

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

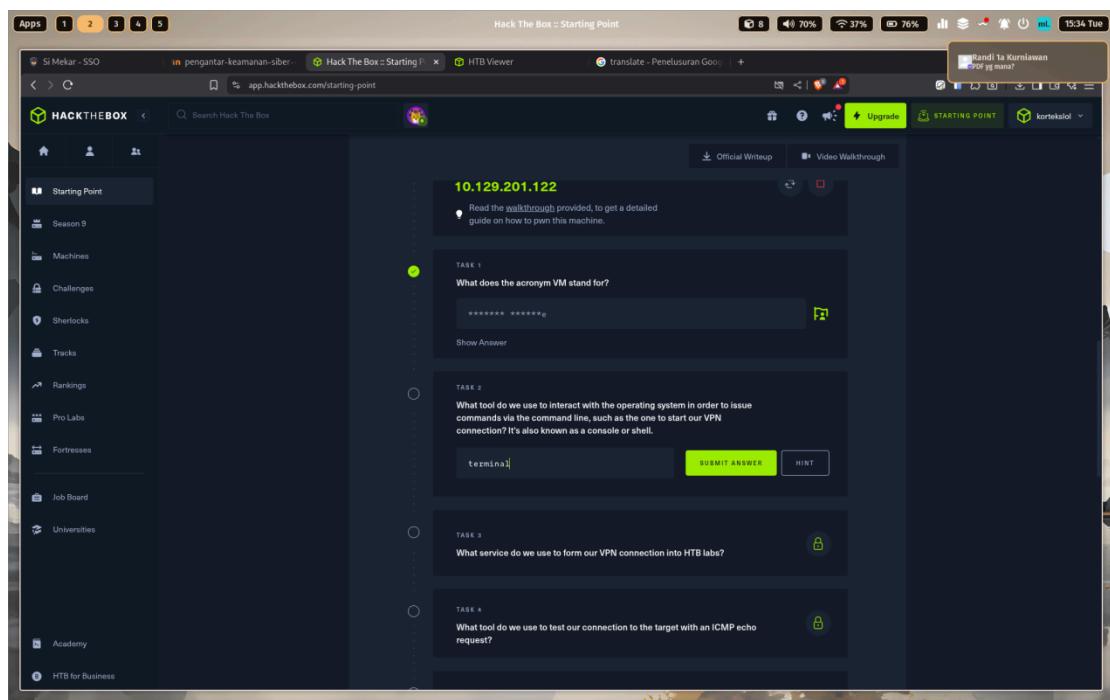
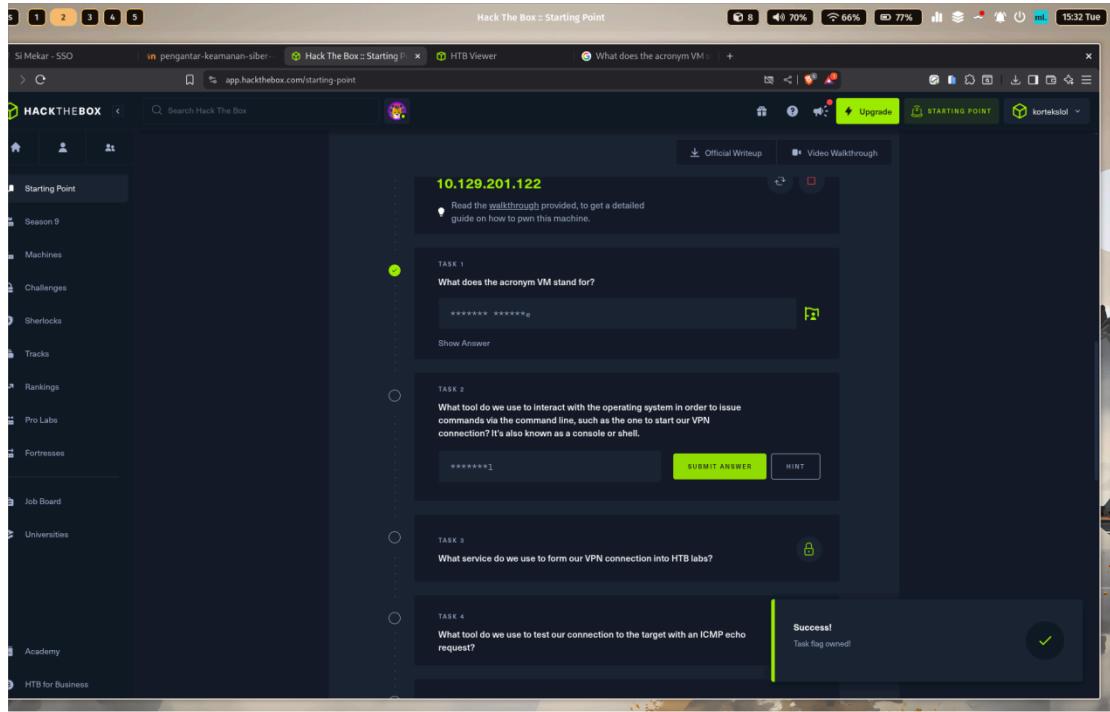
biasanya memanfaatkan form untuk inject query , dan untuk cara amankan dengan cara csrf token

