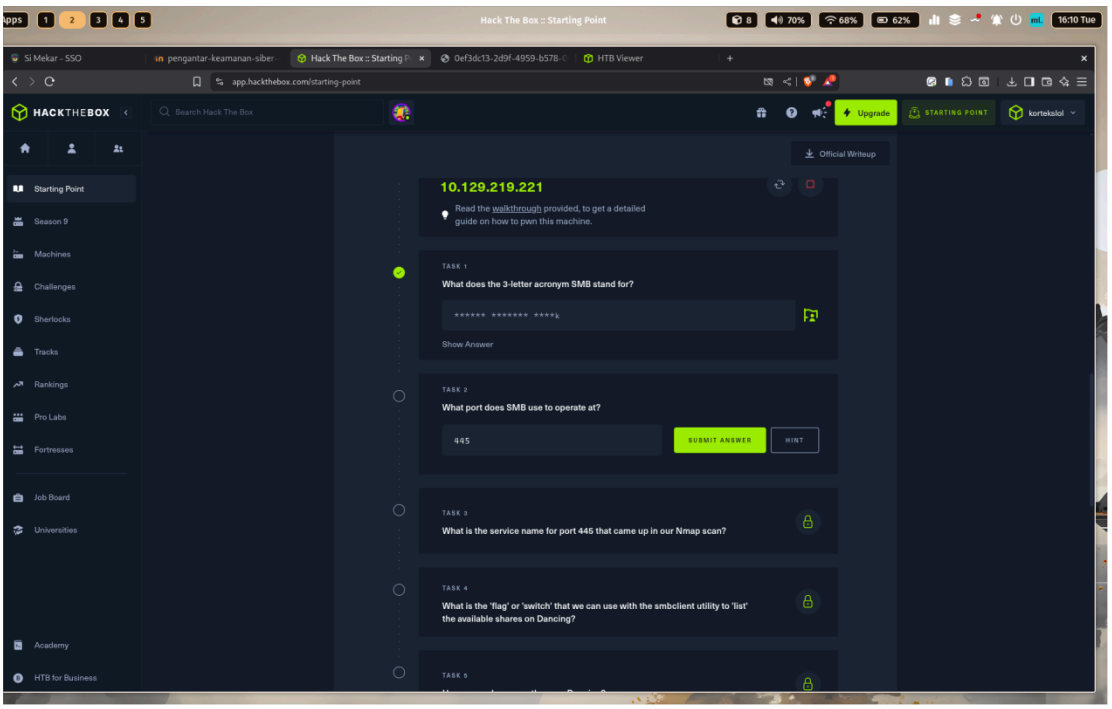

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Official Writeup
Video Walkthrough
Show Answer
TASK 9
What is the response code we get for the FTP message 'Login successful'?
***
Show Answer
TASK 10
There are a couple of commands we can use to list the files and directories 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
SUBMIT ANSWER
HINT
TASK 11
What is the command used to download the file we found on the FTP server?
SUBMIT FLAG
Submit root flag
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business

