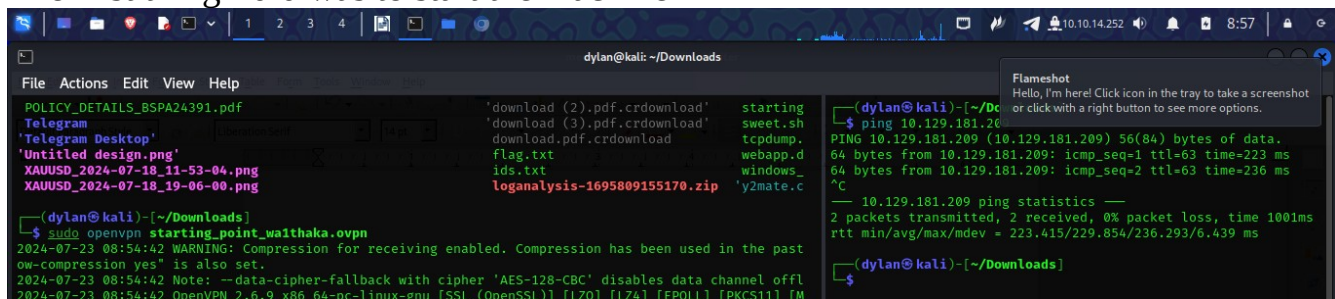


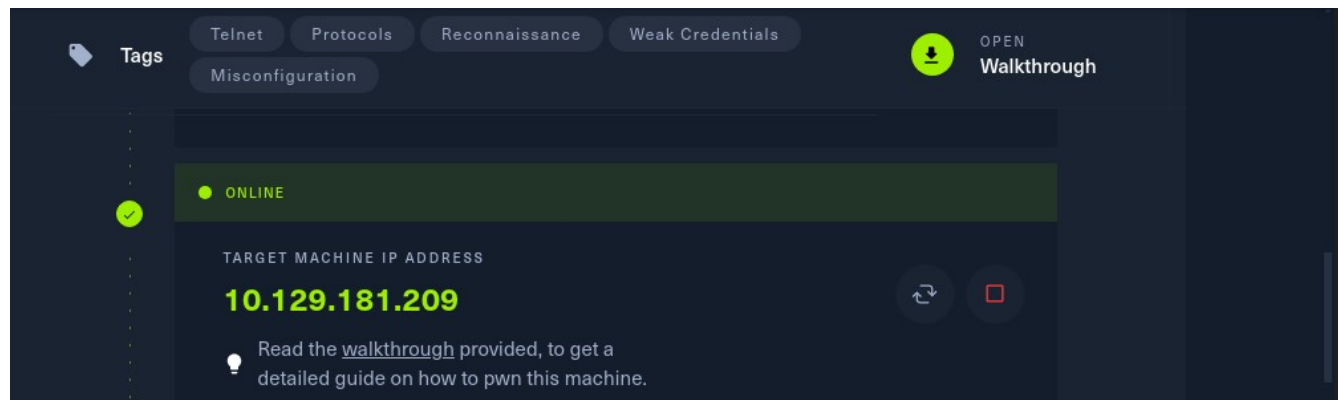
ISSACK WAITHAKA
cs-sa07-24085

Meow

The first thing I did was to start the machine

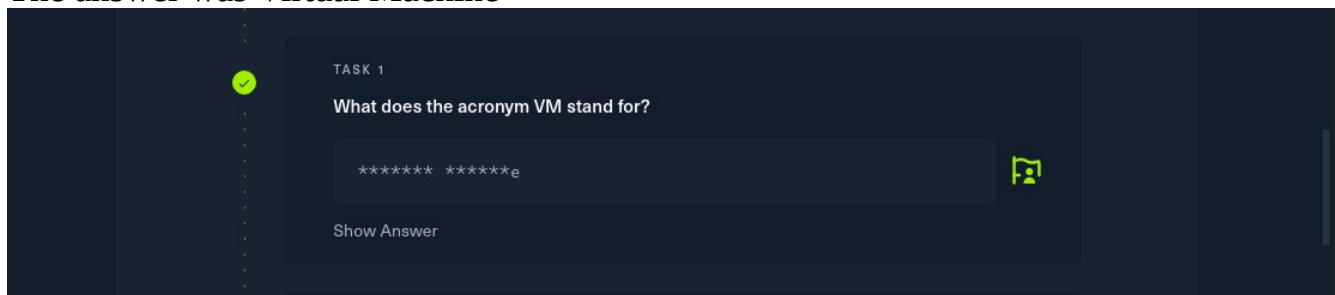


The screenshot shows a Kali Linux terminal window with the title bar 'dylan@kali: ~/Downloads'. The terminal displays a list of downloaded files including 'POLICY_DETAILS_BSPA24391.pdf', 'Telegram Desktop', 'Untitled design.png', 'XAUUSD_2024-07-18_11-53-04.png', and 'XAUUSD_2024-07-18_19-06-00.png'. It also shows the execution of 'sudo openvpn starting_point_waithaka.ovpn' and a 'ping 10.129.181.209' command. The ping results show 56(84) bytes of data, 64 bytes from 10.129.181.209: icmp_seq=1 ttl=63 time=223 ms, and 64 bytes from 10.129.181.209: icmp_seq=2 ttl=63 time=236 ms. The terminal also shows the output of 'ping statistics'.



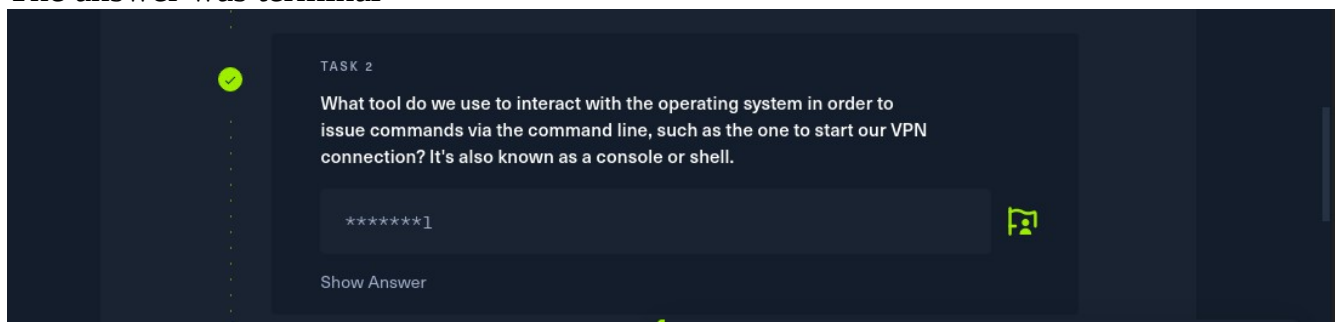
1.

The answer was Virtual Machine



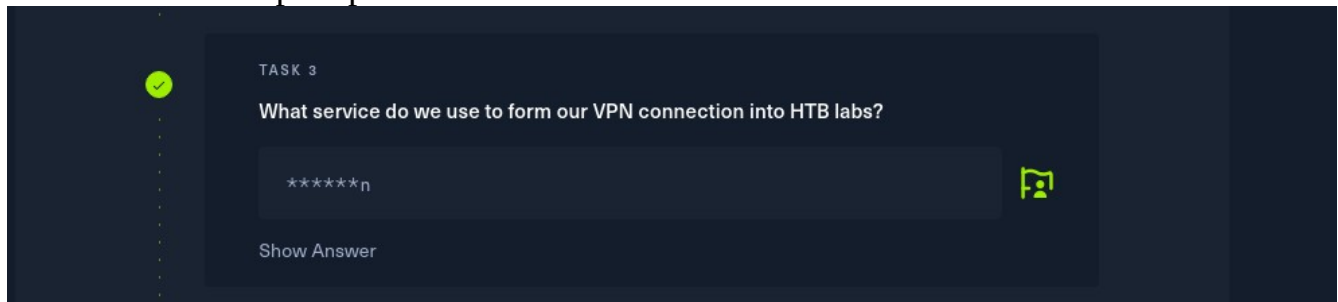
2.

The answer was terminal



3.

The answer was openvpn



A screenshot of a task interface with a dark blue background. On the left, a vertical dashed line with a green checkmark at the top indicates a correct answer. The main area contains the text "TASK 3" and the question "What service do we use to form our VPN connection into HTB labs?". Below the question is a text input field containing "*****n" and a green flag icon to its right. At the bottom of the input area is a "Show Answer" button.