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 tentang protocol2 transfer file , dan pengenalan client server

The screenshot shows the HTB Academy Dashboard. On the left, there's a sidebar with links like Dashboard, Exams, Modules, Paths, My Achievements, Referrals, and HTB Ecosystem. The main area has a 'DASHBOARD' section with three circular progress indicators: Offensive (0.00%), Defensive (0.00%), and General (0.00%). Below this is a 'Favorite Modules List' table with one entry: 'Intro to Academy' (Fundamental) with a 'Start' button. To the right, there's a 'Weekly Streak' section showing 0 streak points for the week, and a 'Refer a friend' section. Further down are 'My Plan' (with a 'Subscribe now!' button), 'Completed Paths' (None), 'Completed Modules' (None), and a 'Getting Started' button.

The screenshot shows the HackTheBox Starting Point interface. On the left, there's a sidebar with links like Starting Point, Season 9, Machines, Challenges, Sherlocks, Tracks, Rankings, Pro Labs, Fortresses, Job Board, Universities, Academy, and HTB for Business. The main area has a 'CONNECT' section with two options: 'Connect using Pwnbox' (Recommended) and 'Connect using OpenVPN'. It also shows a 'CREATING INSTANCE...' progress bar. Below this are two 'TASK' sections: 'TASK 1' asking 'What does the acronym VM stand for?' and 'TASK 2' asking '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?'. There are also 'Official Writeup' and 'Video Walkthrough' buttons at the top right.



Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 42% 76% 15:35 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteekslol

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?

ping SUBMIT ANSWER HINT

TASK 5 What is the name of the most common tool for finding open ports on a target?

SUBMIT ANSWER HINT

TASK 6 What service do we identify on port 23/tcp during our scans?

SUBMIT ANSWER HINT

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 42% 76% 15:35 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point HTB Viewer translate - Penelusuran Google

Kandi Is Kurniawan Kunci ada sini Upgrade STARTING POINT korteekslol

HACKTHEBOX Search Hack The Box

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?

*****2 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?

SUBMIT ANSWER HINT

TASK 6 What service do we identify on port 23/tcp during our scans?

SUBMIT ANSWER HINT

Apps 1 2 3 4 5 Hack The Box :: Starting Point

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point HTB Viewer What is the name of the most common tool for finding open ports on a target?