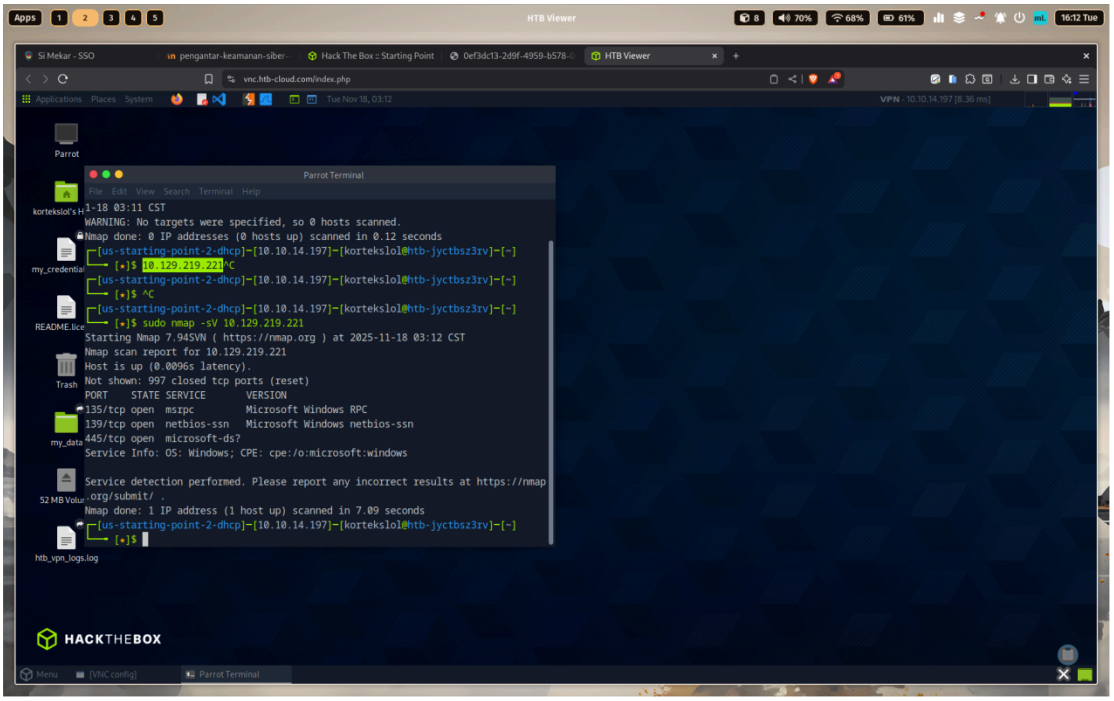

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Official Writeup
Video Walkthrough
Show Answer
TASK 9
What is the response code we get for the FTP message 'Login successful'?
***
Show Answer
TASK 10
There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.
**
Show Answer
TASK 11
What is the command used to download the file we found on the FTP server?
get
SUBMIT ANSWER
HINT
SUBMIT FLAG
Submit root flag
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business

