# Creando payloads con Metasploit

## Introducción

En las sesiones previas pudiste conocer diferentes herramientas que tienen funcionalidades avanzadas, entre ellas destaca Metasploit. Como pudiste observar Metasploit es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está dirigida a auditores de seguridad y equipos Red Team y Blue Team.

Metasploit es muy completa e incluye una diversidad de exploits, es decir, vulnerabilidades conocidas que contienen módulos llamados payloads, códigos que explotan estas vulnerabilidades.

También dispone de otros tipos de módulos, por ejemplo, los encoders, una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

Una de las funcionalidades más atractivas de Metasploit es la posibilidad de crear payloads para diferentes sistemas, dispositivos, lenguajes de programación, entre muchos otros.

En este proyecto crearás payloads para diferentes plataformas, con lo cual establecerás las bases para la creación de tu propio malware.

# ¿Qué debes hacer?

Mediante el uso de Metasploit dentro de Kali Linux, crearás cinco payloads funcionales (*no los ejecutarás*, la idea es que estén armados de tal forma que puedan ser explotados) para las siguientes plataformas:

- **1 payload para Android.**
- **1 payload para Linux.**
- **1 payload para Php.**
- **1 payload para Python.**
- **1 payload para Windows.**

Recuerda que debes hacer uso de los comandos básicos de Metasploit que puedan ser de utilidad para encontrar la información correcta para cada payload, por ejemplo:

- show all.
- search.
- show options.
- help.
- help search.
- history.
- msfvenom.

**Nota:** Es fundamental que *no ejecutes* los payloads que construyas, ya que si lo haces estarías "hackeando" un sistema y, aunque en algún momento de tu carrera lo tendrás que hacer, por el momento solo basta con que sepas crearlos.

### Objetivos

- Crear payloads para diferentes plataformas.
- Documentar y justificar el proceso de búsqueda de los payloads adecuados para cada sistema.
- Compartir los hallazgos mediante un reporte.

## Requisitos y entregables

### Requisitos

- El proyecto debe realizarse de forma individual.
- Crea un reporte y súbelo en una unidad Drive para compartirlo a través de una URL en modo lectura.

**La entrega de este documento es obligatoria, así como todos los elementos que lo conforman.**

### Entregables

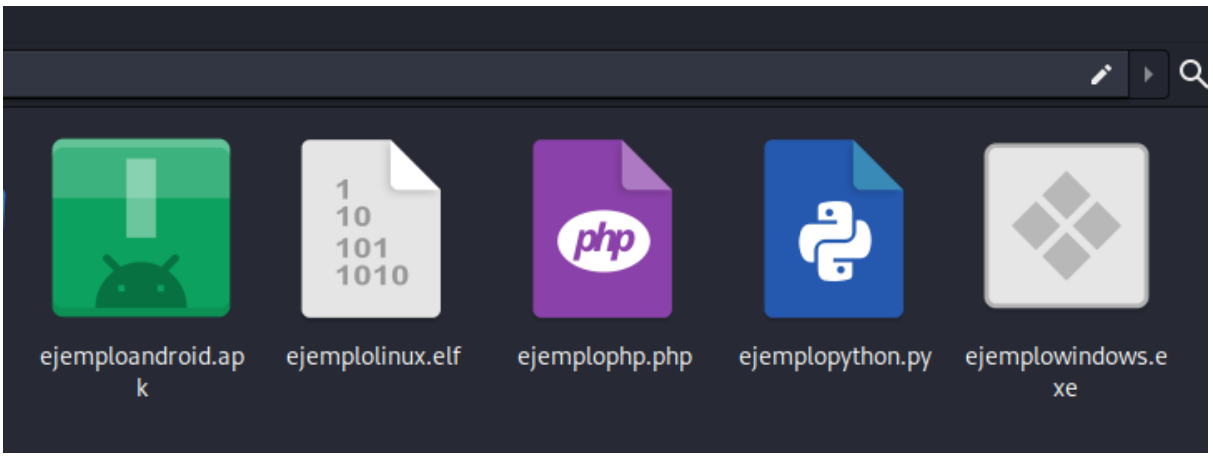
El reporte solicitado deberá elaborarse en un procesador de textos y deberá contener la siguiente información:

Pasos en el uso de Metasploit:

1. Comandos que utilizaste para buscar los payloads.
2. Comandos que utilizaste para crear los payloads.
3. Para qué sirven los payloads que creaste:

a. Es bind (directo): mediante el cual la máquina del hacker se conecta a la de la víctima.
b. Es reverse (inverso): mediante el cual la máquina de la víctima se conecta a la del hacker.
c. Es shellcode: permite ejecutar tareas maliciosas sin ser detenidas por el procesador.
d. Es ejecución de comandos.
e. Es meterpreter: puedes ejecutar código de forma remota, incluso acceder a todas las funciones del sistema. También puedes descargar y subir archivos a la máquina comprometida, tomar capturas de pantalla y fotos desde la webcam.

4. Deberás presentar una captura de pantalla del archivo en donde están guardados los payloads que creaste, tal como aparecen en la siguiente imagen:




Recuerda agregar la metodología y marco teórico que empleaste, esto te permitirá practicar el desarrollo de tus reportes.

## Criterios de evaluación

| Actividad | Puntos | Observaciones |
|---|---|---|
| Creación de payloads | 45 %<br><br>2-1-0 | 2: Creó los 5 payloads.<br>1: Creó de 1 a 3 payloads.<br>0: No creó los payloads. |
| Documentación | 45 % | 2: Entregó el reporte completo con la |

| | | |
|---|---|---|
| | 2-1-0 | descripción de los pasos (1), para qué sirven los payloads que creó (2) y la captura de la imagen del archivo (3).<br>1: El reporte tiene bien una de las acciones requeridas (1, 2 o 3).<br>0: El reporte está incorrecto o incompleto. |
| Entrega a tiempo | 10 %<br><br>2-1-0 | 2: Entregó el documento en la fecha requerida.<br>1: Entregó la URL del documento de proyecto 10 días después de la fecha requerida.<br>0: Entregó la URL del documento de proyecto 11 días después de la fecha requerida o más. |

## Insignia

Seleccionar el grado que corresponde a la insignia, según el logro del proyecto.

| Insignia | Grado | Grado | Puntos |
|---|---|---|---|
| Cyber Security Ethical Hacker (UCSEH) | Intermediate | Principiante | 40 a 79 puntos |
| | | Sobresaliente | 80 a 100 puntos |