Search Hack The Box

HACKTHEBOX

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?
ping

TASK 5
What is the name of the most common tool for finding open ports on a target?
nmap

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

Official Writeup Video Walkthrough

Upgrade STARTING POINT

korteksalol

Apps 1 2 3 4 5 Hack The Box :: Starting Point

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point HTB Viewer translate - Penelusuran Google

Search Hack The Box

HACKTHEBOX

Starting Point

Season 9

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Fortresses

Job Board

Universities

Academy

HTB for Business

translate - Penelusuran Google

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

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 →

Official Writeup Video Walkthrough

Upgrade STARTING POINT

korteksalol

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 42% 74% 15:39 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT kortekekolol

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

***g Show Answer

TASK 5 What is the name of the most common tool for finding open ports on a target? ***p 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 root flag

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 0 of 11

Hack The Box :: Starting Point 73% 70% 15:51 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 275d291-19c8-4fad-bba1-96 HTB Viewer translate - Penelusuran Google Mencari flag.txt HTB

Search Hack The Box Upgrade STARTING POINT kortekekolol

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

***t Show Answer

TASK 7 What username is able to log into the target over telnet with a blank password? ***** Show Answer

SUBMIT FLAG Submit root flag

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 0 of 11

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 73% 70% 15:51 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 275df291-19c8-4fad-bba1-9 HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteislol

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

TASK 1 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 0 of 11

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteislol

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

Important: Most boxes require you to have pre-installed:

Free 2h of Pwbox - 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 pw this machine.

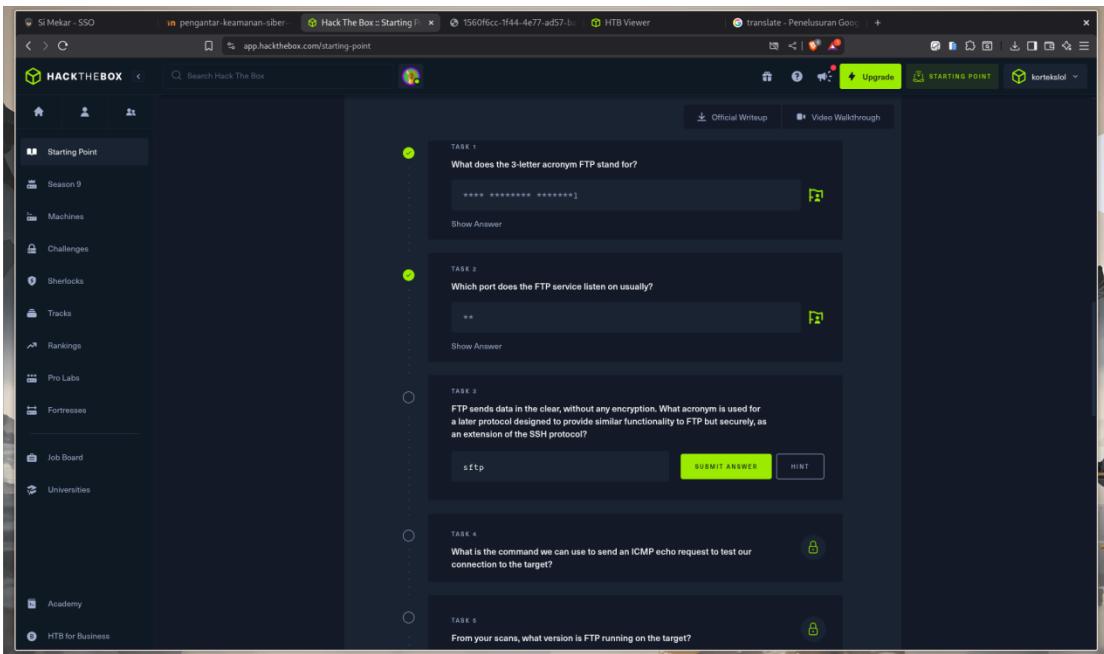
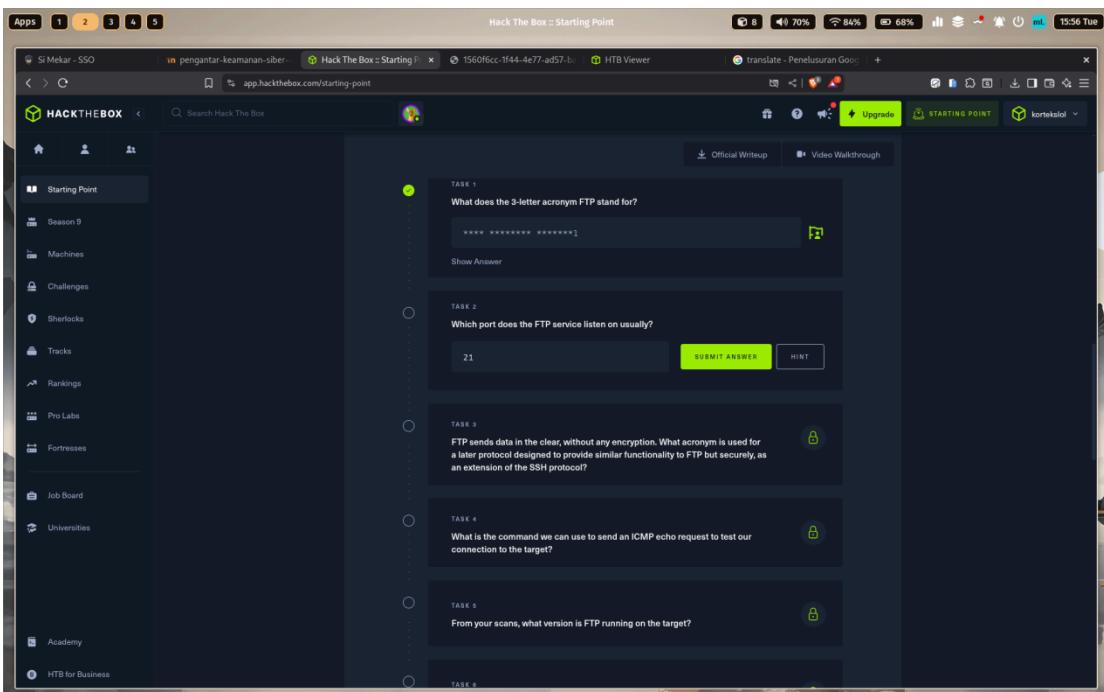
TASK 1 What does the 3-letter acronym FTP stand for?