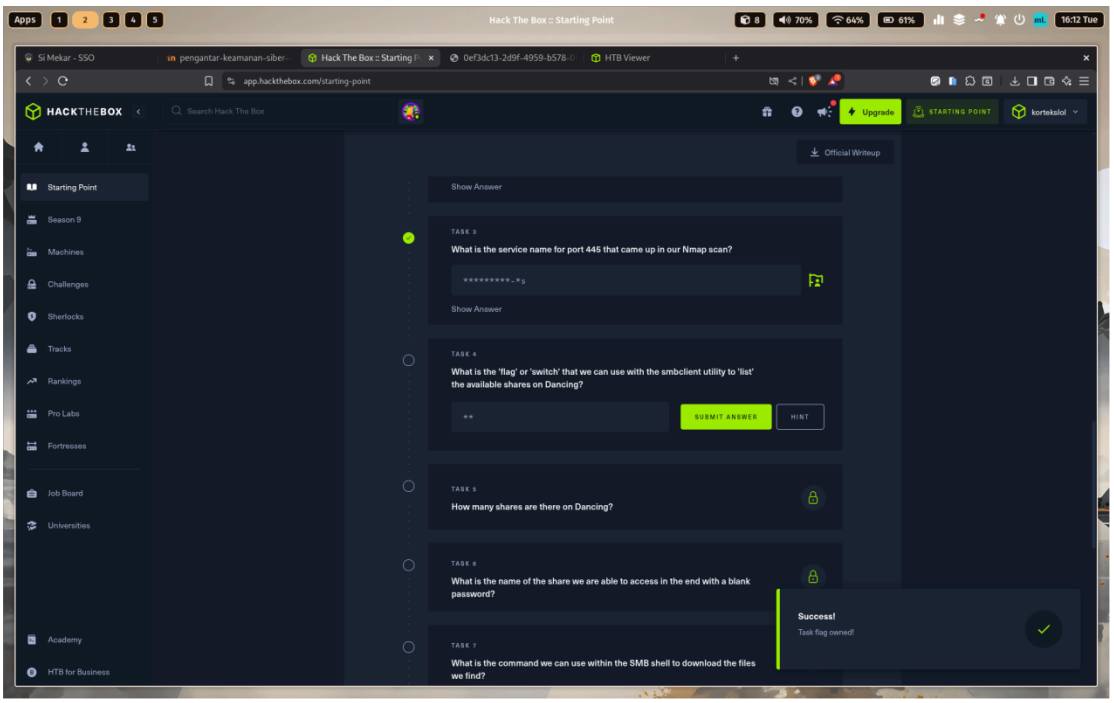

HTB Viewer
vnc.htb-cloud.com/index.php
Parrot Terminal
229 Entering Extended Passive Mode (|||56351|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> cat flag.txt
?Invalid command.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||54975|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |**********| 32 75.66 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (3.39 KiB/s)
ftp> exit
221 Goodbye.
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[+]$ ls
cacert.der Documents flag.txt my_data Public Videos
Desktop Downloads Music Pictures Templates
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[+]$ cat flag.txt
035db21c881520061c53e0536e44f815
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[+]$
HACKTHEBOX

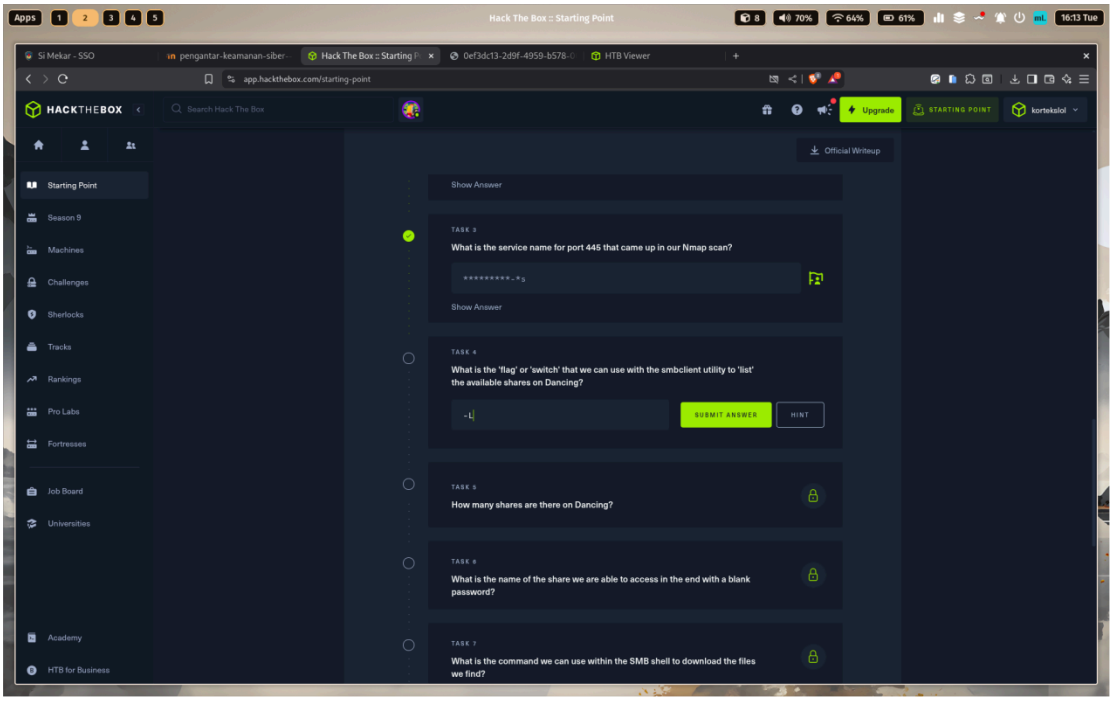

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
Starting Point
Official Writeup
Video Walkthrough
Show Answer
TASK 10
There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.
**
Show Answer
TASK 11
What is the command used to download the file we found on the FTP server?
***
Show Answer
SUBMIT FLAG
Submit root flag
035db21c881520061c53e0536e44f815
SUBMIT FLAG
Dancing
VERY EASY
0 of 8 tasks completed