TASK 3

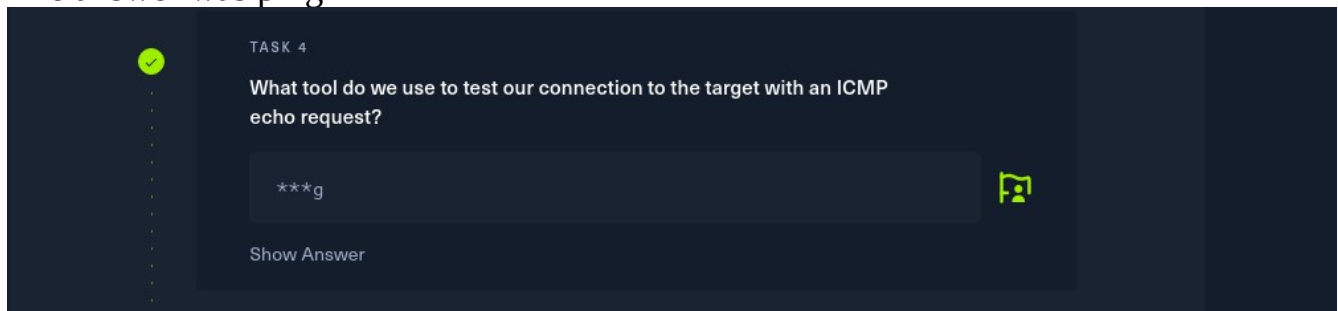
What service do we use to form our VPN connection into HTB labs?

*****n

Show Answer

4.

The answer was ping



A screenshot of a task interface with a dark blue background. On the left, a vertical dashed line with a green checkmark at the top indicates a correct answer. The main area contains the text "TASK 4" and the question "What tool do we use to test our connection to the target with an ICMP echo request?". Below the question is a text input field containing "***g" and a green flag icon to its right. At the bottom of the input area is a "Show Answer" button.

TASK 4

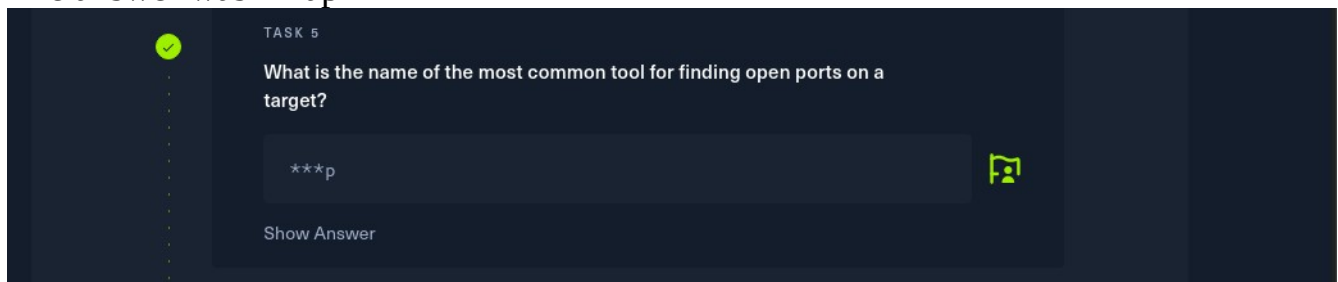
What tool do we use to test our connection to the target with an ICMP echo request?

***g

Show Answer

5.

The answer was nmap



A screenshot of a task interface with a dark blue background. On the left, a vertical dashed line with a green checkmark at the top indicates a correct answer. The main area contains the text "TASK 5" and the question "What is the name of the most common tool for finding open ports on a target?". Below the question is a text input field containing "***p" and a green flag icon to its right. At the bottom of the input area is a "Show Answer" button.

TASK 5

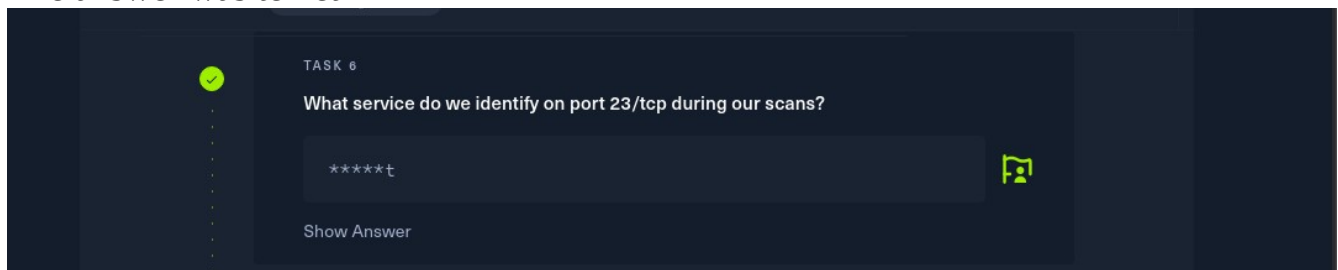
What is the name of the most common tool for finding open ports on a target?

***p

Show Answer

6.

The answer was telnet



A screenshot of a task interface with a dark blue background. On the left, a vertical dashed line with a green checkmark at the top indicates a correct answer. The main area contains the text "TASK 6" and the question "What service do we identify on port 23/tcp during our scans?". Below the question is a text input field containing "*****t" and a green flag icon to its right. At the bottom of the input area is a "Show Answer" button.

TASK 6

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

*****t

Show Answer

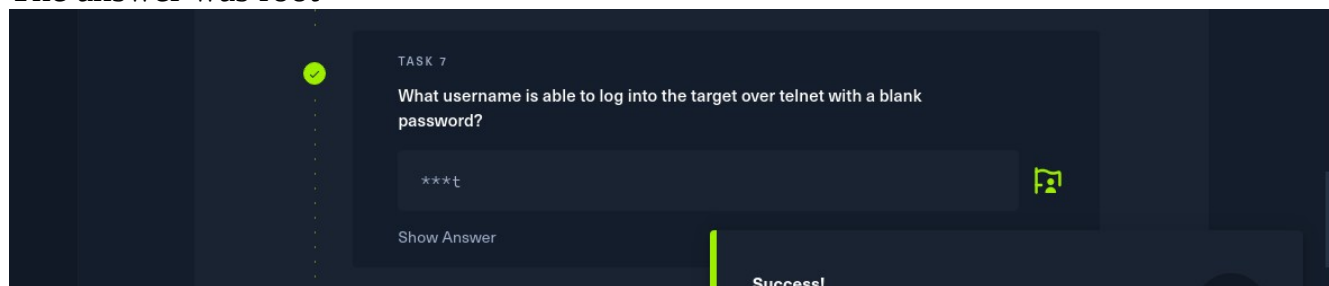
```

(dylan@kali)-[~/Downloads]
$ nmap -sV 10.129.181.209
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 09:07 EAT
Nmap scan report for 10.129.181.209
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
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 77.26 seconds