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



Apps 1 2 3 4 5 Hack The Box :: Starting Point

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 1560f6cc-1f44-4e77-ad57-b... HTB Viewer translate - Penelusuran Google

Show Answer

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?

***** v. .3

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

***x

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'?

Apps 1 2 3 4 5 Hack The Box :: Starting Point

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 1560f6cc-1f44-4e77-ad57-b... HTB Viewer translate - Penelusuran Google

Show Answer

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

***** v. .3

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

***x

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!

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 77% 67% 15:57 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 1560f6cc-1f44-4e77-ad57-b... HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteekolol

Starting Point

Season 9

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Fortresses

Job Board

Universities

Academy

HTB for Business

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

SUMMIT ANSWER HINT

Show Answer

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?

Show Answer

TASK 9
What is the response code we get for the FTP message 'Login successful'?

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 77% 67% 15:58 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 1560f6cc-1f44-4e77-ad57-b... HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteekolol

Starting Point

Season 9

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Fortresses

Job Board

Universities

Academy

HTB for Business

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 -?

SUMMIT ANSWER HINT

Show Answer

TASK 8
What is username that is used over FTP when you want to log in without having an account?

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 77% 67% 15:58 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 1560f6cc-1f44-4e77-ad57-b... HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteksalol

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 'Tfp' 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"? 230

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

This screenshot shows the 'Starting Point' section of the HackTheBox interface. On the left is a sidebar with various navigation links. The main area displays five tasks. Task 7 asks for the command to display the 'Tfp' client help menu, with the answer '*** -?'. Task 8 asks for the anonymous user name for FTP, with the answer 'anonymous'. Task 9 asks for the response code for a successful login, with the answer '230'. Task 10 asks for another command to list files on an FTP server, with the answer 'dir'. Task 11 asks for the command to download a file from an FTP server, with the answer 'SUBMIT FLAG'. At the bottom, there's a 'Dancing VERY EASY' badge and a progress bar indicating '0 of 8 tasks completed'.