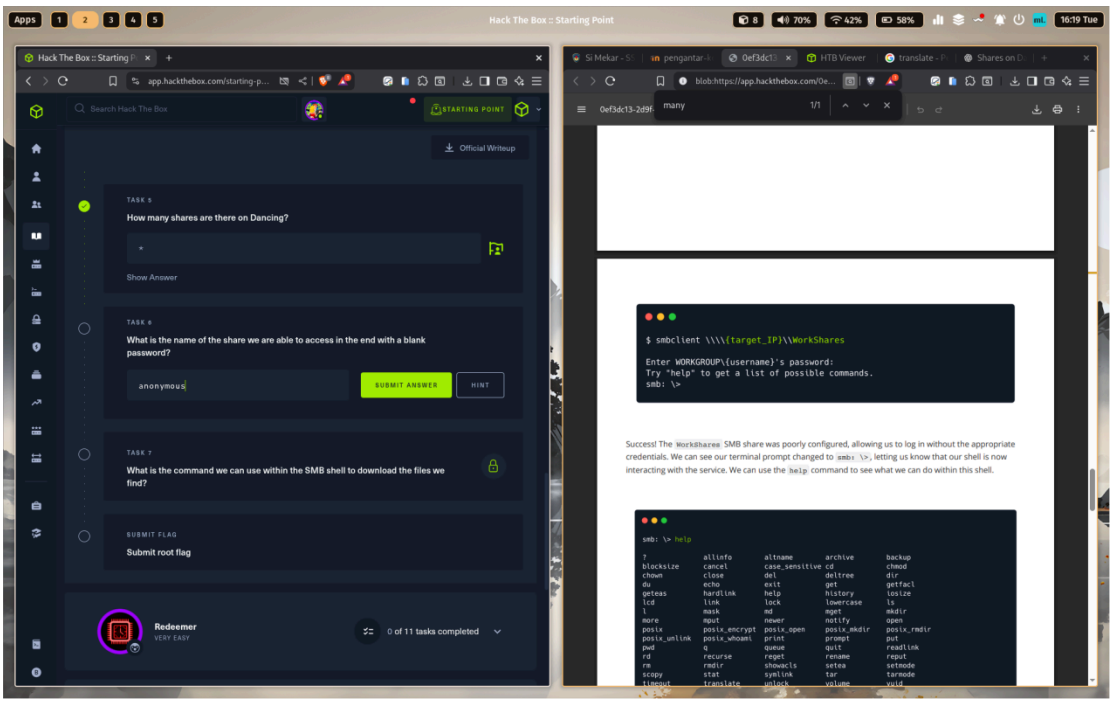

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access
Having Trouble? - Introduction to Lab Access
ONLINE
TARGET MACHINE IP ADDRESS
10.129.219.221
Read the walkthrough provided, to get a detailed guide on how to pwn this machine.
TASK 1
What does the 3-letter acronym SMB stand for?
Show Answer
TASK 2
What port does SMB use to operate at?
SUBMIT ANSWER
HINT
Success!
Task flag owned!
TASK 3
What is the service name for port 445 that came up in our Nmap scan?