```

7.
The answer was root



```

POLIC
Teleg
Teleg
Untit
XAUUS
XAUUS

(dylan@kali)-[~/Downloads]
$ telnet -4 10.129.181.209 -l root
Trying 10.129.181.209 ...
Connected to 10.129.181.209.
Escape character is '^]'.
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 Tue 23 Jul 2024 06:13:04 AM UTC

System load:          0.0
Usage of /:            41.7% of 7.75GB
Memory usage:         4%
Swap usage:           0%
Processes:            138
Users logged in:      0
IPv4 address for eth0: 10.129.181.209
IPv6 address for eth0: dead:beef::250:56ff:feb0:ef15

 * Super-optimized for small spaces - read how we shrank 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

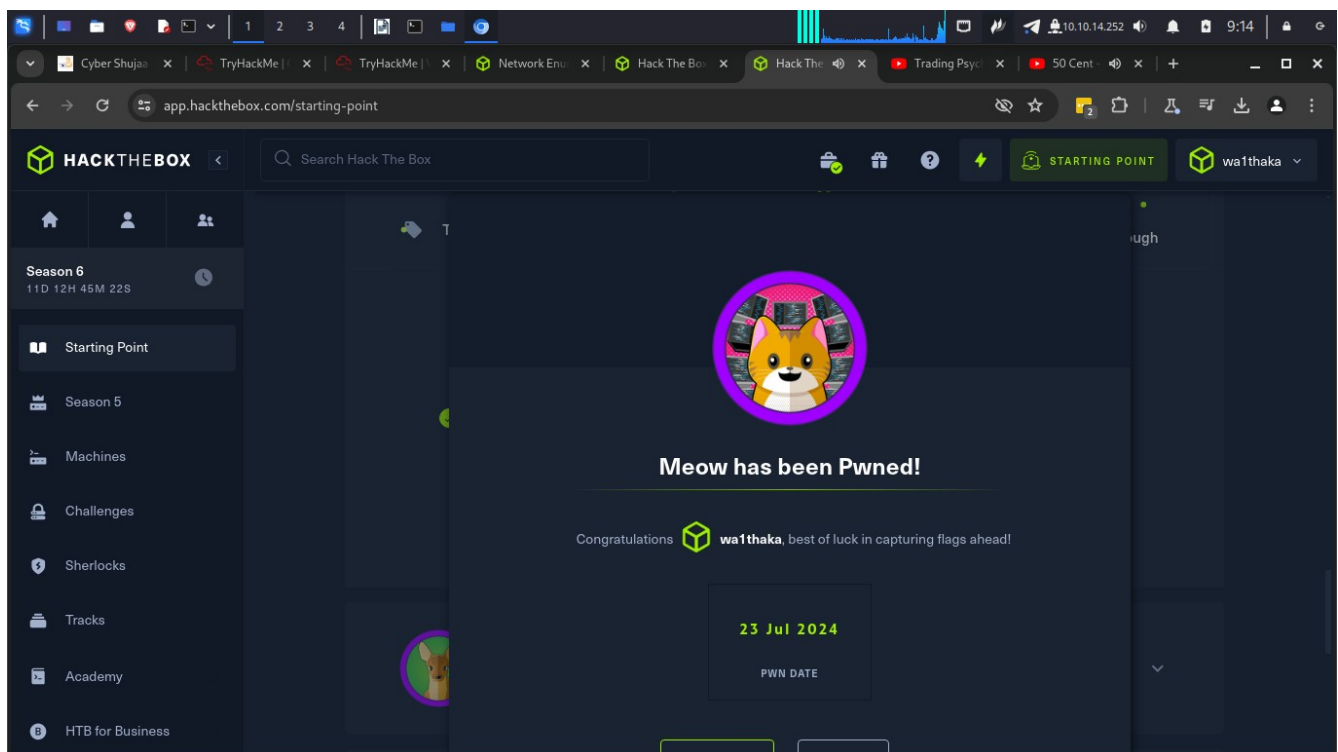
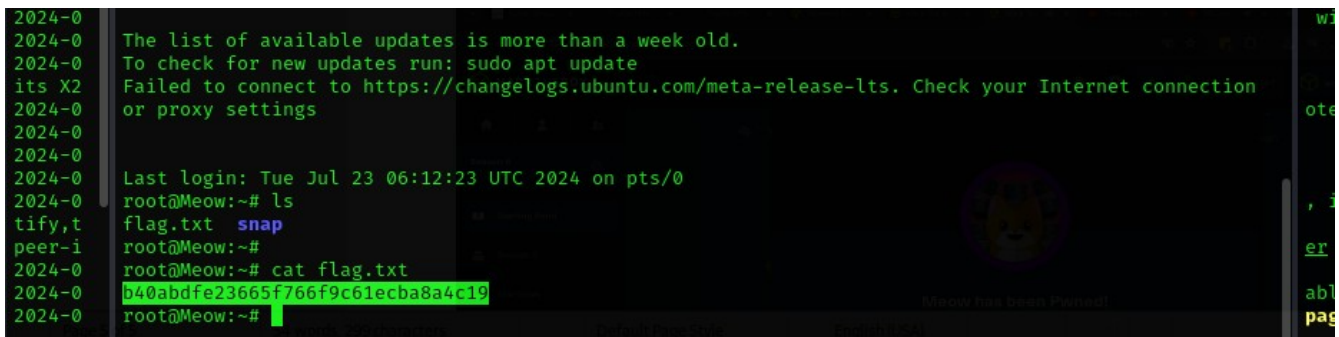
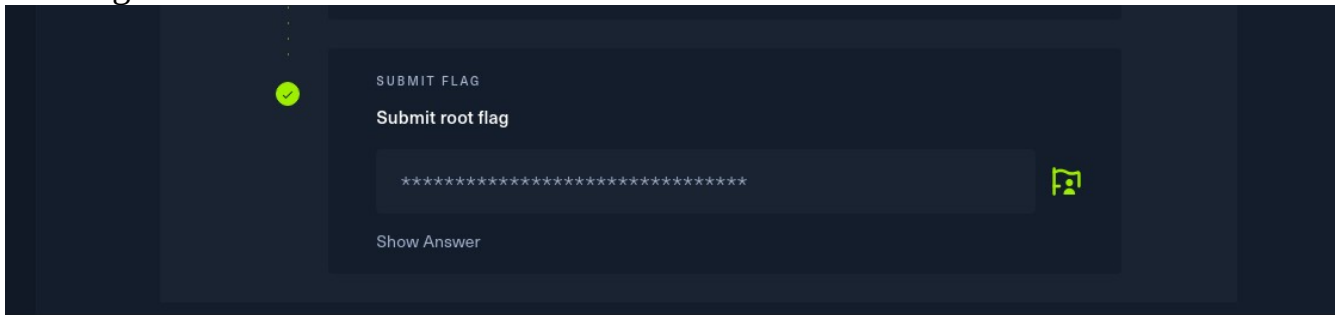
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Last login: Tue Jul 23 06:12:23 UTC 2024 on pts/0
root@Meow:~#

```

8.

The flag was b40abdfе23665f766f9c61ecba8a4c19

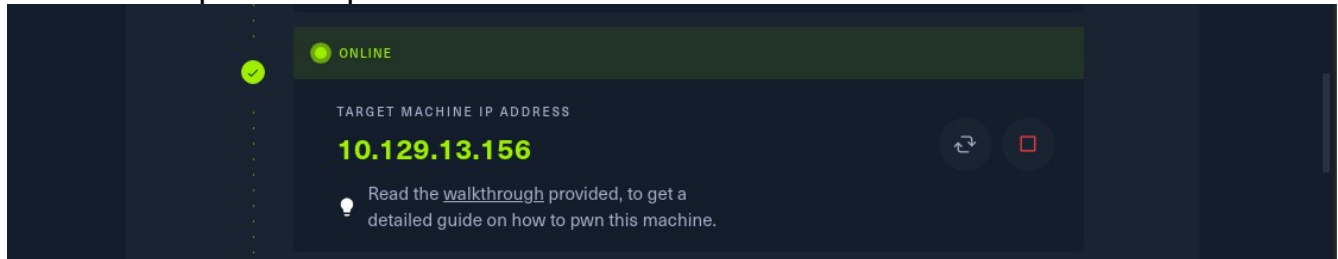


Conclusion

-In this section I was able to learn how to connect to telnet services

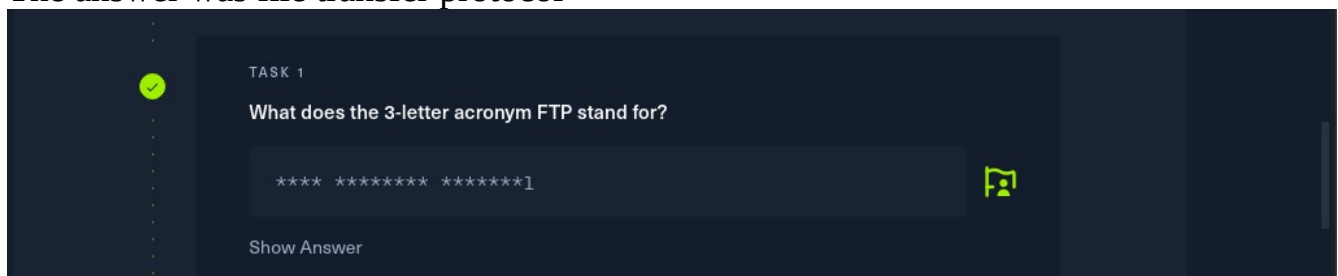
Fawn

-The first step was to spawn the machine



1.

The answer was file transfer protocol



2.

The answer was port 21




3.

The answer was SFTP. This is the secure version of FTP.



4.


The answer Is ping



TASK 4

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


***g



Show Answer

5.


The answer was vsftpd 3.0.3



TASK 5

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

***** *.*.3



Show Answer

```
File Actions Edit View Help
dylan@kali: ~/Downloads

POLICY_DETAILS_BSPA24391
Telegram
Telegram Desktop'
Untitled design.png'
XAUUSD_2024-07-18_11-53-
XAUUSD_2024-07-18_19-06-

(dylan@kali)-[~/Downl]
$ sudo openvpn starting
2024-07-23 08:54:42 WARNI
w-compression yes" is al
2024-07-23 08:54:42 Note:
2024-07-23 08:54:42 OpenV
2024-07-23 08:54:42 libra
2024-07-23 08:54:42 DCO v
2024-07-23 08:54:43 TCP/U
2024-07-23 08:54:43 Socke
2024-07-23 08:54:43 UDPv4
2024-07-23 08:54:43 UDPv4
2024-07-23 08:54:43 TLS:


(dylan@kali)-[~/Downloads]
$ nmap -sV 10.129.13.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 09:31 EAT
Nmap scan report for 10.129.13.156
Host is up (0.22s 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 21.81 seconds

(dylan@kali)-[~/Downloads]
$
The answer was vsftpd 3.0.3
(dylan@kali)-[~/Downloads]
$
```

6.


The answer was unix



TASK 6

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

***x



Show Answer


```
File Actions Edit View Help
POLICY_DETAILS_BSPA24391
Telegram
'Telegram Desktop'
'Untitled design.png'
XAUUSD_2024-07-18_11-53-
XAUUSD_2024-07-18_19-06-


(dylan@kali)-[~/Downloads]
$ sudo openvpn starting
2024-07-23 08:54:42 WARN:
ow-compression yes" is al
2024-07-23 08:54:42 Note:
2024-07-23 08:54:42 OpenV
2024-07-23 08:54:42 libra
2024-07-23 08:54:42 DCO v

(dylan@kali)-[~/Downloads]
$ nmap -sV 10.129.13.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 09:31 EAT
Nmap scan report for 10.129.13.156
Host is up (0.22s 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 21.81 seconds
(dylan@kali)-[~/Downloads]
```

7.

The answer was ftp -h



TASK 7

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

*** -h

Show Answer

8.