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 82% 67% 15:58 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 1560f6cc-1f44-4e77-ad57-b... HTB Viewer translate - Penelusuran Google

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT korteksalol

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

TASK 7 *****5 Show Answer

TASK 8 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

This screenshot shows the same 'Starting Point' section as the first one, but with answers already entered. Task 7 now shows '*****5'. Task 8 shows '230'. Task 10 shows 'dir'. Task 11 shows 'SUBMIT FLAG'. The rest of the interface is identical to the first screenshot, including the sidebar and the 'Dancing VERY EASY' badge at the bottom.

The screenshot shows the HackTheBox web interface on a Linux desktop environment. The left sidebar contains navigation links such as Starting Point, Season 9, Machines, Challenges, Sherlocks, Tracks, Rankings, Pro Labs, Fortresses, Job Board, Universities, Academy, and HTB for Business. The main content area displays three tasks:

- TASK 9:** What is the response code we get for the FTP message 'Login successful'?
Input field: ***
Buttons: Show Answer, Hint, Submit 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?
Input field: **
Buttons: Show Answer, Hint, Submit Answer
- TASK 11:** What is the command used to download the file we found on the FTP server?
Input field: get
Buttons: Show Answer, Hint, Submit Answer

At the bottom of the interface, there are buttons for SUBMIT FLAG and Submit root flag.

The screenshot shows a Kali Linux desktop environment with several windows open:

- Parrot Terminal:** A terminal window titled "Parrot Terminal" showing a session on a "Starting Point" machine. The user is interacting with an FTP server. The terminal output includes:

```
229 Entering Extended Passive Mode (|||56351|)  
150 Here comes the directory listing.  
  .w-i--I-- 1 0 0 32 Jun 04 2021 flag.txt  
226 Directory send OK.  
my_credentials: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]~[-]  
my_data [~]$ ls  
Gacerit_des Documents flag.txt my_data Public Videos  
Desktop Downloads Music Pictures Templates  
[us-starting-point-2-dhcp]~[10.10.14.197]~[kortekslol@htb-jyctbsz3rv]~[-]  
[~]$ 035db21c881520061c53e0536e44f815 [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:** A web browser window showing the HackTheBox interface for the "Starting Point" challenge. The sidebar lists various sections like Starting Point, Season 9, Machines, Challenges, etc. The main content area displays tasks and challenges, including:
 - TASK 10:** A question about common Linux file listing commands.
 - TASK 11:** A question about the command used to download files from an FTP server.
 - SUBMIT FLAG:** A text input field containing the flag `035db21c881520061c53e0536e44f815` and a "SUBMIT FLAG" button.
- HTB Viewer:** A window showing system status and network information.
- translate - Penelusuran Google:** A search results window.

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 75% 62% 16:10 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 0ef3dc13-2d9f-4959-b578-0 HTB Viewer +

HACKTHEBOX Search Hack The Box Upgrade STARTING POINT Official Writeup

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

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?

Apps 1 2 3 4 5 Hack The Box :: Starting Point 70% 66% 62% 16:10 Tue

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 0ef3dc13-2d9f-4959-b578-0 HTB Viewer +

HACKTHEBOX Search Hack The Box 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?

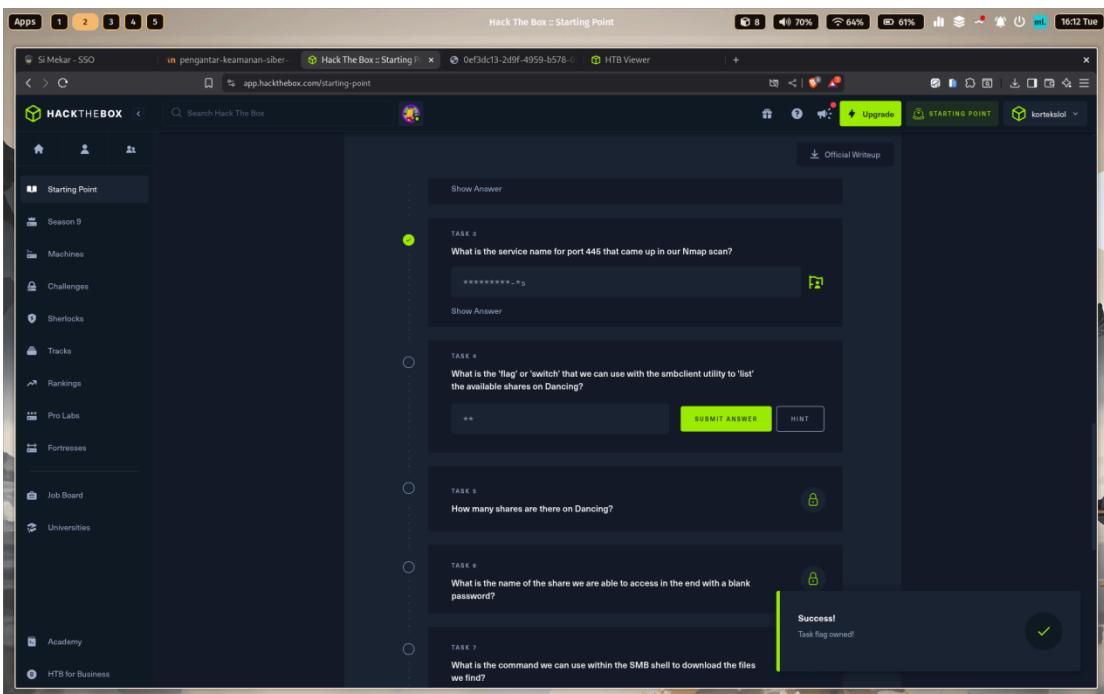
TASK 5