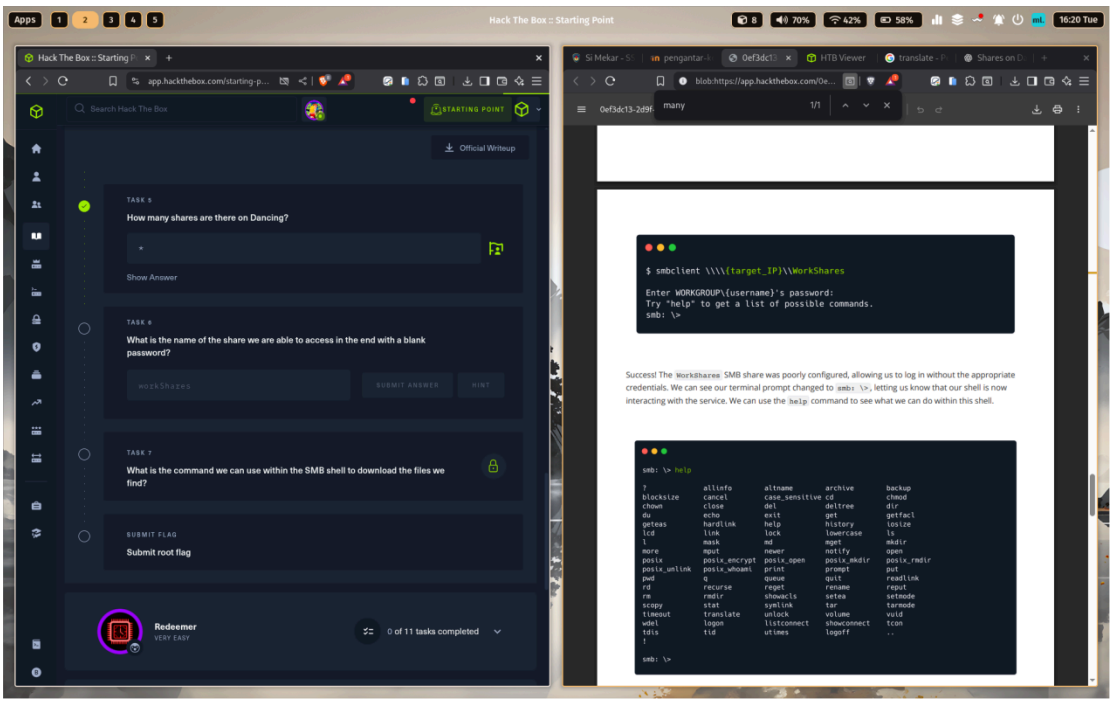

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Upgrade
STARTING POINT
Official Writeup
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
10.129.219.221
Read the walkthrough provided, to get a detailed guide on how to pwn this machine.
TASK 1
What does the 3-letter acronym SMB stand for?
Show Answer
TASK 2
What port does SMB use to operate at?
445
SUBMIT ANSWER
HINT
TASK 3
What is the service name for port 445 that came up in our Nmap scan?
TASK 4
What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?
TASK 5

