

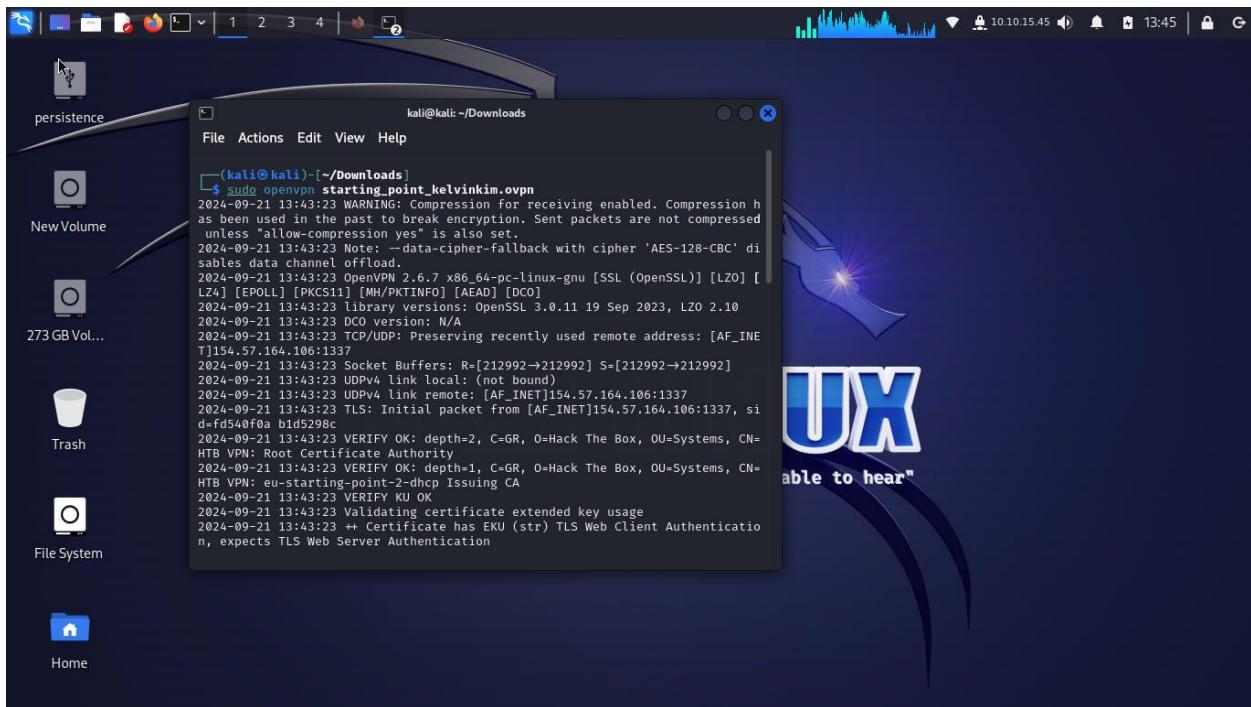
NAME: Kelvin Kimotho

LinkedIn: [kelvin kimotho](#)

GETTING STARTED ON HACK THE BOX TIER 0

Meow

- First, I learnt how to connect to the hackthebox vpn using the following command. "sudo openvpn vpn_file"



- Then to test connectivity i just need to ping the target IP using this command. "ping IP"
- The first step in penetration testing is enumeration which involves documenting the state of the target machine by gaining information about it.
- We start by scanning for open ports on the system to see what services are running and which can we exploit. We use nmap a tool.
- " nmap -sV IP" is the command format, where V flag gives us the version of the services running and also the operating system information.
- For telnet services that usually run on port 23, we can use the telnet tool and try connect.

" telnet Target_IP" is the command. We can use username "root" to login without a password.

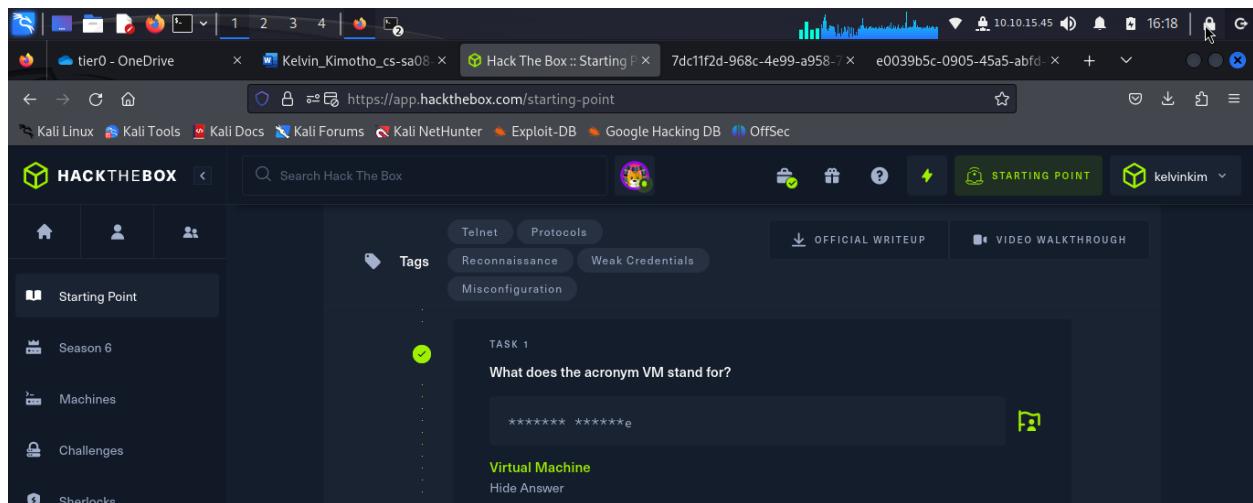
- After a successful login, we can use ls command to list contents.
- Cat command to read contents of a file.

Then i went ahead and answered the questions that followed.

Task 1

Question: What does the acronym VM stand for?

Answer: Virtual Machine



Task 2

Question: 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.

Answer: Terminal

Task 3

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

Answer: Openvpn

The screenshot shows the HackTheBox website interface. On the left, there's a sidebar with navigation links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', 'Rankings', 'Academy', and 'HTB for Business'. The main content area has tabs for 'Telnet', 'Protocols', 'Reconnaissance', 'Weak Credentials', and 'Misconfiguration'. A challenge titled '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.' is displayed. Below it, another challenge titled 'TASK 3' asks 'What service do we use to form our VPN connection into HTB labs?' with the answer 'openvpn'.

I connected to hackthebox vpn via my linux machine terminal.

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is 'kali:kali:~/Downloads'. The command run is '\$ sudo openvpn starting_point_kelvinkim.ovpn'. The terminal output shows the configuration file being loaded and the OpenVPN daemon starting up, including logs about cipher selection, compression, and certificate verification. The terminal window is titled 'persistence' and is part of a desktop environment with icons for OneDrive, a browser, and other tools.

Task 4

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

Answer: ping

Task 5

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

Answer: Nmap

The screenshot shows the HackTheBox web application. On the left, there's a sidebar with navigation links: Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, and Academy. The main area displays a task card for 'Starting Point'. At the top of the card, there are tabs for Telnet, Protocols, Reconnaissance, Weak Credentials, and Misconfiguration. Under the 'Misconfiguration' tab, the word 'ping' is listed with a 'Hide Answer' button. Below the card, under the heading 'TASK 5', is the question: 'What is the name of the most common tool for finding open ports on a target?'. A text input field contains the answer '***p', and below it, the word 'nmap' is listed with a 'Hide Answer' button. There are also 'OFFICIAL WRITEUP' and 'VIDEO WALKTHROUGH' buttons.