The answer was anonymous



TASK 8

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

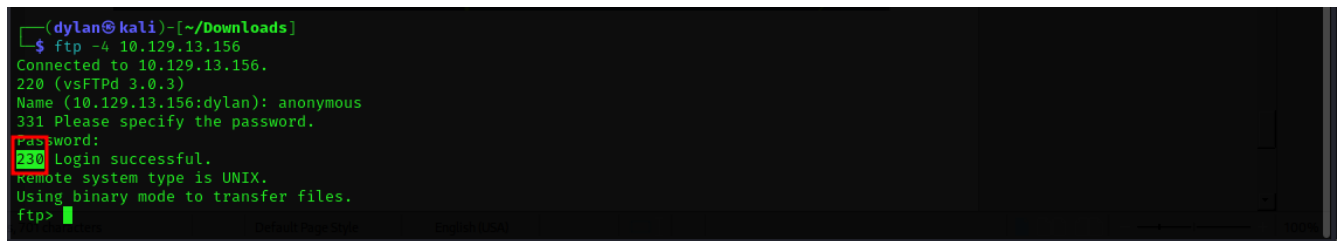
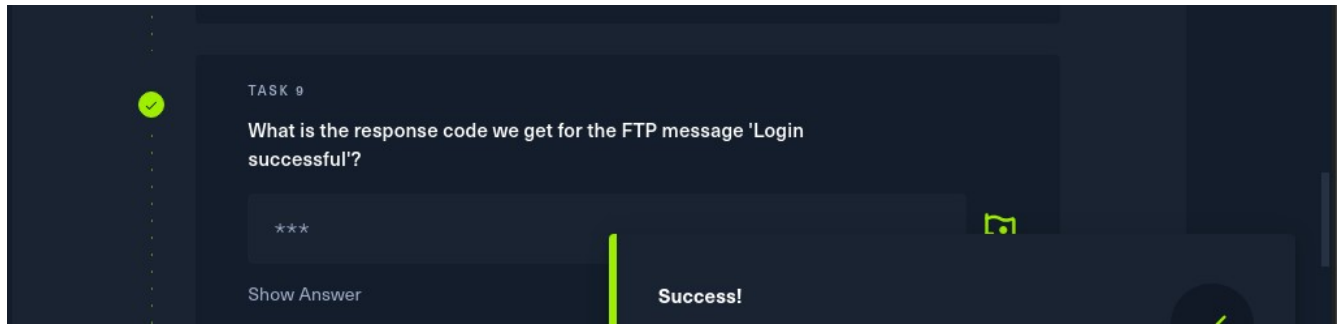
*****s