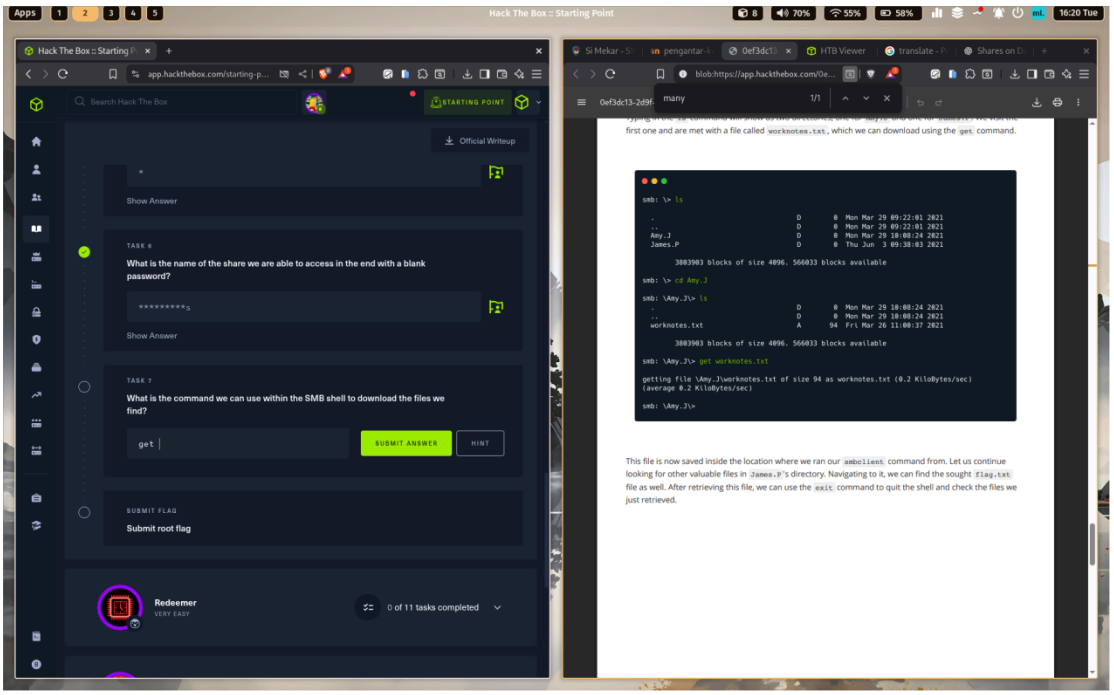

HTB Viewer
vnc.htb-cloud.com/index.php
Parrot Terminal
1-18 03:11 CST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[•]$ 10.129.219.221^C
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[•]$ ^C
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[•]$ sudo nmap -sV 10.129.219.221
Starting Nmap 7.94SVN (https://nmap.org) at 2025-11-18 03:12 CST
Nmap scan report for 10.129.219.221
Host is up (0.0096s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[~]
[•]$
HACKTHEBOX

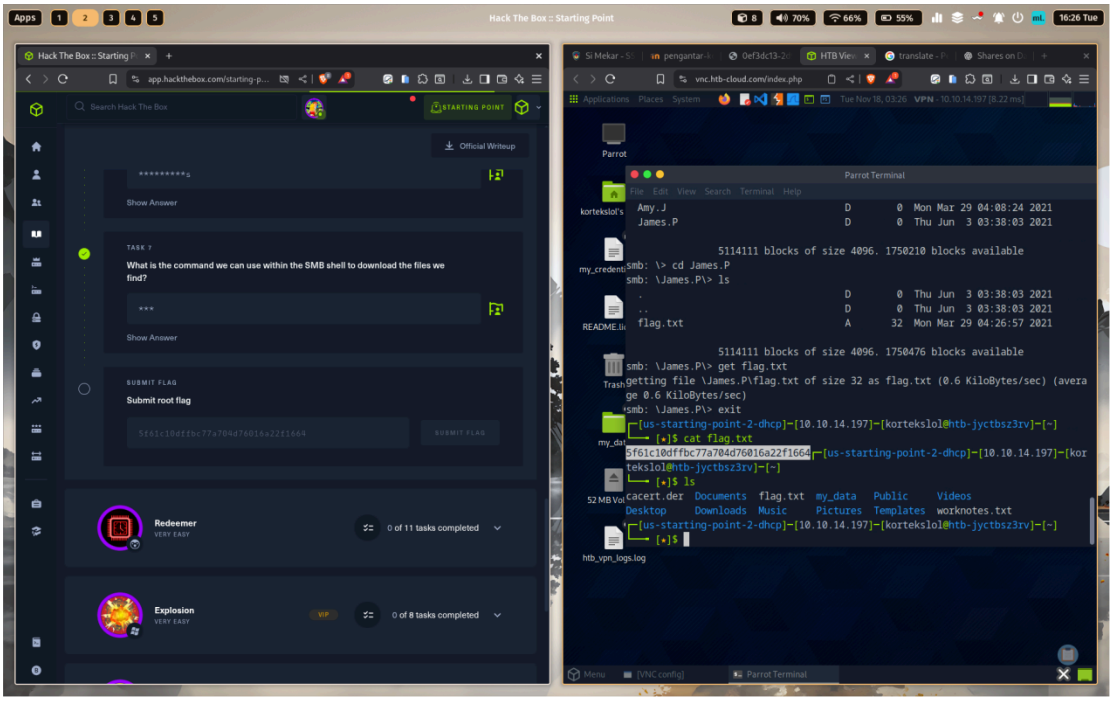

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Official Writeup
Show Answer
TASK 3
What is the service name for port 445 that came up 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
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?
Success!
Task flag owned!
TASK 7
What is the command we can use within the SMB shell to download the files we find?