```
File Edit View Search Terminal Help
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

[*] [+] $ [+] 10.129.219.221 C
[*] [+] $ [+] 10.10.14.197 [-] [kortekslol@htb-jyctbsz3rv](-)
[*] [+] $ ^C
[*] [+] $ sudo nmap -sv 10.129.219.221
Starting Nmap 7.94VN ( https://nmap.org ) at 2025-11-18 03:12 CST
Nmap scan report for 10.129.219.221
Host is up (0.0006s 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/ .
52 MB Vulnerability Scan Report Generated: 2025-11-18 03:12 CST
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds
[*] [+] $ [+] 10.10.14.197 [-] [kortekslol@htb-jyctbsz3rv](-)
[*] [+] $
```



Apps 1 2 3 4 5 Hack The Box :: Starting Point

Si Mekar - SSO pengantar-keamanan-siber Hack The Box :: Starting Point 0ef3dc13-2d9f-4959-b578-0 HTB Viewer

Show Answer
Official Writeup

TASK 2
What is the service name for port 445 that came up in our Nmap scan?
*****-k9

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?

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?

Starting Point Season 9 Machines Challenges Sherlocks Tracks Rankings Pro Labs Fortresses Job Board Universities Academy HTB for Business

Apps 1 2 3 4 5 Hack The Box :: Starting Point

Si Mekar - SSI pengantar-keamanan-siber 0ef3dc13-2d9f-4959-b578-0 HTB Viewer translate - P Shares on D

STARING POINT

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

Redeemer VERY EASY

0 of 11 tasks completed

many 1/1

\$ 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 !lsip command to see what we can do within this shell.

smb:> help

!allinfo	!cancel	!clsname	!archive	!backup
!lockfile	!close	!case_insensitive	!cd	!change
!chown	!del	!deltree	!dir	!getacl
!du	!exit	!get	!gettree	!getxattr
!getpass	!hardlink	!history	!ls	!lowercase
!lcd	!lock	!lock	!mdir	!mdir
!l	!makedirs	!mknod	!mknod	!mknod
!more	!naut	!notify	!open	!open
!posix	!post_encrypt	!posix_open	!posix_mkdir	!posix_rmdir
!postx_unlink	!postx_wchan	!postx_readdir	!postx_rmdir	!postx_rmdir
!pwd	!queue	!quit	!readlink	!readlink
!rd	!reget	!rename	!rmdir	!rmdir
!rm	!recuse	!setxattr	!setxattr	!setxattr
!scopy	!stat	!symlink	!tar	!tarmode
!timestat	!translate	!unlock	!volume	!volume

Hack The Box :: Starting Point

Task 6: 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?

Redeemer VERY EASY

0 of 11 tasks completed

Si Mekar - S | sn pengantar-k... 0ef3dc13-2d9f many HTB Viewer translate - i Shares on D... +

Terminal Output:

```
$ 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.

