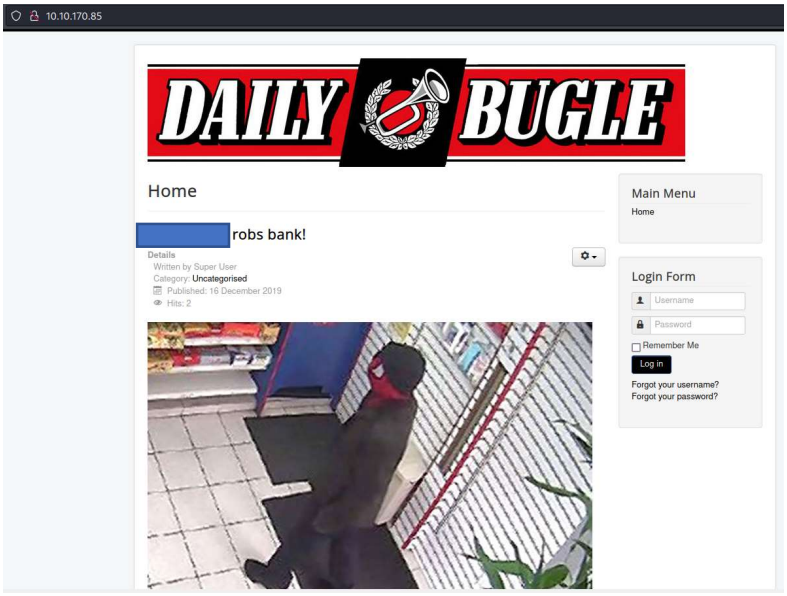
Utilizando la herramienta Nmap realizamos un escaneo de la máquina objetivo para descubrir puertos y servicios abiertos/activos:

```
┌──(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=7.92%E=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)
```

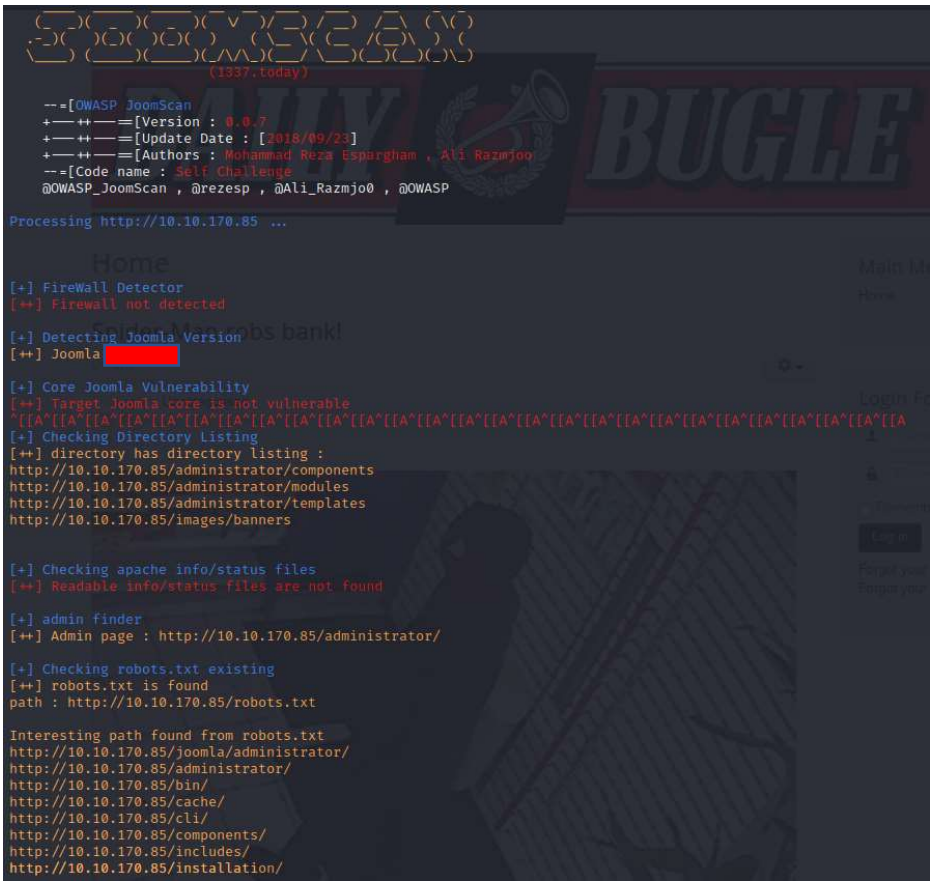
Encontramos lo siguiente:

- 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

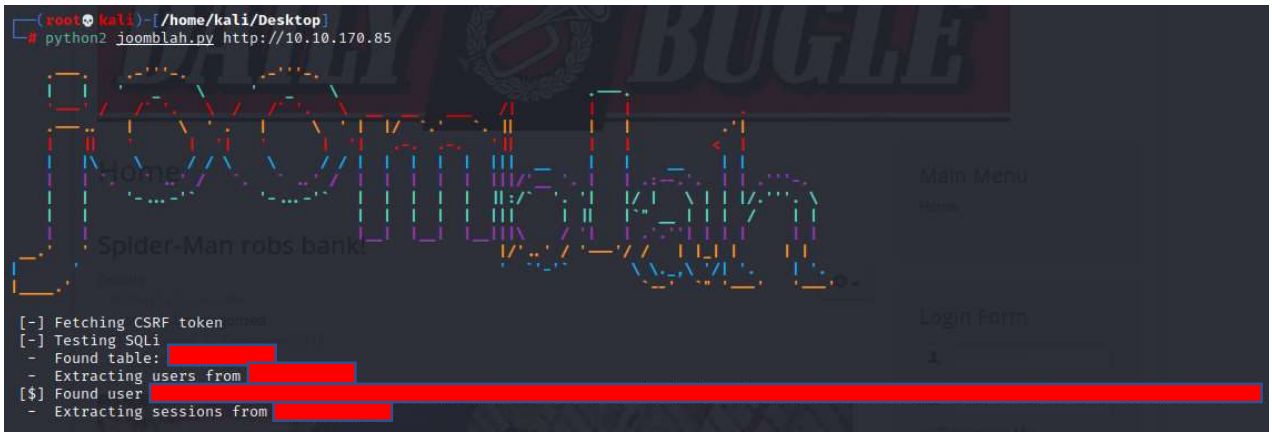
Entrando en la página del Apache en el puerto 80 encontramos una noticia y un formulario de inicio de sesión:



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

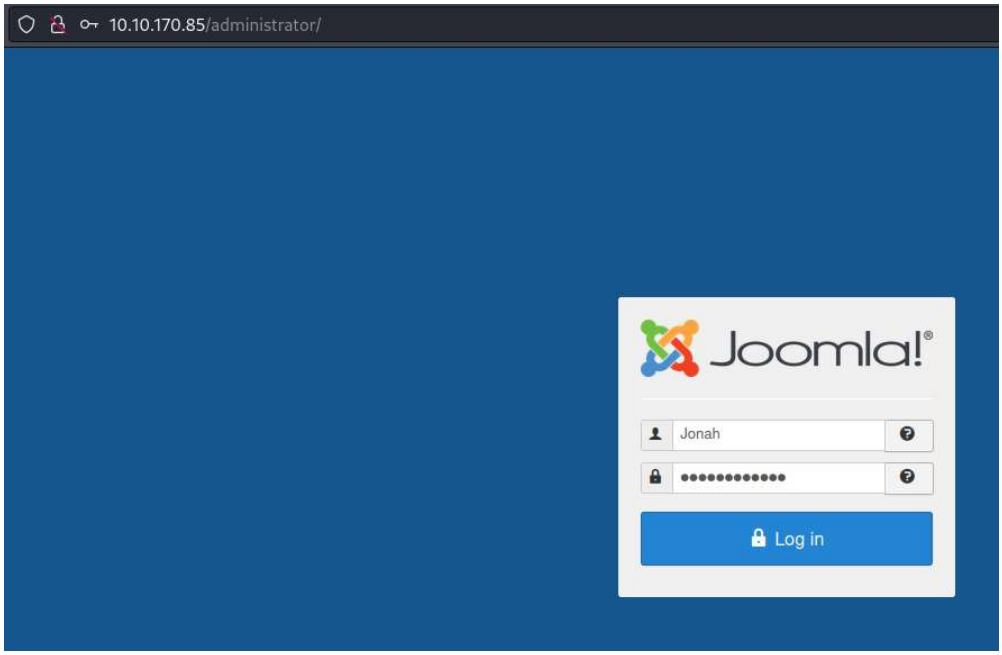


A continuación, utilizando un script escrito en Python llamado joomblah.py podemos sonsacar los usuarios de la base de datos de la máquina objetivo:

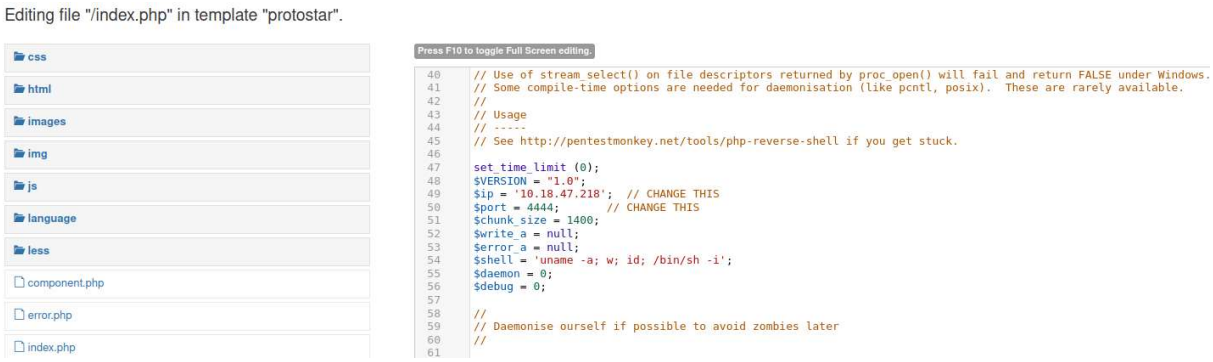


Una vez tenemos los usuarios y la contraseña hasheada solo debemos romperla, para ello utilizaremos John the Ripper con el diccionario rockyou:

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

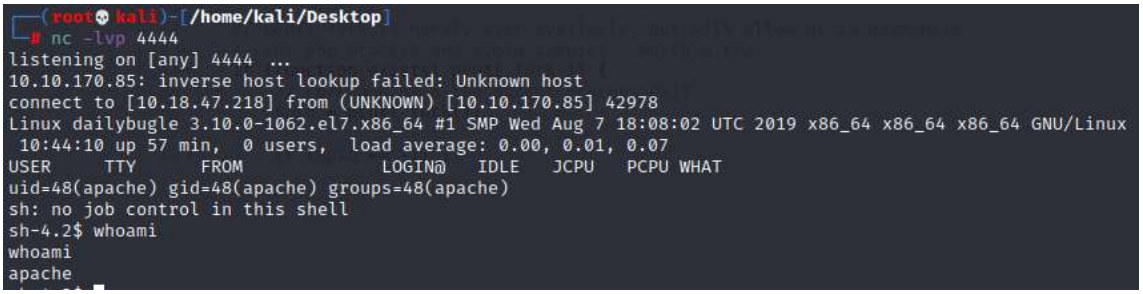


Una vez conectados como administrador y tener control del CMS solo debemos subir una Shell reversa con nuestra IP y un puerto de escucha intercambiando la plantilla del index.php:

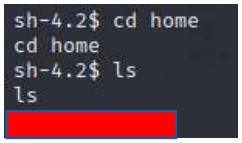


He utilizado la Shell reversa de pentestmonkey*

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



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:

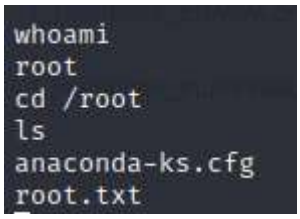


Ahora que sabemos el usuario necesitamos su contraseña, para ello deberemos mirar el archivo de configuración del CMS:

Nos cambiamos de usuario y encontramos la flag de usuario:

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

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



Y ya estaría resuelto el robo!