Task 6

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

Answer: Telnet

Task 7

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

Answer: root

The screenshot shows the HackTheBox starting point page. On the left sidebar, there are links for Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area displays a task titled "telnet". It asks, "What username is able to log into the target over telnet with a blank password?". Below the question, there is a text input field containing "root" and a "Hide Answer" link. At the bottom right of the task box is a "SUBMIT FLAG" button.

The screenshot shows a terminal window on Kali Linux with the command `nmap -sV 10.129.16.190` running. The output shows various ports and services, including port 23/tcp open telnet. The terminal also shows a file browser window with a file named "Flag.txt" visible.

```
(kali㉿kali)-[~/Desktop] $ nmap -sV 10.129.16.190
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 16:23 UTC
Nmap scan report for 10.129.16.190
Host is up (0.23s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE     SERVICE VERSION
23/tcp    open      telnet   Linux telnetd
481/tcp   filtered dvs
1068/tcp  filtered instl_bootc
1309/tcp  filtered jtag-server
1434/tcp  filtered ms-sql-m
1840/tcp  filtered netopia-v02
2135/tcp  filtered gris
4001/tcp  filtered newoak
5030/tcp  filtered surfpass
9485/tcp  filtered unknown
9575/tcp  filtered unknown
32769/tcp filtered filenet-rpc
49159/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.21 seconds
(kali㉿kali)-[~/Desktop] $
```

Question: Submit root flag

Answer: b40abdfa23665f766f9c61ecba8a4c19

The screenshot displays two windows from a Linux desktop environment. The top window is a web browser showing the HackTheBox platform. The URL is https://app.hackthebox.com/starting-point. The page title is "Hack The Box :: Starting Point". The main content area shows a "Submit root flag" section with a placeholder text area containing the flag "b40abdf23665f766f9c61ecba8a4c19". Below this is a "Hide Answer" button. The left sidebar of the browser window shows "Season 6", "Machines", and "Challenges". The bottom window is a terminal window titled "root@Meow:". The terminal output shows:

```

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 Fri 20 Sep 2024 04:27:56 PM UTC

System load: 0.0
Usage of /: 41.7% of 7.75GB
Memory usage: 4%
Swap usage: 0%
Processes: 137
Users logged in: 0
IPv4 address for eth0: 10.129.16.190
IPv6 address for eth0: dead:beef::250:56ff:fe94:9117

* Super-optimized for small spaces - read how we shrunk the memory
footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Sep 20 16:27:22 UTC 2024 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdf23665f766f9c61ecba8a4c19
root@Meow:~#

```

Fawn

- This is where I learnt About FTP (file transfer protocol) used for simple file transfer tasks.
- It is used to transfer files from a server to a client within the same network.
- FTP may allow authentication using passwords and usernames in plain text.
- One can connect to an ftp server using username "anonymous" if the server allows it.
- We can secure FTP with SSL or use SSH (ssh file transfer protocol) SFTP.

- Traffic via FTP can be intercepted during man in the middle attack. The contents of the files can be read since they are in plain text.
- FTP runs on port 21.
- SSH on port 22
- webservers run on port 80.
- For enumeration we first ping the target IP. "ping Target_IP"
- Then use Nmap to see the open ports. "Nmap Target_IP"
- Adding -sV flag reveals more information including the Version of the server and the os information.

To gain foothold.

- We type ftp -? command to see more on how to use it.
- Then use "ftp Target_IP" to connect to the target.
- We can use anonymous username followed by any password to login if the server is misconfigured to allow this.
- Once in, we can type, help, --help to see the commands available for us users.
- We can use man command to see more on how to use a given tool available for us. e.g. "man get"
- We use ls to list contents.
- We use get command to download files from the server to our local machine.

I answered the questions that followed.

Task 1

Question: What does the 3-letter acronym FTP stand for?

Answer: File Transfer Protocol

Task 2

Question: Which port does the FTP service listen on usually?

Answer: 21

The screenshot shows a web browser window with the URL <https://app.hackthebox.com/starting-point>. The page is titled "Hack The Box :: Starting Point". On the left, there's a sidebar with links like "Starting Point", "Season 8", "Machines", "Challenges", "Sherlocks", "Tracks", "Rankings", "Academy", and "HTB for Business". The main content area has two tasks. Task 1 asks "What does the 3-letter acronym FTP stand for?" with the answer "File Transfer Protocol". Task 2 asks "Which port does the FTP service listen on usually?" with the answer "21". There are also buttons for "OFFICIAL WRITEUP" and "VIDEO WALKTHROUGH".

I confirmed the port where the ftp service was running from on the spawned machine.

The screenshot shows a terminal window on Kali Linux with the command `nmap -sV` run against the IP address 10.129.86.255. The output shows that port 21 is open and running vsftpd 3.0.3. The terminal window is located on a desktop environment with a "KALI LINUX" watermark.

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV 10.129.86.255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 15:49 UTC
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 96.36% done; ETC: 15:51 (0:00:03 remaining)
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 15:51 (0:00:00 remaining)
Nmap scan report for 10.129.86.255
Host is up (0.24s latency)
Not shown: 999 closed tcp ports (conn-refused)
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 127.41 seconds
```

Task 3

Question: 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?

Answer: SFTP

Task 4

Question: What is the command we can use to send an ICMP echo request to test our connection to the target?

Answer: ping

The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with navigation links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', 'Rankings', and 'Academy'. The main area has tabs for 'FTP', 'Protocols', and 'Reconnaissance'. Below these are buttons for 'OFFICIAL WRITEUP' and 'VIDEO WALKTHROUGH'. A search bar at the top says 'Search Hack The Box'. The main content area displays Task 4, which asks 'What is the command we can use to send an ICMP echo request to test our connection to the target?'. The answer 'ping' is listed as correct. Below this is Task 5, which is partially visible.

I tried sending ICMP echo request to test our connection to the spawned machine.

```
(kali㉿kali)-[~/Desktop]
$ ping 10.129.86.255
PING 10.129.86.255 (10.129.86.255) 56(84) bytes of data.
64 bytes from 10.129.86.255: icmp_seq=3 ttl=63 time=227 ms
64 bytes from 10.129.86.255: icmp_seq=4 ttl=63 time=219 ms
64 bytes from 10.129.86.255: icmp_seq=5 ttl=63 time=242 ms
64 bytes from 10.129.86.255: icmp_seq=6 ttl=63 time=243 ms
64 bytes from 10.129.86.255: icmp_seq=8 ttl=63 time=225 ms
^C
--- 10.129.86.255 ping statistics ---
9 packets transmitted, 5 received, 44.4444% packet loss, time 8079ms
rtt min/avg/max/mdev = 218.644/231.073/242.927/9.717 ms
```

I tried sending ICMP echo request to test our connection to the spawned machine.

Task 5

Question: From your scans, what version is FTP running on the target?

Answer: vsftpd 3.0.3

Task 6

Task 5

Question: From your scans, what version is FTP running on the target?

Answer: vsftpd 3.0.3

(kali㉿kali)-[~/Desktop]

```
$ nmap -sV 10.129.86.255 | grep ftp
21/tcp open  ftp  vsftpd 3.0.3
```

(kali㉿kali)-[~/Desktop]

File Actions Edit View Help

Task 6

Question: From your scans, what version is FTP running on the target?

Answer: vsftpd 3.0.3

Task 6

Question: From your scans, what OS type is running on the target?

Answer: Unix

Task 7

Task 6

Question: From your scans, what OS type is running on the target?

Answer: Unix

(kali㉿kali)-[~/Desktop]