Show Answer

```
(dylan@kali)-[~/Downloads]
$ ftp -4 10.129.13.156
Connected to 10.129.13.156.
220 (vsFTPd 3.0.3)
Name (10.129.13.156:dylan): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

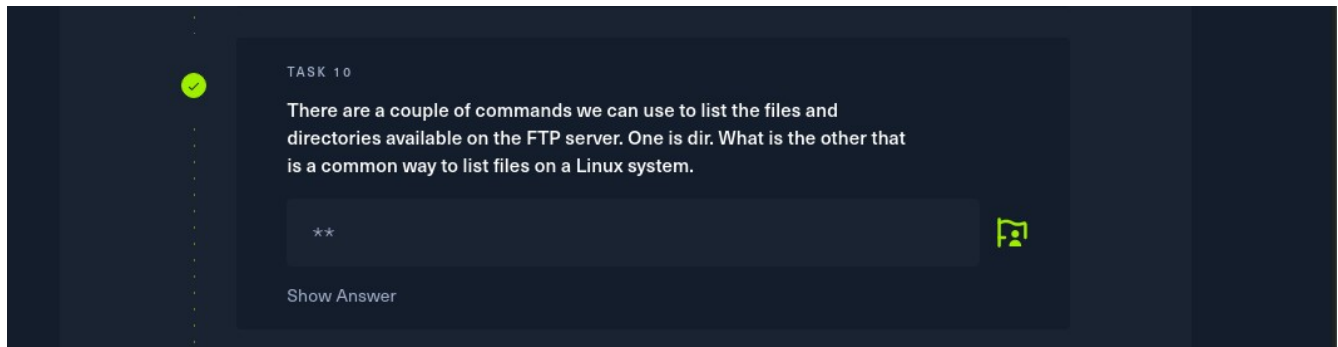

9.

The answer was 230



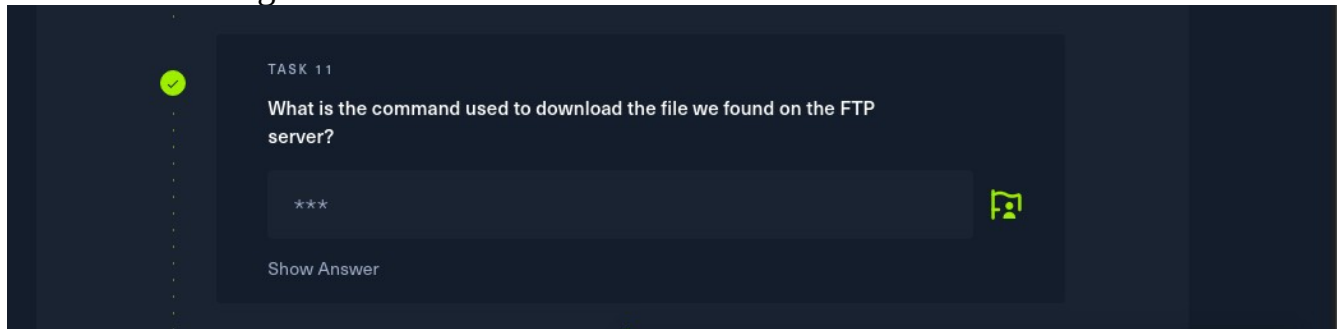
10.

The answer was ls



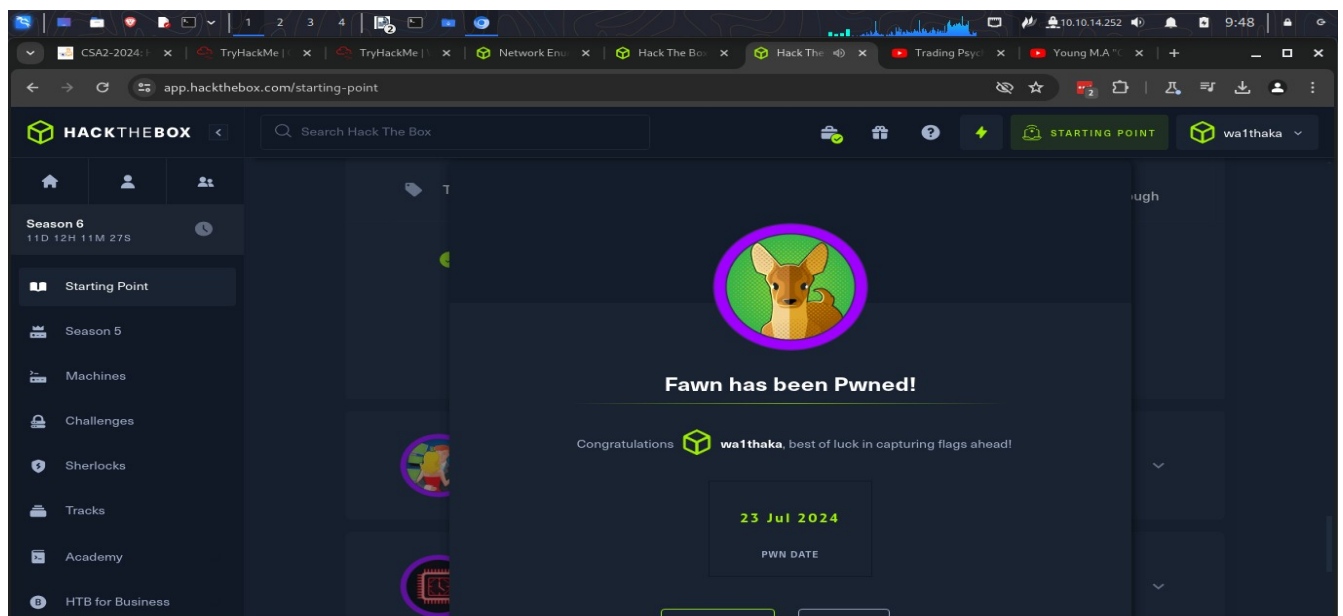
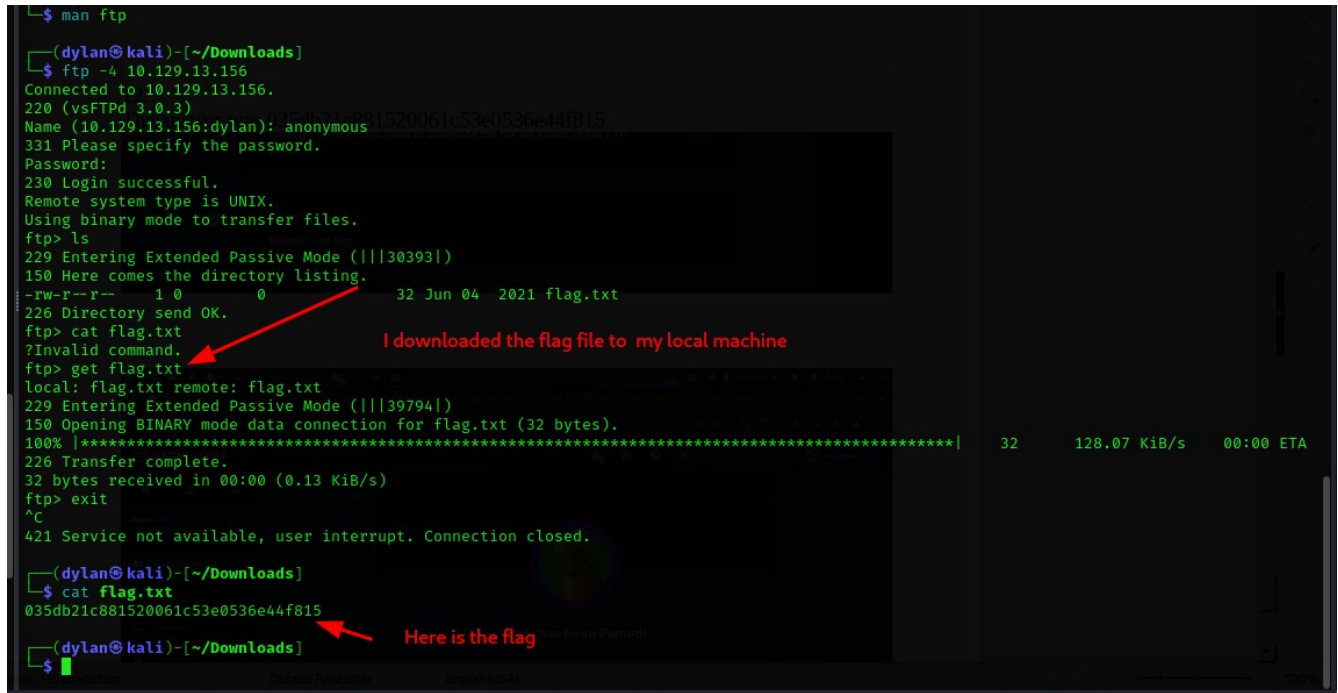
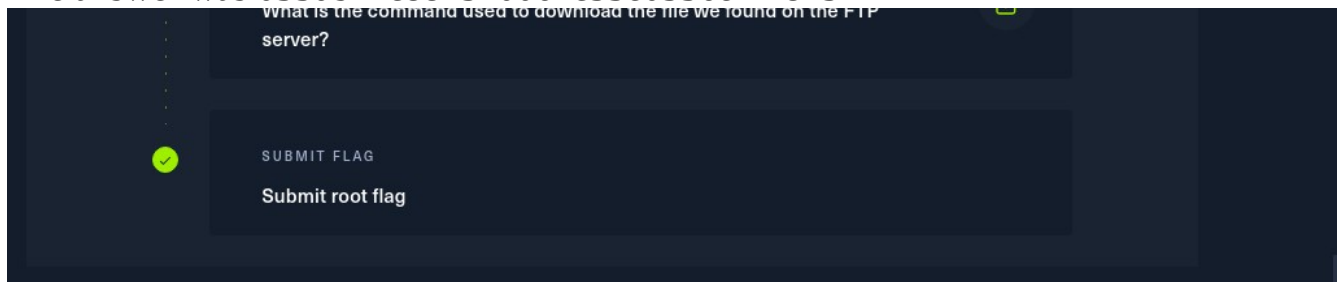
11.

The answer was get



12.

The answer was 035db21c881520061c53e0536e44f815

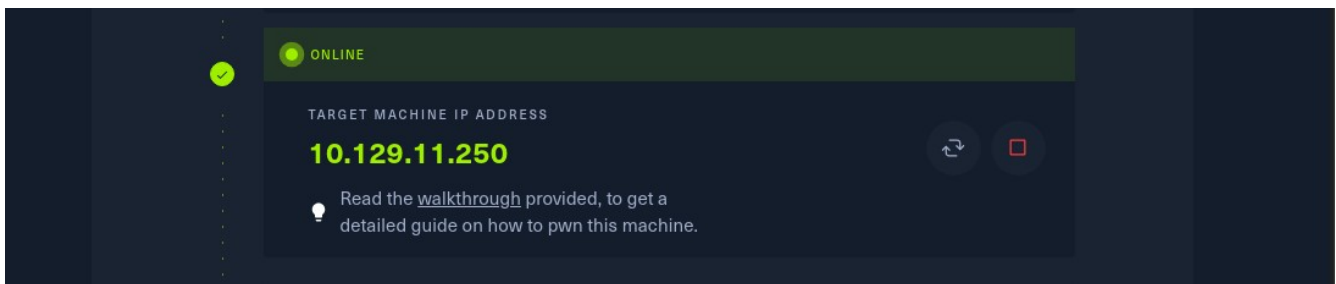


Conclusion

In this room I learnt how to connect to FTP

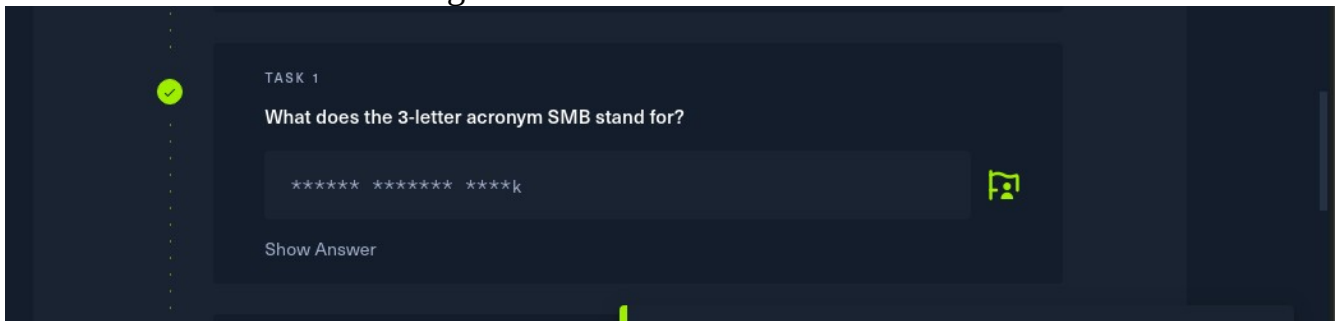
Dancing

I started by spawning the target machine

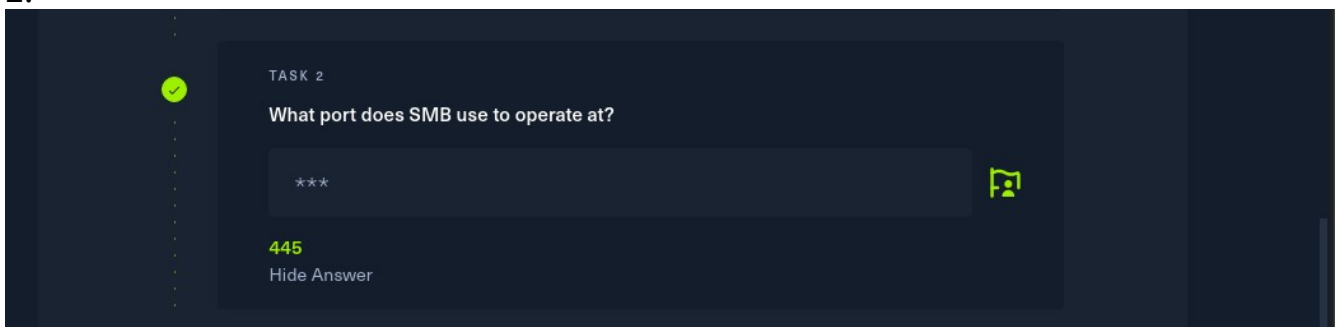


1.

The answer was server message book



2.



3.

TASK 3

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

*****_*s

microsoft-ds

Hide Answer

```
(dylan@kali) [~/Downloads]
(dylan@kali) [~/Downloads]
$ nmap -sV 10.129.11.250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 09:59 EAT
Nmap scan report for 10.129.11.250
Host is up (0.22s 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?   Microsoft Windows
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 73.00 seconds

(dylan@kali) [~/Downloads]
```

4.

TASK 4

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

**

-l

Hide Answer

```
By default, the client writes messages to standard output - typically the user's tty.