Terminal Output:

```
smb: > !help
allinfo    alternate   archive    backup
blocksize  cancel     del        dir
chown     close      exit      get
du         echo       history   lowercase
getpass   hardlink  lseek    ls
lcd       llink      locale   more
l          map       never    notify
more      maut      open     posix
posix     posix_encrypt  posix_open  posix_mkdir
posix_unlink  posix_whomai  queue   readlink
pwd       recurse   reget    rename
rd        recursive  select   reboot
scopy     stat      symlink  tarmode
timeout   translate  unlock   vold
smb      talloc     listconnect  tcon
tdis     tdir      utimes   tlogoff
!
```

Hack The Box :: Starting Point

Task 6: What is the name of the share we are able to access in the end with a blank password?

get

Task 7: What is the command we can use within the SMB shell to download the files we find?

Redeemer VERY EASY

0 of 11 tasks completed

Si Mekar - S | sn pengantar-k... 0ef3dc13-2d9f many HTB Viewer translate - i Shares on D... +

Terminal Output:

```
smb: > ls
.
..
Key_J
Jones_P
worknotes.txt

3883903 blocks of size 4096. 566933 blocks available
smb: > cd Key_J
smb: \Key_J> ls
.
..
D  8 Mon Mar 29 09:22:01 2021
D  8 Mon Mar 29 09:22:01 2021
A 94 Fri Mar 26 11:00:07 2021
worknotes.txt

3883903 blocks of size 4096. 566933 blocks available
smb: \Key_J> get worknotes.txt
getting file \Key_J\worknotes.txt of size 94 as worknotes.txt (0.2 Kilobytes/sec)
(saverage 0.2 Kilobytes/sec)
smb: \Key_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 `Jones_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.

The image shows a dual-monitor setup. The left monitor displays the HackTheBox website in a web browser. The right monitor shows a VNC session of a Parrot OS terminal window.

Parrot Terminal Content:

```
SMB: > cd James.P
SMB: \James.P> ls
.
..
flag.txt
README.txt
5114111 blocks of size 4096. 1750210 blocks available
SMB: \James.P> get flag.txt
Trash getting file \James.P\flag.txt of size 32 as flag.txt (0.6 Kilobytes/sec)
SMB: \James.P> exit
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
my_data
5f61c10effbc77a704d76016a2ff1664-[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
htb_vpn_logs.log
```

HackTheBox Web Browser Content:

The HackTheBox website shows the "Starting Point" challenge. A task asks for the command to download files from an SMB shell. The answer is provided as "cd James.P & get flag.txt".

Left Monitor (HackTheBox Website):

- Starting Point
- Season 9
- Machines
- Challenges
- Sherlocks
- Tracks
- Rankings
- Pro Labs
- Fortresses
- Job Board
- Universities
- Academy
- HTB for Business

Right Monitor (Parrot Terminal):

- File Edit View Search Terminal Help
- kortekslol's Amy.J James.P
- D 0 Mon Mar 29 04:08:24 2021
- D 0 Thu Jun 3 03:38:03 2021
- 5114111 blocks of size 4096. 1750210 blocks available
- my_data
- SMB: > cd James.P
- SMB: \James.P> ls
- .
- ..
- flag.txt
- README.txt
- 5114111 blocks of size 4096. 1750476 blocks available
- SMB: \James.P> get flag.txt
- Trash getting file \James.P\flag.txt of size 32 as flag.txt (0.6 Kilobytes/sec)
- SMB: \James.P> exit
- [us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
- my_data
- 5f61c10effbc77a704d76016a2ff1664-[us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
- [us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
- [us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
- [us-starting-point-2-dhcp]-[10.10.14.197]-[kortekslol@htb-jyctbsz3rv]-[-]
- htb_vpn_logs.log