```
$ nmap -sV 10.129.86.255 | grep OS
Service Info: OS: Unix
```

(kali㉿kali)-[~/Desktop]

ftp -u URL FILE ...

From the excerpt above, we can see that we can connect to the target host using the command below. This will initiate a request to authenticate on the FTP service running on the target, which will return a prompt back to our host:

```
$ ftp {target_IP}
Connected to {target_IP}.
220 (vsFTPd 3.0.3)
Name ({target_IP}:{username}):
```

Task 7

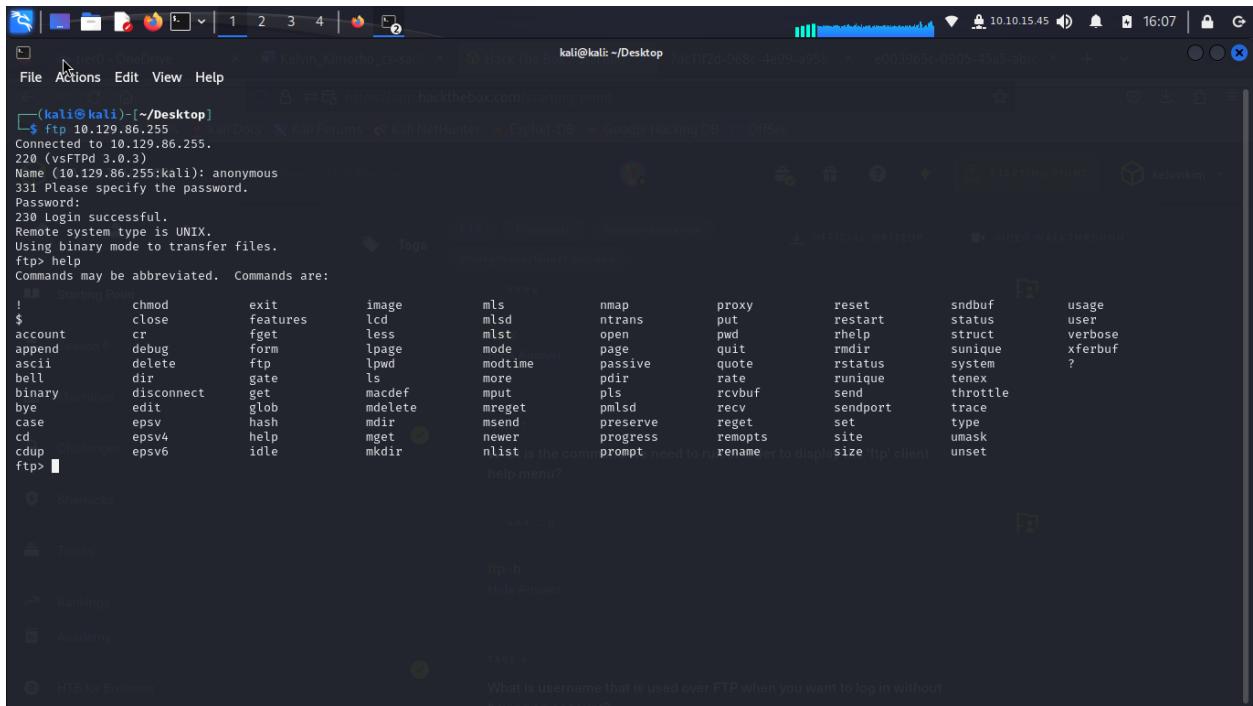
Question: What is the command we need to run in order to display the 'ftp' client help menu?

Answer: ftp -h

Task 8

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

Answer: Anonymous



```
(kali㉿kali)-[~/Desktop]
$ ftp 10.129.86.255
Connected to 10.129.86.255.
220 (vsFTPd 3.0.3)
Name (10.129.86.255:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated. Commands are:
!      chmod      exit      image      mls      mmap      proxy      reset      sndbuf      usage
$      close      features   lcd       mlsd      ntrans    put       restart    status      user
account  cr       fget      less      mlst      open     page      quit      rhelp      struct
append   debug      form      lpage    mode      rmdir     rstatus   sunique    verbose
ascii    delete    ftp       lpwd      modtime  passive  quote     rstatus   system
bell     dir       gate      ls       more      pdir     rate      runique  tenex
binary   disconnect get      macdef   mput      pls      rcvbuf   send      throttle
bye     edit      glob      mdelete  mreget   pmlsd    recv     sendport  trace
case    epsv      hash      mdir      msend    preserve  reget    set       type
cd      epsv4     help      mget     newer    progress  remopts  site     umask
cdup   epsv6      idle      mkdir    nlist   is the command prompt need to run or to display the ftp client
ftp> help menu?
```

Task 9

Question: What is the response code we get for the FTP message 'Login successful'?

Answer: 230

The screenshot shows the HackTheBox application interface. On the left is a sidebar with icons for Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area has tabs for FTP, Protocols, and Reconnaissance, with 'Anonymous/Guest Access' selected. A search bar at the top says 'Search Hack The Box'. Below it, there are two tasks:

- Task 1:** What is the command used over FTP when you want to log in without having an account?
Answer: anonymous
- Task 2:** What is the response code we get for the FTP message 'Login successful'?
Answer: 230

Task 10

Question: 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.

Answer: ls

Task 11

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

Answer: get

The screenshot shows the HackTheBox starting point page. On the left, there's a sidebar with links like Starting Point, Season 6, Machines, Challenges, Tracks, Rankings, Academy, and HTB for Business. The main area has two tasks:

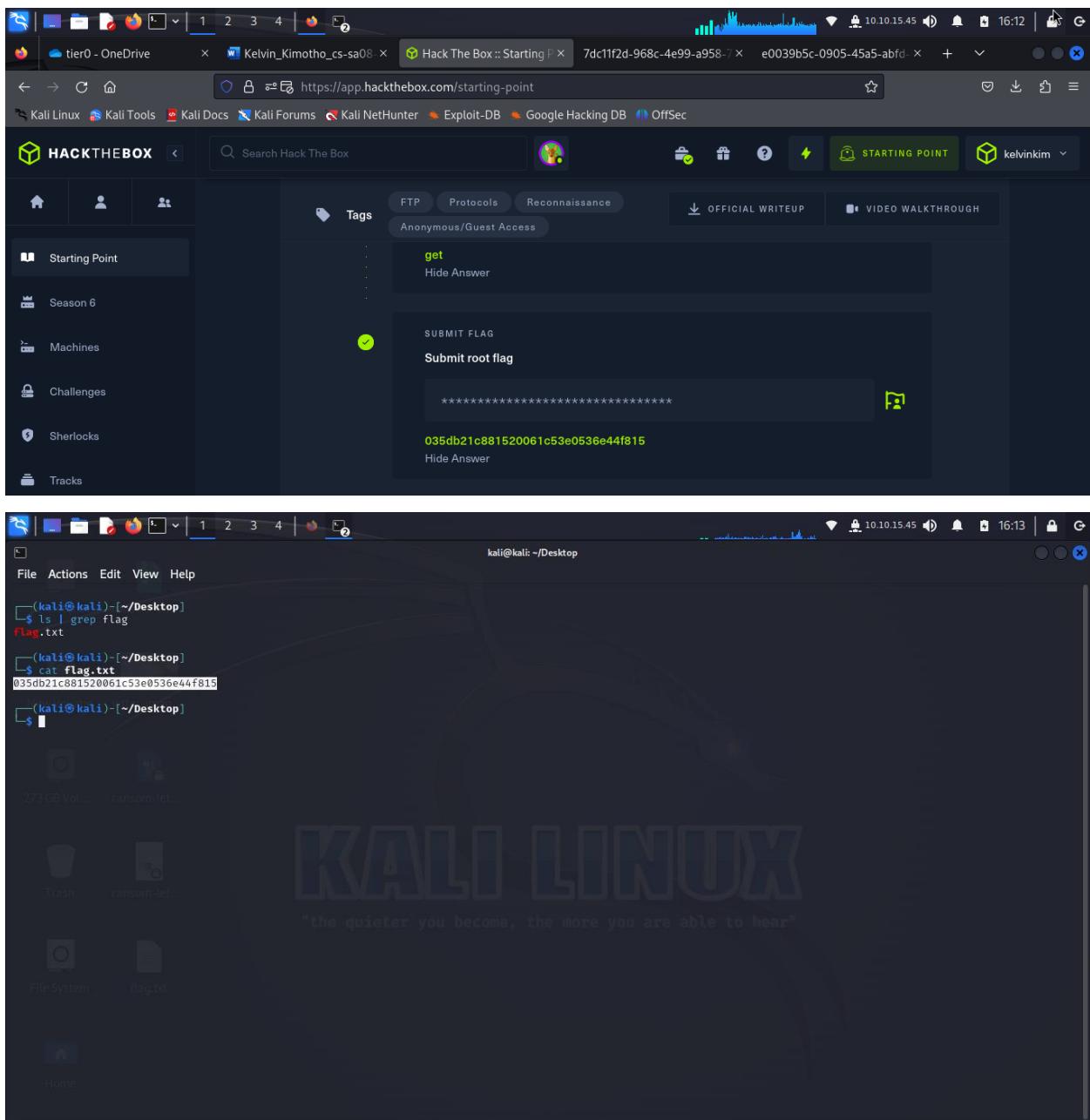
- TASK 10**: A question about file listing commands. It shows a command input field with "ls" and a "Hide Answer" link.
- TASK 11**: A question about the command to download a file from an FTP server. It shows a command input field with "get" and a "Hide Answer" link.

The screenshot shows a terminal window on a Kali Linux system. The user is connected via an FTP session to a host at 10.129.86.255. The session output is as follows:

```
(kali㉿kali)-[~/Desktop]$ ftp 10.129.86.255
Connected to 10.129.86.255.
220 (vsFTPd 3.0.3)
Name (10.129.86.255:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||62249|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||54515|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% [*****] 32 16.71 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.09 KiB/s)
```

Submit root flag

Answer: 035db21c881520061c53e0536e44f815



Dancing

- Here, I learnt on how to transfer files between computers on the same network.
- SMB (server message block) for example is a protocol mostly in windows machines used share files and other resources between end points in a network.

- SMB protocol runs on port 445.
- SMB runs on the application layer as per the OSI model.
- Microsoft SMB Protocol is often used with NetBIOS over TCP/IP.
- A share is an SMB-enabled storage on the network.
- A share can be accessed by any client with an address to the server and the correct username and password.
- We can use guest account or even make anonymous logins incase the network admin misconfigured.

For Enumeration,

- We will use Nmap to scan for open ports and services running there. -sV flag will allow us get both the service and the version running.

```
"nmap -sV Target_IP"
```

- We can access the shares in the target machine from our Linux attacking machine using "smbclient" tool.
- To install it we run " apt-get install smbclient"
- And to run it, this is the format. "smbclient -L Target_IP", where the -L helps us Select the targeted host for the connection request.
- Without the correct login creds, we can login as quest or anonymous users.

Shares present in our target may include,

- ADMIN\$ share which is a hidden share that allows system administrators to have remote access to every disk volume on a network connected system.
- IPCS\$ share is used for inter process communication via named pipes.
- c\$ is an administrative share where the operating system resides.

To gain access to a share we use smbclient.

- We use the following command format "smbclient \\\Target_IP\share"
- We need to have the correct credentials to access the share, otherwise we will always get an error "NT_STATUS_ACCESS_DENIED"

Human made shares are prone to attacks, we should always focus on those.

- After a successful login, we use "help" command to see what we can do in the shell.
- we have commands like, cd to navigate through directories, ls for file listing, get for downloading contents/files, exit for exiting the smb shell,etc.

Then I answered the questions that followed.

Task 1

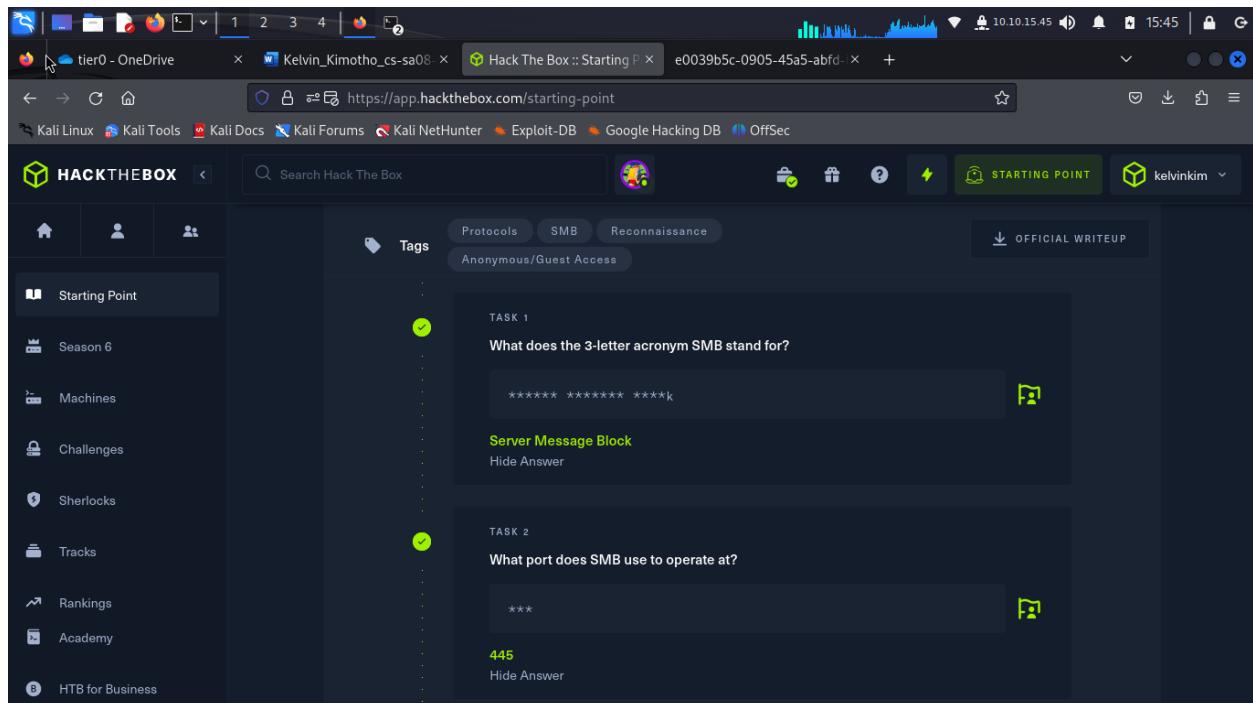
Question: What does the 3-letter acronym SMB stand for?

Answer: server message block

Task 2

Question: What port does SMB use to operate at?

Answer: 445



Task 3

Question: What is the service name for port 445 that came up in our Nmap scan?

Answer: microsoft-ds

The screenshot shows the HackTheBox interface. On the left, there's a sidebar with tabs for Starting Point, Season 6, Machines, Challenges, and Sherlocks. The Starting Point tab is selected. In the center, under the 'Tags' section, there are buttons for Protocols, SMB, Reconnaissance, and Anonymous/Guest Access. Below these buttons, a green checkmark icon indicates Task 3 is completed. The task details are as follows:

TASK 3
What is the service name for port 445 that came up in our Nmap scan?
*****_*_s
microsoft-ds
Hide Answer

At the bottom right of the interface, there's a green 'STARTING POINT' button.

The screenshot shows a terminal window on Kali Linux with the command `nmap -sV 10.129.1.12` running. The output of the Nmap scan is displayed, showing various ports and their services. The relevant part of the output is:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 15:28 UTC
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 15:29 (0:00:04 remaining)
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 83.33% done; ETC: 15:29 (0:00:00 remaining)
Nmap scan report for 10.129.1.12
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (conn-refused)
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 60.25 seconds
```

Below the terminal, the HackTheBox interface is visible, showing the same task details as the first screenshot. The 'microsoft-ds' answer is listed under the task details.