-l|--list
This option allows you to look at what services are available on a server. You use it as smbclient -L host and a list should appear. The -I option may be useful if your NetBIOS names don't match your TCP/IP DNS host names or if you are trying to reach a host on another network.
```

5.

TASK 5

How many shares are there on Dancing?

*

4

Hide Answer

```
(dylan@kali)~/Downloads
$ smbclient -L \\10.129.11.250
Password for [WORKGROUP\dylan]:

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
WorkShares     Disk      Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.11.250 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(dylan@kali)~/Downloads
$
```

6.

TASK 6

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

*****s

WorkShares

Hide Answer

```
(dylan@kali)~/Downloads
$ smbclient \\\\10.129.11.250\\WorkShares
Password for [WORKGROUP\dylan]:
Try "help" to get a list of possible commands.
smb: \> ^C

(dylan@kali)~/Downloads
$ smbclient \\\\10.129.11.250\\WorkShares
Password for [WORKGROUP\dylan]:
Try "help" to get a list of possible commands.
smb: \>
```

7.

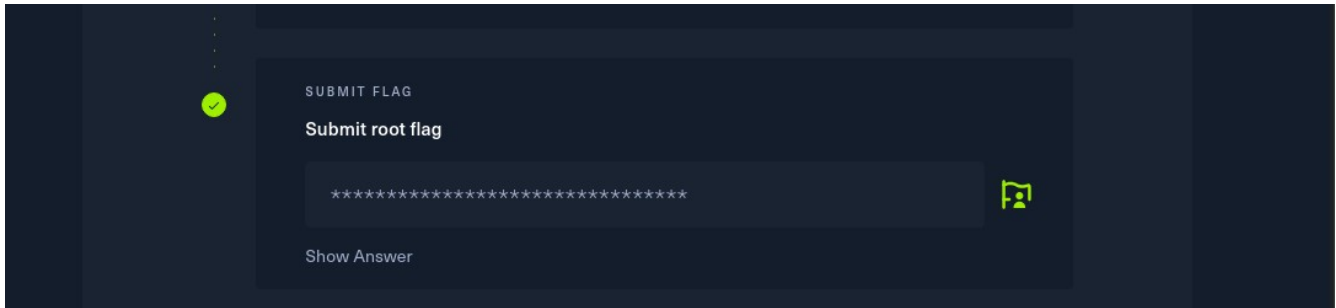
TASK 7

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

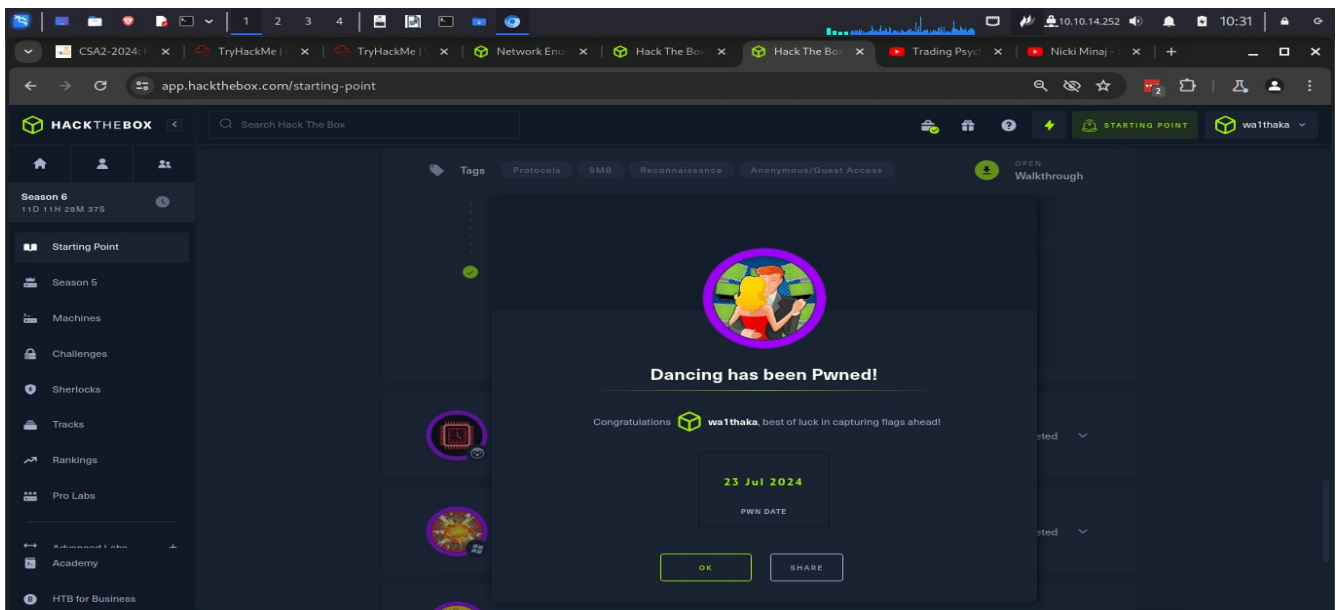
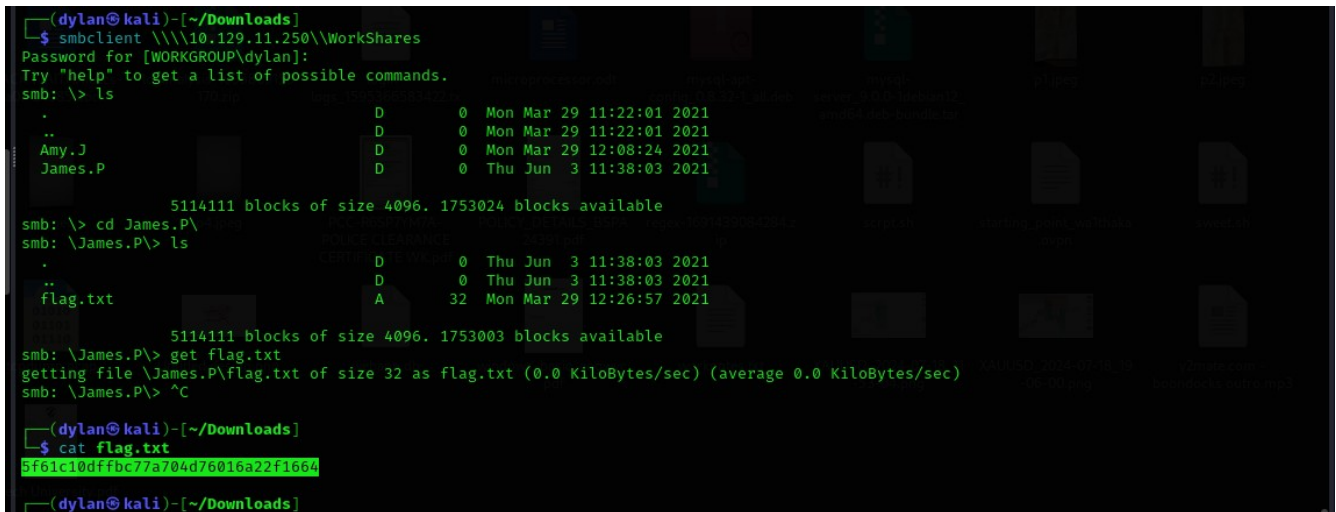
get

Hide Answer

8.



After gaining access I navigated to the James.p directory where I got the flag

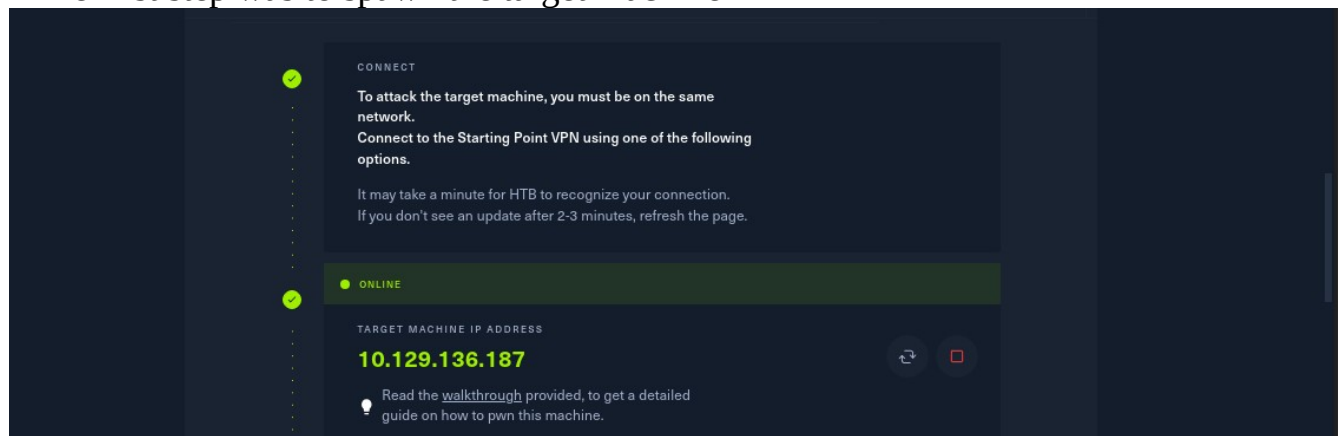


Conclusion

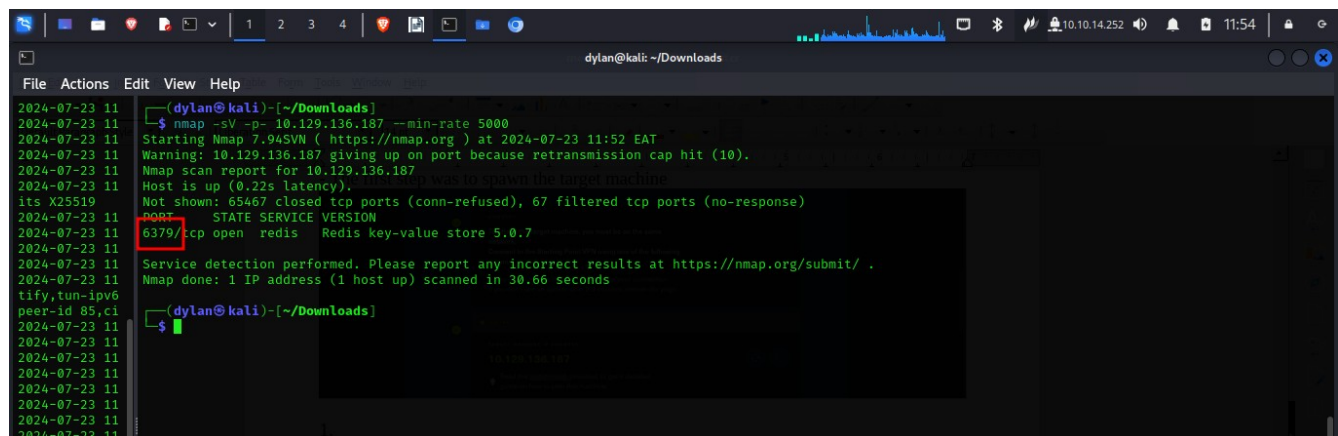
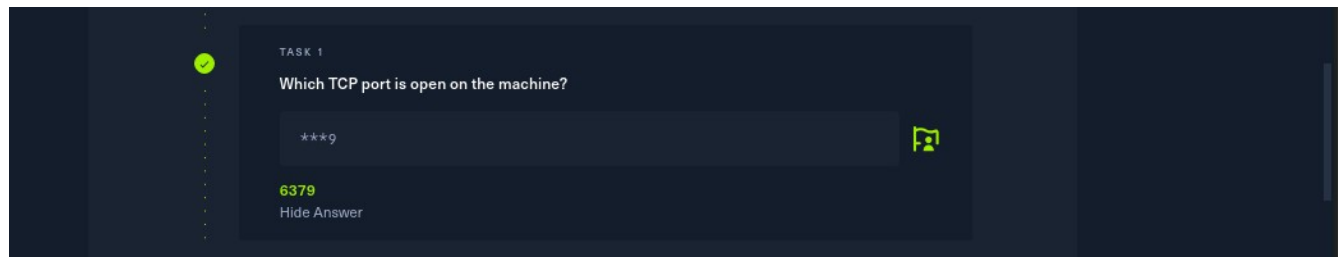
- In this section I learned how to connect and access an smb server

Redeemer

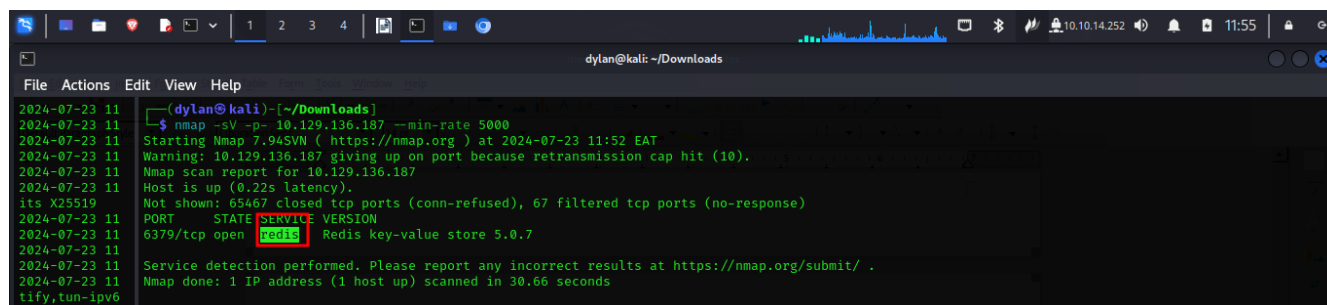
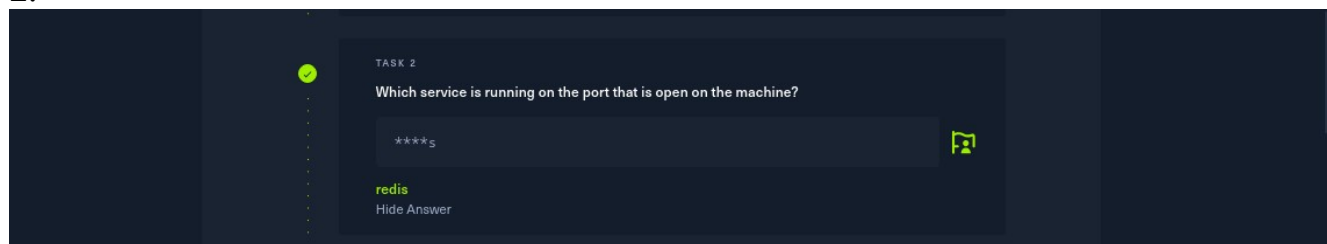
- The first step was to spawn the target machine



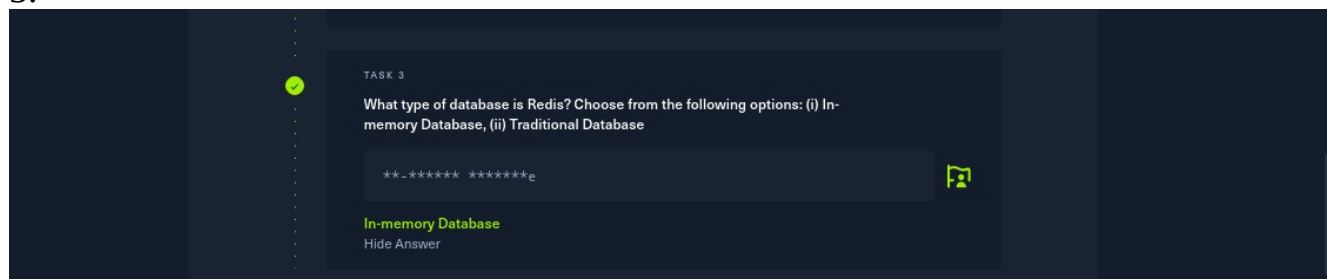
1.



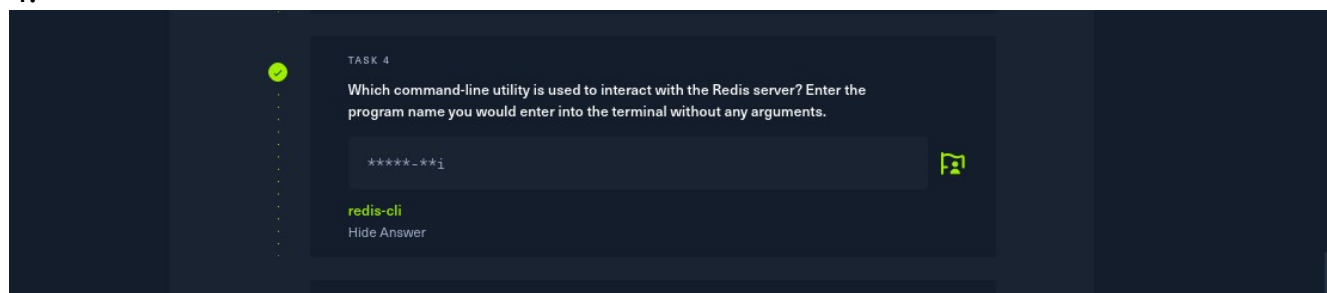
2.



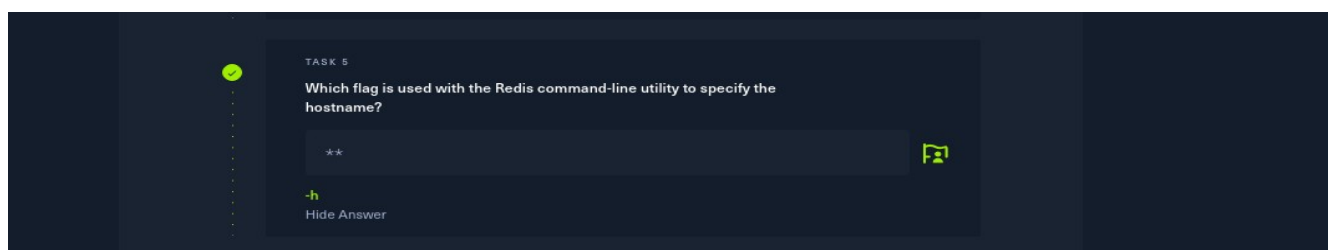
3.



4.



5.