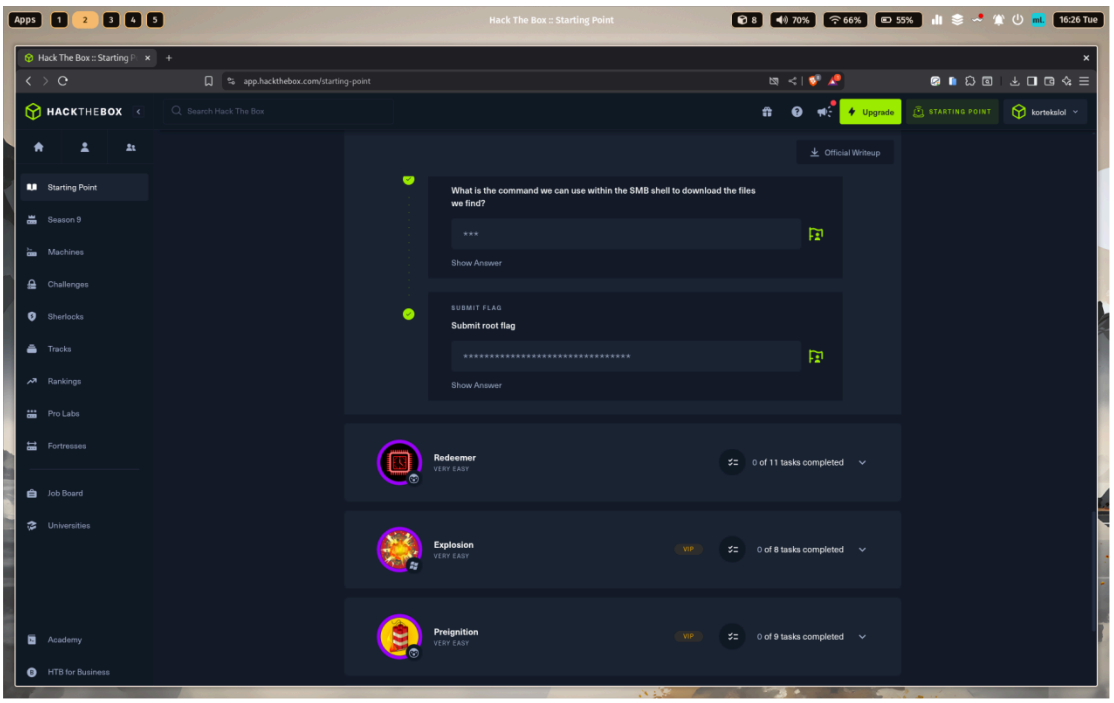

Hack The Box :: Starting Point
app.hackthebox.com/starting-point
HACKTHEBOX
Starting Point
Season 9
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Fortresses
Job Board
Universities
Academy
HTB for Business
Official Writeup
Show Answer
TASK 3
What is the service name for port 445 that came up 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?
-L
SUBMIT ANSWER
HINT
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?
TASK 7
What is the command we can use within the SMB shell to download the files we find?


Hack The Box :: Starting Point
Official Writeup
TASK 5
How many shares are there on Dancing?
Show Answer
TASK 6
What is the name of the share we are able to access in the end with a blank password?
anonymous
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
Redeemer
VERY EASY
0 of 11 tasks completed
$ smbclient \\\\{target_IP}\\WorkShares
Enter WORKGROUP\{username}'s password:
Try "help" to get a list of possible commands.
smb: \>
Success! The WorkShares SMB share was poorly configured, allowing us to log in without the appropriate credentials. We can see our terminal prompt changed to smb: \>, letting us know that our shell is now interacting with the service. We can use the help command to see what we can do within this shell.
smb: \> help


Hack The Box :: Starting Point
Official Writeup
TASK 5
How many shares are there on Dancing?
Show Answer
TASK 6
What is the name of the share we are able to access in the end with a blank password?
workShares
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
Redeemer
VERY EASY
0 of 11 tasks completed
$ smbclient \\\\{target_IP}\\WorkShares
Enter WORKGROUP\{username}'s password:
Try "help" to get a list of possible commands.
smb: \>
Success! The WorkShares SMB share was poorly configured, allowing us to log in without the appropriate credentials. We can see our terminal prompt changed to smb: \>, letting us know that our shell is now interacting with the service. We can use the help command to see what we can do within this shell.
smb: \> help
? allinfo altname archive backup
blocksize cancel case_sensitive cd chmod
chown close del deltree dir
du echo exit get getfacl
geteas hardlink help history iosize
lcd link lock lowercase ls
l mask md mget mkdir
more mput newer notify open
posix posix_encrypt posix_open posix_mkdir posix_rmdir
posix_unlink posix_whoami print prompt put
pwd q queue quit readlink
rd recurse reget rename reput
rm rmdir showacls setea setmode
scopy stat symlink tar tarmode
timeout translate unlock volume vuid
wdel logon listconnect showconnect tcon
tdis tid utimes logoff ..
!
smb: \>