Task 4

Question: What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

Answer: -L

Task 5

Question: How many shares are there on Dancing?

Answer: 4

The screenshot shows the HackTheBox web interface. On the left, a sidebar lists various sections: Starting Point (selected), Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area displays Task 5 under the 'Starting Point' section. The task asks: "What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?". The answer provided is "-L". Below this, another task is listed: "How many shares are there on Dancing?", with the answer "4". The interface includes navigation bars at the top and a search bar.

(kali㉿kali)-[~/Desktop]\$ smbclient -L 10.129.1.12
Password for [WORKGROUP\kali]:
Sharename Type Comment
ADMIN\$ Disk Remote Admin
C\$ Disk Default share
IPC\$ IPC Remote IPC
WorkShares Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.1.12 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(kali㉿kali)-[~/Desktop]\$ ls

What is the 'flag' or 'switch' that we can use with the smbclient utility to list the available shares on Dancing?

Machines Challenges Sherlocks Tracks Rankings Academy HTB for Business

Task 6

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

Answer: workshares

HACKTHEBOX Search Hack The Box

Tags: Protocols, SMB, Reconnaissance, Anonymous/Guest Access

OFFICIAL WRITEUP

TASK 6
What is the name of the share we are able to access in the end with a blank password?
*****5
WorkShares Hide Answer

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

get Hide Answer

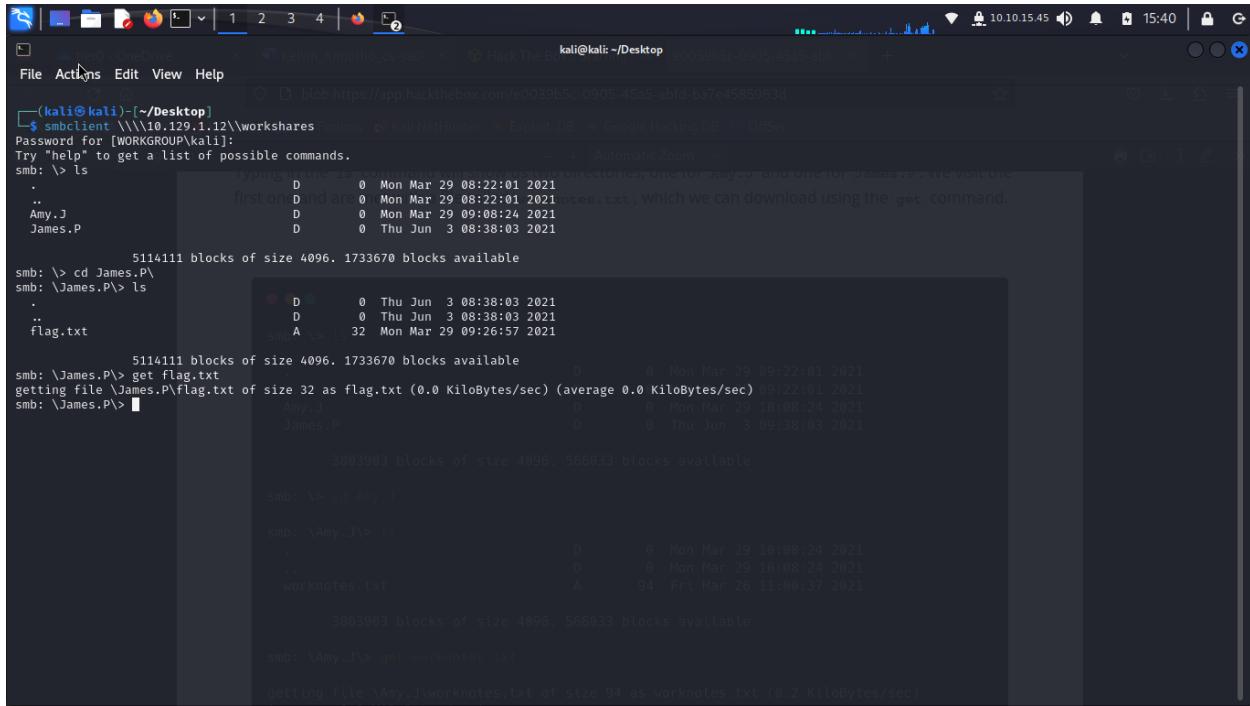
Starting Point Season 6 Machines Challenges Sherlocks Tracks Rankings Academy HTB for Business

Task 7

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

Answer: get

I used get command to retrieve a flag.txt file from a user folder that was in the workshare.