```
(dylan@kali)-[~/Downloads]
$ redis-cli -h
redis-cli 7.0.15

Usage: redis-cli [OPTIONS] [cmd [arg [arg ...]]]
-h <hostname>      Server hostname (default: 127.0.0.1).
-p <port>          Server port (default: 6379).
-s <socket>        Server socket (overrides hostname and port).
-a <password>      Password to use when connecting to the server.
```

6.

✓

TASK 6

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

***o

info

Hide Answer

7.

✓

TASK 7

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

..7

5.0.7

Hide Answer

```
(dylan@kali)-[~/Downloads]
$ nmap -sV -p- 10.129.136.187 --min-rate 5000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 11:52 EAT
Warning: 10.129.136.187 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.136.187
Host is up (0.22s latency).
Not shown: 65467 closed tcp ports (conn-refused), 67 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
6379/tcp  open  redis    Redis key-value store 5.0.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.66 seconds
```

8.

✓

TASK 8

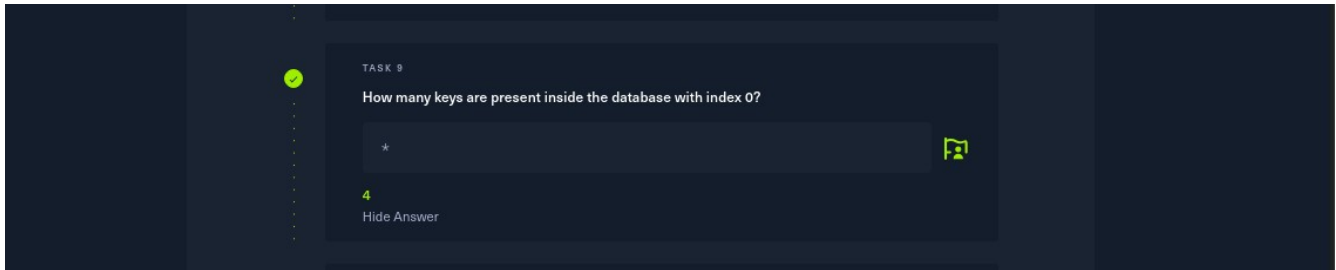
Which command is used to select the desired database in Redis?

*****t

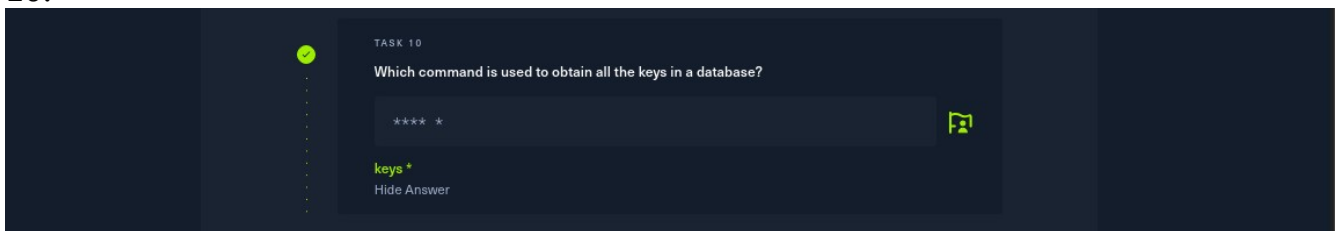
select

Hide Answer

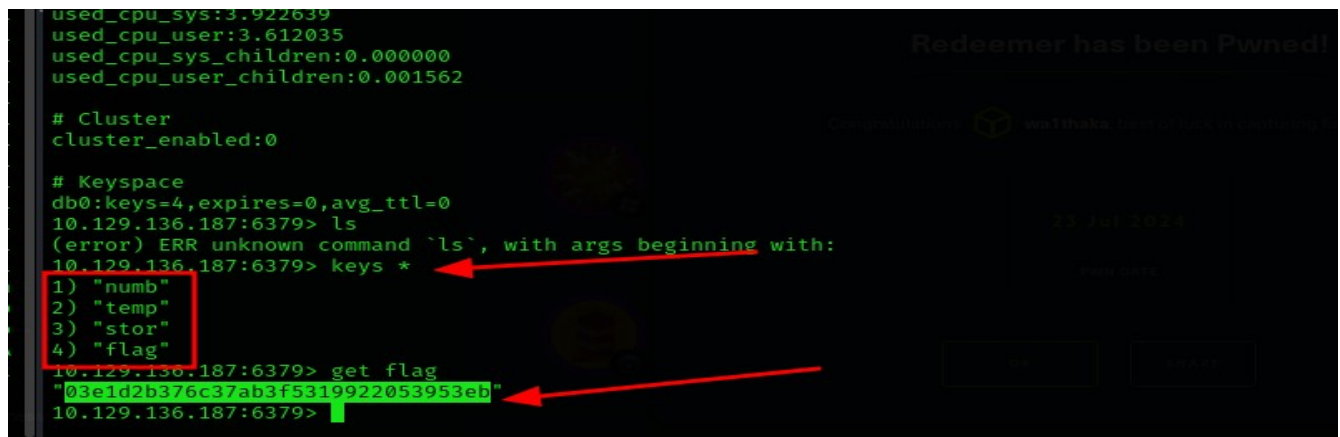
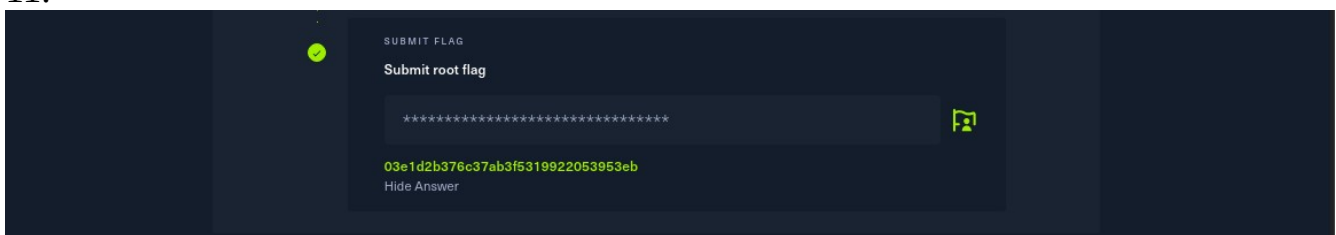
9.

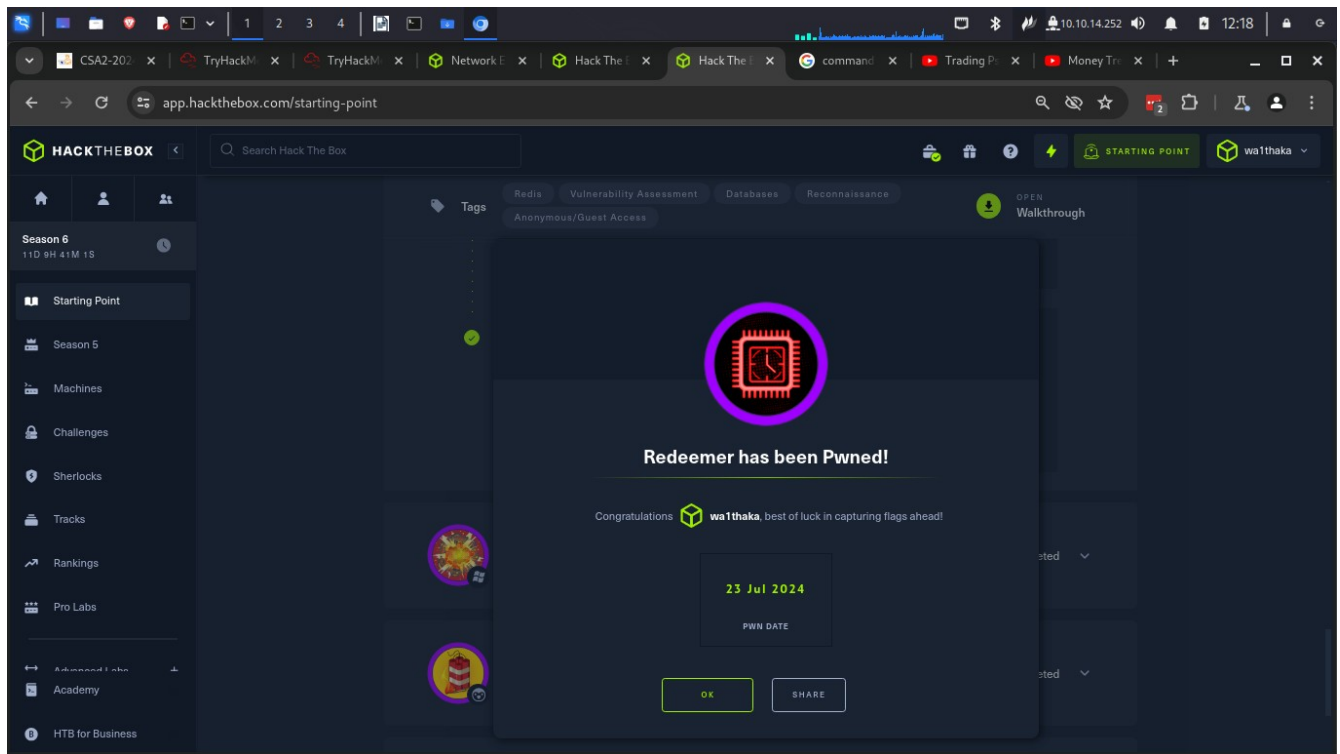


10.



11.





Conclusion

In this section I learnt how to connect and navigate through the redis databases