Hack The Box :: Starting Point
Official Writeup
Show Answer
TASK 6
What is the name of the share we are able to access in the end with a blank password?
Show Answer
TASK 7
What is the command we can use within the SMB shell to download the files we find?
get
SUBMIT ANSWER
HINT
SUBMIT FLAG
Submit root flag
Redeemer
VERY EASY
0 of 11 tasks completed
first one and are met with a file called worknotes.txt, which we can download using the get command.
smb: \> ls
. D 0 Mon Mar 29 09:22:01 2021
.. D 0 Mon Mar 29 09:22:01 2021
Amy.J D 0 Mon Mar 29 10:08:24 2021
James.P D 0 Thu Jun 3 09:38:03 2021
3803903 blocks of size 4096. 566033 blocks available
smb: \> cd Amy.J
smb: \Amy.J\> ls
. D 0 Mon Mar 29 10:08:24 2021
.. D 0 Mon Mar 29 10:08:24 2021
worknotes.txt A 94 Fri Mar 26 11:00:37 2021
3803903 blocks of size 4096. 566033 blocks available
smb: \Amy.J\> get worknotes.txt
getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.2 KiloBytes/sec)
(average 0.2 KiloBytes/sec)
smb: \Amy.J\>
This file is now saved inside the location where we ran our smbclient command from. Let us continue looking for other valuable files in James.P's directory. Navigating to it, we can find the sought flag.txt file as well. After retrieving this file, we can use the exit command to quit the shell and check the files we just retrieved.


Apps
Hack The Box :: Starting Point
16:26 Tue
Hack The Box :: Starting P
app.hackthebox.com/starting-p...
Search Hack The Box
STARTING POINT
Official Writeup
Show Answer
TASK 7
What is the command we can use within the SMB shell to download the files we find?
***
Show Answer
SUBMIT FLAG
Submit root flag
5f61c10dffbc77a704d76016a22f1664
SUBMIT FLAG
Redeemer
VERY EASY
0 of 11 tasks completed
Explosion
VERY EASY
VIP
0 of 8 tasks completed
vnc.htb-cloud.com/index.php
Parrot Terminal
Amy.J D 0 Mon Mar 29 04:08:24 2021
James.P D 0 Thu Jun 3 03:38:03 2021
5114111 blocks of size 4096. 1750210 blocks available
smb: \> cd James.P
smb: \James.P\> ls
. D 0 Thu Jun 3 03:38:03 2021
.. D 0 Thu Jun 3 03:38:03 2021
flag.txt A 32 Mon Mar 29 04:26:57 2021
5114111 blocks of size 4096. 1750476 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec)
smb: \James.P\> exit
[us-starting-point-2-dhcp]-[10.10.14.197]-[korteksl0l@htb-jyctbsz3rv]-[~]
[*]$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664
[us-starting-point-2-dhcp]-[10.10.14.197]-[korteksl0l@htb-jyctbsz3rv]-[~]
[*]$ ls
cacert.der Documents flag.txt my_data Public Videos
Desktop Downloads Music Pictures Templates worknotes.txt
[us-starting-point-2-dhcp]-[10.10.14.197]-[korteksl0l@htb-jyctbsz3rv]-[~]
[*]$
Parrot
korteksl0l's
README.li
Trash
52 MB Vol
htb_vpn_logs.log
Menu
[VNC config]
Parrot Terminal


Apps
Hack The Box :: Starting Point
16:26 Tue
app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
Upgrade
STARTING POINT
korteksl0l
Official Writeup
Starting Point
Season 9
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 FLAG
Submit root flag
Show Answer
Redeemer
VERY EASY
0 of 11 tasks completed
Explosion
VERY EASY
VIP
0 of 8 tasks completed
Preignition
VERY EASY
VIP
0 of 9 tasks completed