The screenshot shows a terminal window on a Kali Linux system. The user is connected via an SMB session to a share named 'workshares' on a host at 10.129.1.12. The terminal shows the following sequence of commands and outputs:

```
(kali㉿kali)-[~/Desktop]
$ smbclient \\\\10.129.1.12\\\\workshares -U James.P -P P@ssw0rd
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: > ls
.
..
Amy.J
James.P
      D   0  Mon Mar 29 08:22:01 2021
      D   0  Mon Mar 29 08:22:01 2021  notes.txt, which we can download using the get command.

smb: > cd James.P\\
smb: \James.P> ls
.
..
flag.txt
      D   0  Thu Jun  3 08:38:03 2021
      D   0  Thu Jun  3 08:38:03 2021
      A  32  Mon Mar 29 09:26:57 2021

      5114111 blocks of size 4096. 1733670 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) 09:22:01 2021
smb: \James.P> 

      3803903 blocks of size 4096. 566033 blocks available

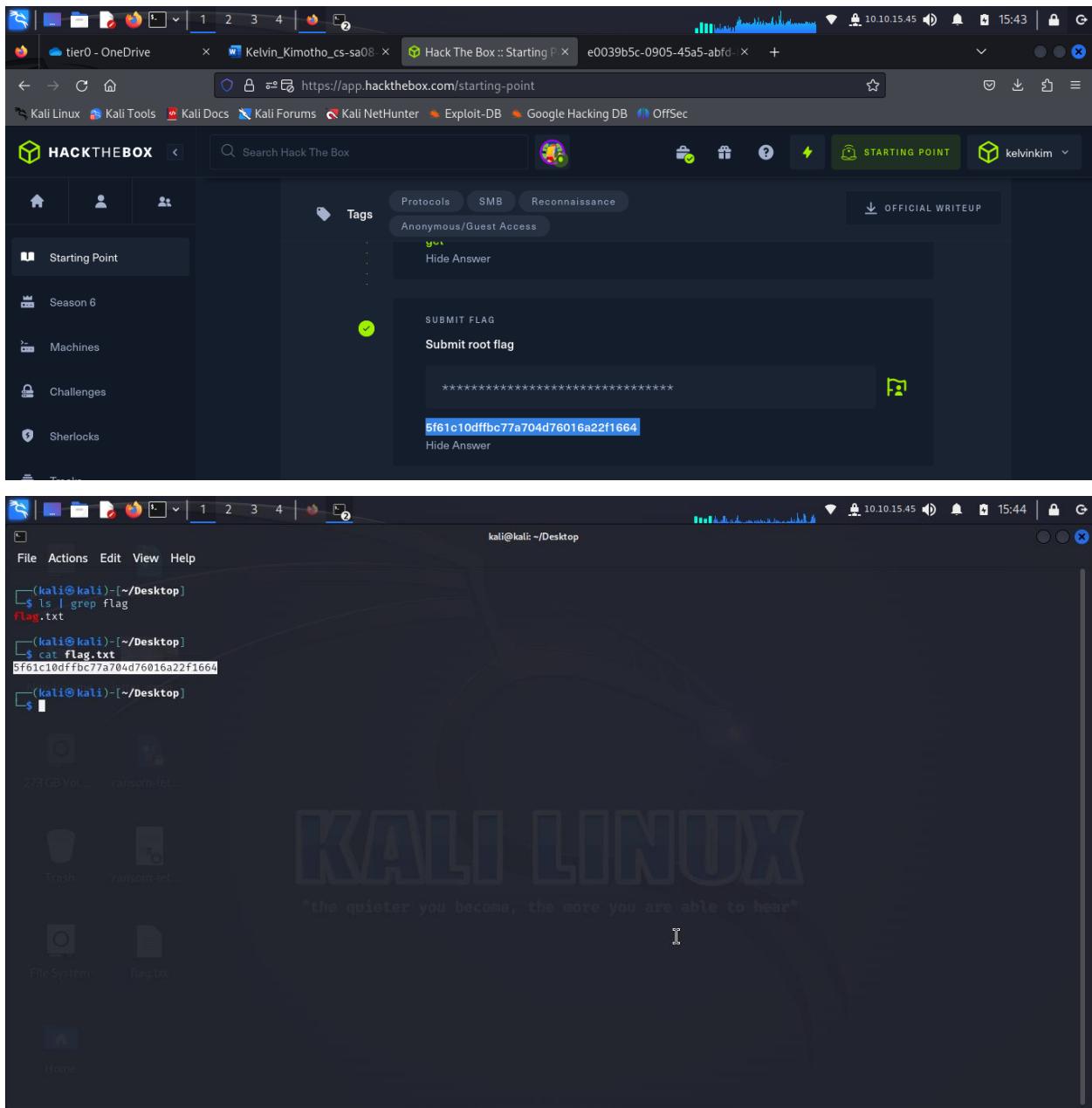
smb: \> cd Amy.J
smb: \Amy.J> ls
.
..
worknotes.txt
      D   0  Mon Mar 29 10:08:24 2021
      D   0  Mon Mar 29 10:08:24 2021
      A   94  Fri Mar 26 11:00:37 2021

      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)
```

Submit root flag

Answer: 5f61c10dffbc77a704d76016a22f1664



Redeemer

The following is what i learnt under this section.

- A database is a collection of organized information that we can update, manage,etc.
- In-memory databases are those that managed in the RAM system. Like, they rely on primary memory for data storage. An example is Redis.

- Since primary memory is faster than secondary memory, Redis offers efficient and minimal response time.

During the enumeration phase,

- We first ping the target IP to test our connectivity.
- Then we can do a nmap scan to see what ports are running on the target machine.

"nmap -p- -sV IP", where -sV determines both the service and its version

- Redis (Remote dictionary server) is an advanced NoSQL database used as a cache, database and also a message broker.
- Data is stored in dictionary format (in key value pairs).
- CLI (command line interface) is a tool we can use to gain access to Redis's data and also its functionalities.
- The database is stored in the server ram for fast data access.
- To install Redis we can use the following command. "sudo apt install redis-tools"
- we can use "redis-cli --help" gives us switches we can use.
- To specify the host, we are targeting we use the -h flag. An example include, "redis-cl -h Target_IP"
- After a successful connection, we see a prompt in terminal. "Info" command will give use information about the server.
- We then select the target database using it index. "Select INDEX". We will get an ok message if the selection succeeded.
- we can list all the keys present in the database using the command. "keys *"
- we can view the values stored for a corresponding key using the get command followed by the keynote. "get KEY".

I went ahead and answered the questions that followed.

Task 1

Question: Which TCP port is open on the machine?

Answer: 6379

Task 2

Question: Which service is running on the port that is open on the machine?

Answer: Redis

The screenshot shows the HackTheBox starting point page. On the left, there's a sidebar with links like Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area has tabs for Redis, Vulnerability Assessment, Databases, and Reconnaissance. Below these are sections for TASK 1 and TASK 2. TASK 1 asks "Which TCP port is open on the machine?" with the answer "6379" highlighted in green. TASK 2 asks "Which service is running on the port that is open on the machine?" with the answer "Redis" highlighted in green.

The terminal window shows the following Nmap command and its output:

```
$ nmap -p- -T4 -SVC 10.129.105.10 -oA nmap - https://nmap.org ) at 2024-09-21 14:09 UTC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 14:09 UTC
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 1.00% done; ETC: 14:18 (0:08:15 remaining)
Warning: 10.129.105.10 giving up on port because retransmission cap hit (6).
Stats: 0:08:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.13% done; ETC: 14:32 (0:13:57 remaining)
Stats: 0:11:49 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 52.17% done; ETC: 14:32 (0:10:49 remaining)
Stats: 0:19:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 86.80% done; ETC: 14:32 (0:02:57 remaining)
Stats: 0:20:37 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.98% done; ETC: 14:32 (0:01:33 remaining)
Stats: 0:21:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.47% done; ETC: 14:31 (0:00:07 remaining)
Nmap scan report for 10.129.105.10
Host is up (0.20s latency).
Not shown: 65277 closed tcp ports (conn-refused), 257 filtered tcp ports (no-response)
```

The output indicates that Redis is running on port 6379. Below the terminal, a list of steps is provided for interacting with Redis:

- we can use "redis-cli --help" gives us switches we can use.
- To specify the host, we are targeting we use the -h flag. An example [code]redis-cli -h Target_IP[code]
- After a successful connection, we see a prompt in terminal, "Info" command will give use information about the server.
- We then select the target database using it index. "Select INDEX". We will get an ok message if the selection succeeded.
- we can list all the keys present in the database using the command, "keys *"
- now we can do that value stored has a password for our new user password (which

Task 3

Question: What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database

Answer: in-memory database

Task 4

Question: Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments.

Answer: redis-cli

The screenshot shows a web browser window with the URL <https://app.hackthebox.com/starting-point>. The page is titled "Hack The Box :: Starting P". On the left, there's a sidebar with navigation links: Home, Profile, Starting Point (which is selected and highlighted in blue), Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main content area has a dark background with white text. At the top, it says "Tags" and lists "Redis", "Vulnerability Assessment", "Databases", "Reconnaissance", and "Anonymous/Guest Access". Below this is a section titled "in-memory database" with a "Hide Answer" link. Further down, there's a task section for "TASK 4" asking "Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments." The answer provided is "redis-cli". There are also "OFFICIAL WRITEUP" and "HTB for Business" buttons at the bottom of this section. The browser's address bar shows "tier0 - OneDrive" and "Kelvin_Kimotho_cs-sa08". The status bar at the bottom right shows the IP address 10.10.15.45, the time 14:16, and a lock icon.

Task 5

Question: Which flag is used with the Redis command-line utility to specify the hostname?

Answer: -h

Task 6

Question: Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?

