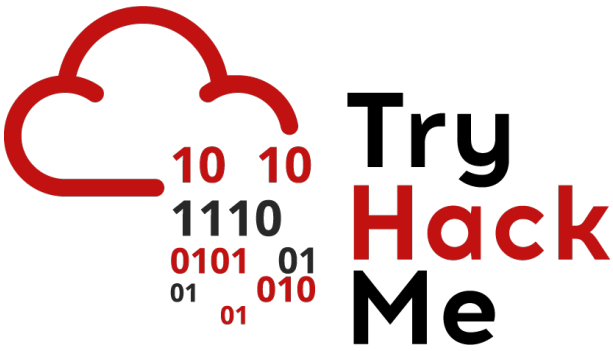
Writeup: Sala *Metasploit: introduction*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

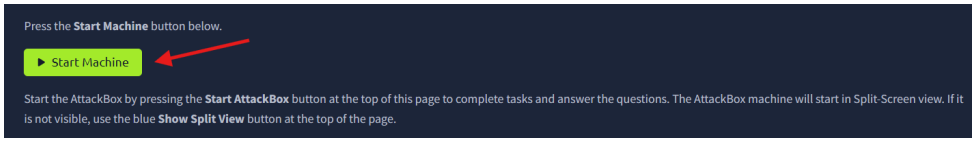
En esta sala conoceremos el uso del **Framework Metasploit**, una de las herramientas más utilizadas en pruebas de penetración. Esta sala explica los fundamentos del framework, sus principales componentes, y cómo utilizar la consola interactiva **msfconsole** para trabajar con diferentes módulos.

2. Sala

2.1. Tarea 1 - Introducción a Metasploit

En esta primera tarea vamos a conocer a **Metasploit** como un framework abierto y muy utilizado en pentesting que permite realizar desde actividades de reconocimiento hasta explotación y post-explotación. Aprenderemos que está compuesto por una interfaz principal (msfconsole), módulos (exploits, payloads, scanners) y herramientas independientes como msfvenom (creación de payloads), pattern_create y pattern_offset.

Antes de continuar, podemos iniciar la máquina objetivo con la cual podremos interactuar a lo largo de la sala para poner en práctica lo aprendido en las diferentes tareas. Para ello, haremos clic en **Start Machine**.



Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Principales componentes de Metasploit

Aprenderemos sobre los principales componentes que contiene Metasploit. Además, algunos conceptos de módulos, cada uno con una función específica dentro del ciclo de ataque.

- **Auxiliary**
- **Encoders**
- **Evasion**
- **Exploits**
- **NOPs**

- **Payloads**
- **Post**

Después de lograr entender los diferentes conceptos, procederemos a responder las siguientes preguntas.

Pregunta: What is the name of the code taking advantage of a flaw on the target system?
Respuesta: **Exploit**

Pregunta: What is the name of the code that runs on the target system to achieve the attacker's goal?
Respuesta: **Payload**

Pregunta: What are self-contained payloads called?
Respuesta: **Singles**

Pregunta: Is windows/x64/pingback_reverse_tcp among singles or staged payload?
Respuesta: **Singles**

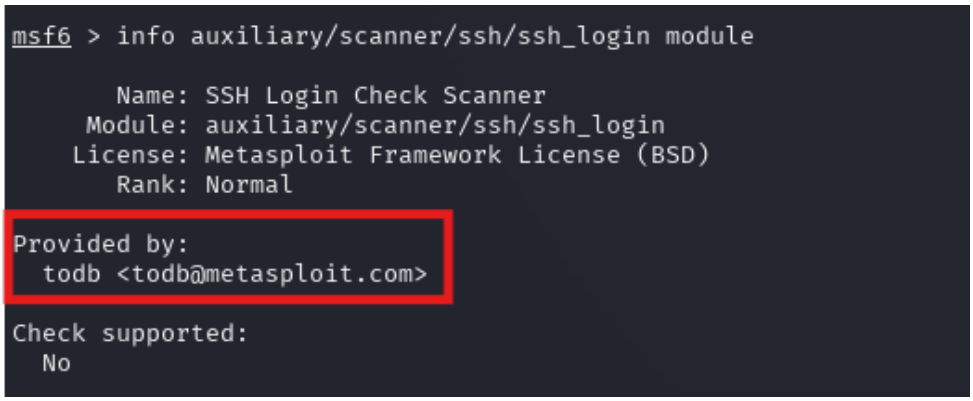
2.3. Tarea 3 - Msfconsole

Ahora, vamos a aprender cómo lanzar Metasploit con **msfconsole**, aprovechando funciones de terminal, uso de comandos básicos (**help**, **use**, **show options**, **info**, **search**, etc.), y la estructura de contexto dentro de msfconsole.

Una vez que comprendemos **msfconsole**, podemos empezar a responder las siguientes preguntas:

Pregunta: How would you search for a module related to Apache?
Respuesta: **search apache**

Pregunta: Who provided the auxiliary/scanner/ssh/ssh_login module? Para encontrar la respuesta a la pregunta, debemos dirigirnos a nuestra terminal e iniciar Metasploit, después, escribiremos el siguiente comando:
info auxiliary/scanner/ssh/ssh_login



Respuesta: todb

2.4. Tarea 4 - Trabajando con módulos

En esta tarea vamos a conocer cómo interactuar con los módulos dentro de Metasploit usando msfconsole, aprenderemos mediante el proceso de:

- **Seleccionar un módulo**
- **Inspeccionar sus opciones**
- **Asignar valores**
- **Verificar el contexto y que los valores esten bien**
- **Ejecutar el módulo**

Ahora que sabemos como trabajar con módulos, pasamos a responder las siguientes preguntas:

Pregunta: How would you set the LPORT value to 6666?
Respuesta: **set LPORT 6666**

Pregunta: How would you set the global value for RHOSTS to 10.10.19.23 ?
Respuesta: **setg RHOSTS 10.10.19.23**

Pregunta: What command would you use to clear a set payload?
Respuesta: **unset PAYLOAD**

Pregunta: What command do you use to proceed with the exploitation phase?
Respuesta: **exploit**

2.5. Tarea 5 - Resumen

En esta última tarea, vamos a reconocer que el uso de Metasploit implica tres fases esenciales:

- **Encontrar un exploit**
- **Personalizarlo con los parámetros adecuados**
- **Ejecutar la explotación contra el servicio vulnerable**

Además, Metasploit acelera estas etapas gracias a sus múltiples módulos y funcionalidades centrales.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

3. Conclusión sobre la Sala

Finalizamos la sala logrando comprender los aspectos fundamentales del funcionamiento de **Metasploit**, incluyendo sus distintos tipos de módulos, la estructura de los payloads y el uso de la consola para gestionar ataques. También, hemos adquirido una base práctica para interactuar con exploits, configurar parámetros y ejecutar módulos en un entorno controlado.