Answer: info

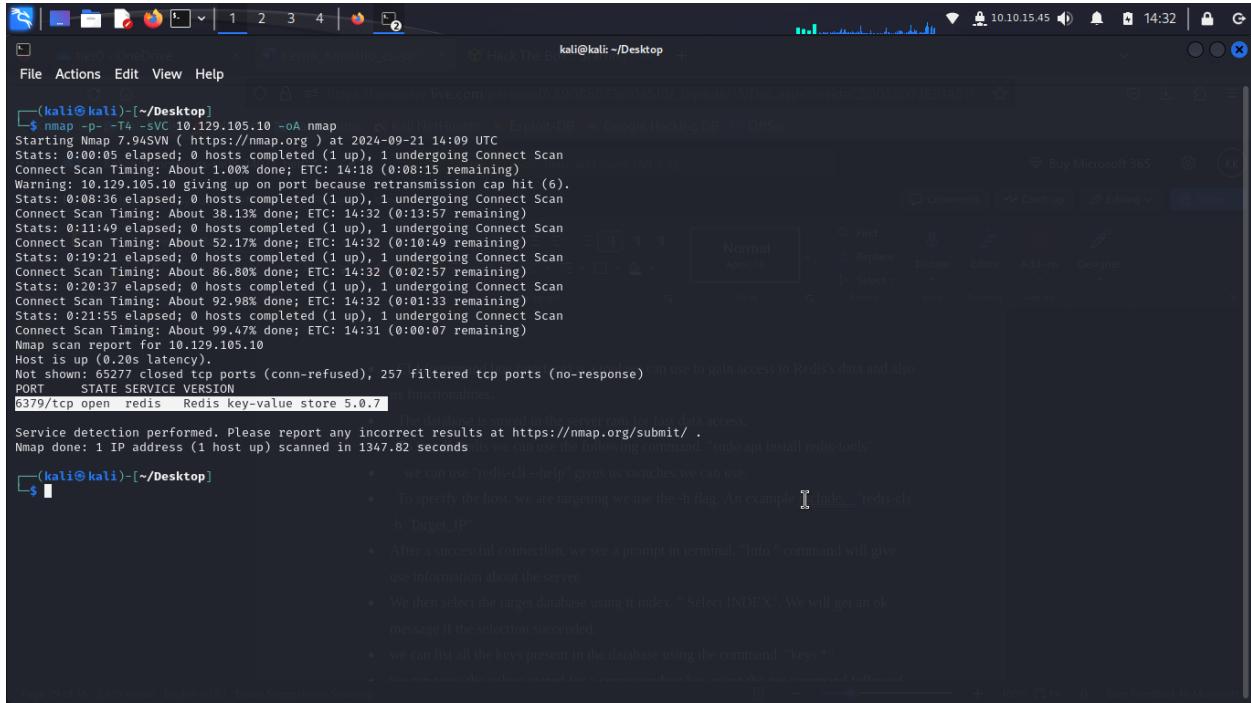
The image shows two screenshots of a Kali Linux desktop environment. The top screenshot is a browser window displaying a challenge from 'Hack The Box :: Starting Point'. It asks: 'Which flag is used with the Redis command-line utility to specify the hostname?'. The answer is given as '-h'. Below this is another challenge: 'Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?'. The answer is given as 'info'. The bottom screenshot shows a VNC viewer window titled 'HTB Viewer' showing a terminal session on a machine named 'eu-starting-point-2-dhcp'. The terminal shows the user has run the command 'redis-cli -h 10.129.105.10' and is now in the Redis info command, displaying various system statistics.

```
[*]$ redis-cli -h 10.129.105.10
10.129.105.10:6379> info
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.3.0
process_id:753
run_id:34221fab3941501e39d501332f53f47fb663e186
tcp_port:6379
uptime_in_seconds:3104
uptime_in_days:0
```

Task 7

Question: What is the version of the Redis server being used on the target machine?

Answer: 5.0.7



```
(kali㉿kali)-[~/Desktop]$ nmap -p- -T4 -sV 10.129.105.10 -oA nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-21 14:09 UTC
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 1.00% done; ETC: 14:18 (0:08:15 remaining)
Warning: 10.129.105.10 giving up on port because retransmission cap hit (6).
Stats: 0:08:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 38.13% done; ETC: 14:32 (0:13:57 remaining)
Stats: 0:11:49 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 52.17% done; ETC: 14:32 (0:10:49 remaining)
Stats: 0:19:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 86.80% done; ETC: 14:32 (0:02:57 remaining)
Stats: 0:20:37 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.98% done; ETC: 14:32 (0:01:33 remaining)
Stats: 0:21:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.47% done; ETC: 14:31 (0:00:07 remaining)
Nmap scan report for 10.129.105.10
Host is up (0.20s latency).
Not shown: 65277 closed tcp ports (conn-refused), 257 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
6379/tcp  open  redis  Redis key-value store 5.0.7
Nmap done: 1 IP address (1 host up) scanned in 1347.82 seconds
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1347.82 seconds
```

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running an nmap scan against the IP address 10.129.105.10. The output indicates that port 6379 is open and identified as a Redis service running version 5.0.7. Other ports are either closed or filtered. The terminal window has a dark background with light-colored text. There are several tabs open in the browser above the terminal, including 'Kali Linux - Google Chrome' and 'Hack The Box - Exploit - Exploit - Google Hacking Dorks'. The status bar at the bottom of the screen shows the IP address 10.10.15.45, the time 14:32, and other system information.

Task 8

Question: Which command is used to select the desired database in Redis?

Answer: select

The screenshot shows the HackTheBox web interface. On the left, a sidebar lists various sections: Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The 'Starting Point' section is currently selected. In the main area, there are two tasks:

- TASK 7**: What is the version of the Redis server being used on the target machine?
Answer: 5.0.7
- TASK 8**: Which command is used to select the desired database in Redis?
Answer: select

The screenshot shows a VNC session of a Parrot OS desktop. On the left, a file browser window shows files like 'Parrot', 'kelvinkim's Home', 'my_credentials.txt', and 'README.license'. On the right, a terminal window titled 'Parrot Terminal' displays Redis configuration and a session:

```
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0

# CPU
used_cpu_sys:2.706897
used_cpu_user:2.147805
used_cpu_sys_children:0.000000
used_cpu_user_children:0.001555

# Cluster
cluster_enabled:0

# Keyspace
db0:keys=4,expires=0,avg_ttl=0
10.129.105.10:6379> select 0
OK
10.129.105.10:6379>
```

Task 9

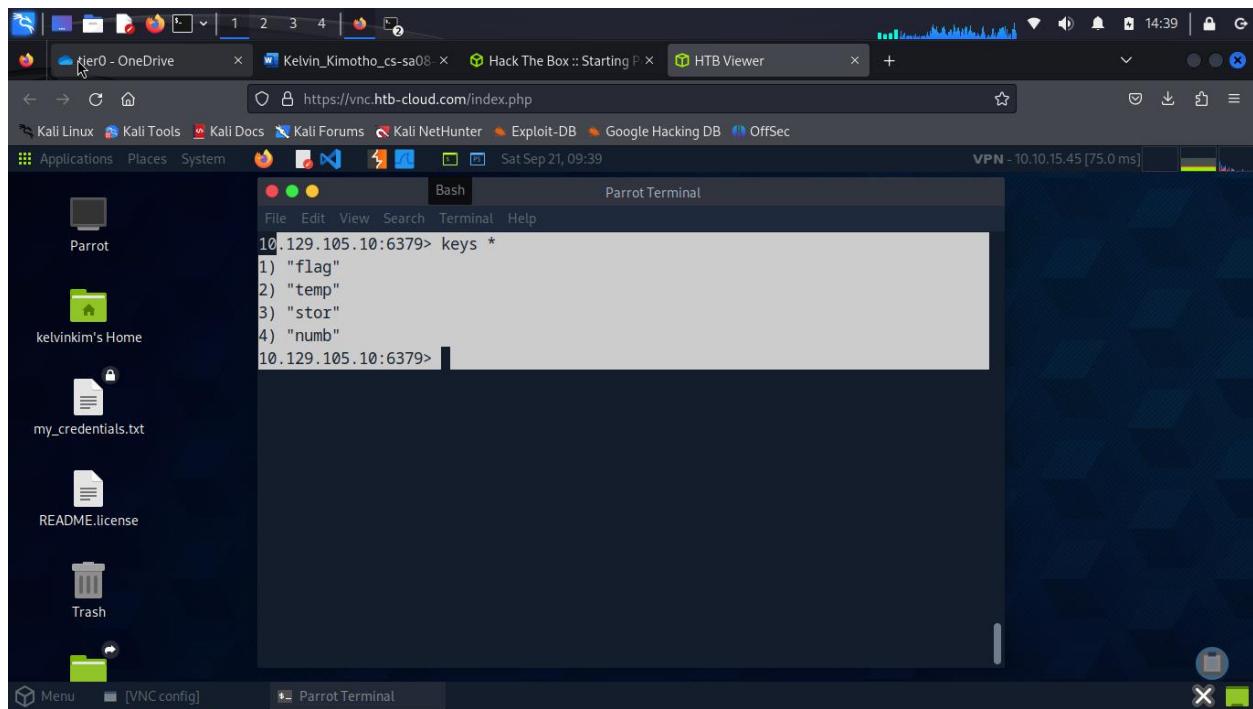
Question: How many keys are present inside the database with index 0?

ANswer: 4

Task 10

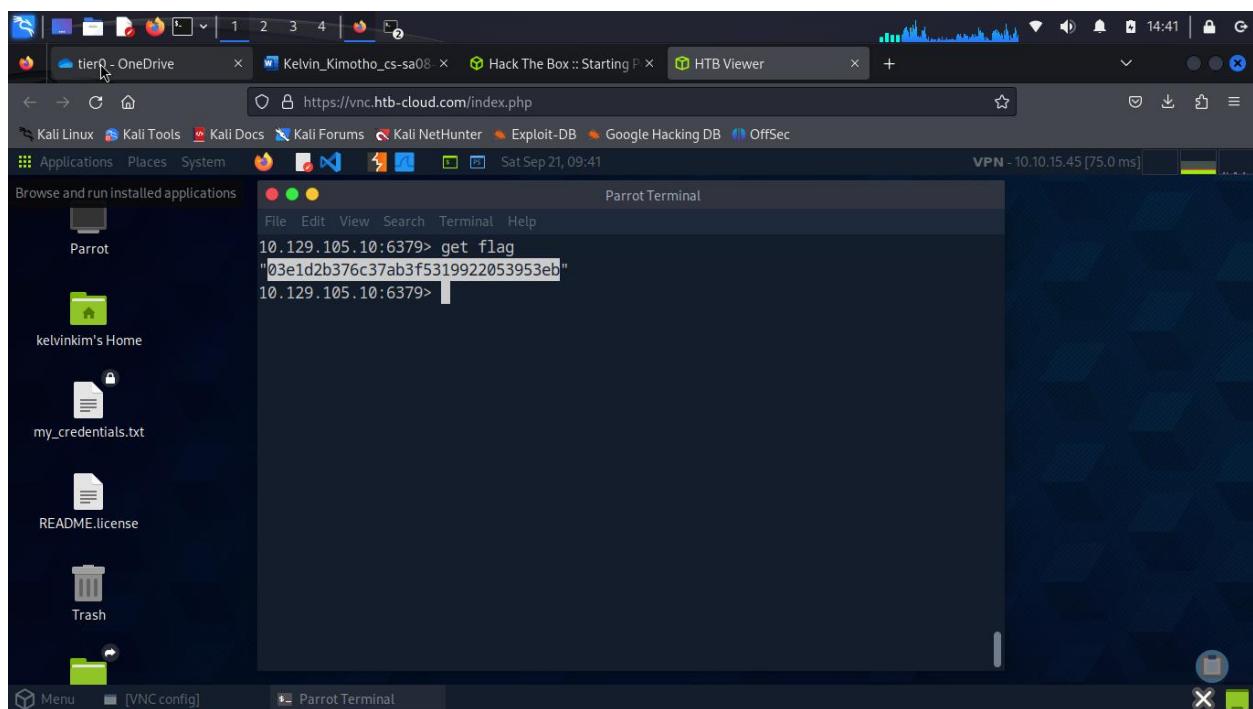
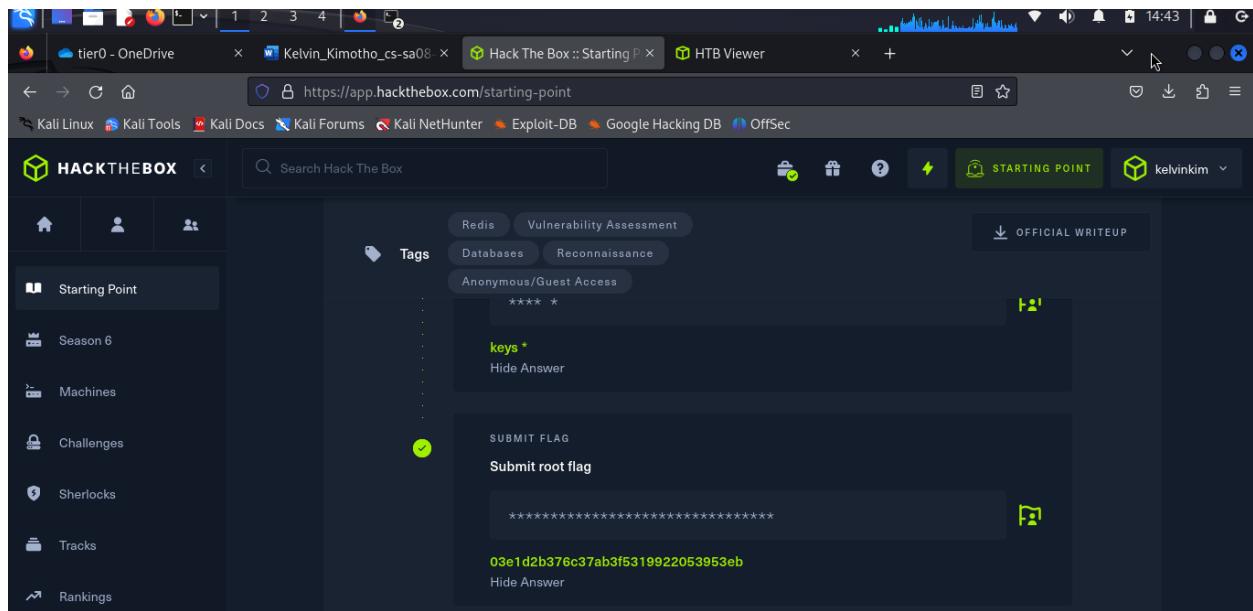
Question: Which command is used to obtain all the keys in a database?

Answer: keys *



Submit root flag

Answer: 03e1d2b376c37ab3f5319922053953eb



Conclusion

After completing this tier, I have gained the practical knowledge on how to connect to a vpn from my machines terminal. I gained insight on various tools and techniques used in the entire penetration testing. How to use Nmap to perform port scans on our target machines, how to gather information about the services running on the machine and how to exploit vulnerabilities associated with the services we find running. I also learnt about databases, In-memory databases for this case and how to exploit or access them. Also gained insight on the server message block protocol for windows systems and how i can access shares from my kali machine using smbclient tool even without the access rights. By exploiting vulnerabilities mostly on human created shares.

