

Metasploit: Introducción

Tarea 1: Introducción a Metasploit

Metasploit es el framework de explotación más utilizado. Es una potente herramienta que soporta todas las fases de una prueba de penetración, desde la recopilación de información hasta la post explotación.

Metasploit tiene dos versiones principales:

- **Metasploit Pro** : La versión comercial que facilita la automatización y gestión de tareas. Esta versión cuenta con una interfaz gráfica de usuario (GUI).
- **Metasploit Framework** : La versión de código abierto que funciona desde la línea de comandos. Esta sesión se centrará en esta versión, instalada en AttackBox y en las distribuciones de Linux más utilizadas para pruebas de penetración .

Metasploit Framework es un conjunto de herramientas que permiten la recopilación de información, el escaneo, la explotación, el desarrollo de exploits, la post explotación y mucho más. Si bien su uso principal se centra en las pruebas de penetración , también es útil para la investigación de vulnerabilidades y el desarrollo de exploits.

Los componentes principales del Framework Metasploit se pueden resumir de la siguiente manera:

- **msfconsole** : La interfaz de línea de comandos principal.
- **Módulos** : módulos de soporte como exploits, escáneres, cargas útiles, etc.
- **Herramientas** : Herramientas independientes que facilitan la investigación y evaluación de vulnerabilidades , o las pruebas de penetración. Algunas de estas herramientas son msfvenom, pattern_create y pattern_offset. En este módulo, abordaremos msfvenom, pero pattern_create y pattern_offset son herramientas útiles para el desarrollo de exploits, lo cual queda fuera del alcance de este módulo.

Esta sala cubrirá los componentes principales de Metasploit y le proporcionará una base sólida para encontrar exploits relevantes, configurar parámetros y explotar servicios vulnerables en el sistema objetivo. Una vez completada esta sala, podrá navegar y usar la línea de comandos de Metasploit con facilidad.

P: No se necesita respuesta

R: No se necesita respuesta

Tarea 2: Componentes principales de Metasploit

P1: ¿Cómo se llama el código que aprovecha una falla en el sistema de destino?

R1: Exploit

P2: ¿Cuál es el nombre del código que se ejecuta en el sistema de destino para lograr el objetivo del atacante?

R2: Payload

P3: ¿Cómo se llaman las cargas útiles autónomas?

R3: Singles

P4: ¿" windows/x64/pingback_reverse_tcp" está entre las cargas útiles individuales o preconfiguradas?

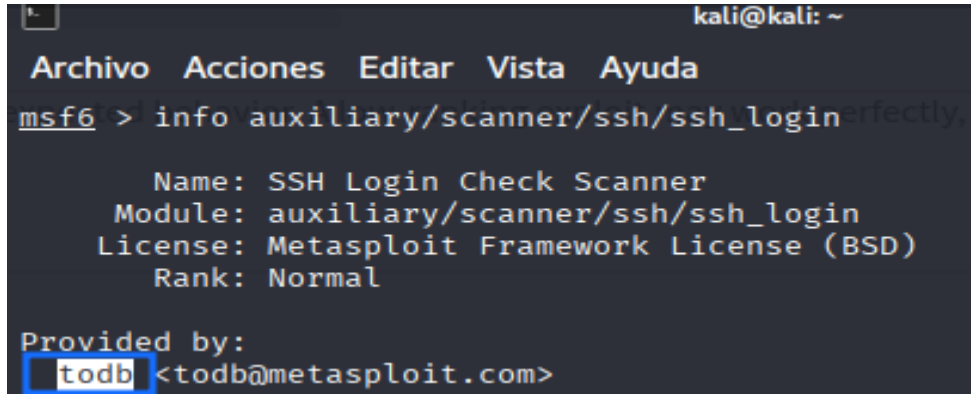
R4: Singles

Tarea 3: Consola Msf

P1: ¿Cómo buscarías un módulo relacionado con Apache?

R1: Search Apache / Buscar Apache

P2: ¿Quién proporcionó el módulo auxiliar/scanner/ssh/ssh_login?



```
kali@kali: ~  
Archivo Acciones Editar Vista Ayuda  
msf6 > info auxiliary/scanner/ssh/ssh_login  
  
Name: SSH Login Check Scanner  
Module: auxiliary/scanner/ssh/ssh_login  
License: Metasploit Framework License (BSD)  
Rank: Normal  
  
Provided by:  
todb <todb@metasploit.com>
```

R2: todb

Tarea 4: Trabajar con módulos

P1: ¿Cómo establecerías el valor LPORT en 6666?

R1: Set LPORT 6666

P2: ¿Cómo establecerías el valor global de RHOSTS en 10.10.19.23?

R2: Setg RHOSTS 10.10.19.23

P3: ¿Qué comando usarías para borrar una carga útil establecida?

R3: unset PAYLOAD

P4: ¿Qué comando utilizas para proceder con la fase de explotación?

R4: Exploit

Tarea 5: Resumen

Como hemos visto hasta ahora, Metasploit es una herramienta potente que facilita el proceso de explotación. Este proceso consta de tres pasos principales: encontrar el exploit, personalizarlo y explotar el servicio vulnerable.

Metasploit ofrece numerosos módulos que puedes usar en cada paso del proceso de explotación. En esta sala, hemos visto los componentes básicos de Metasploit y su respectivo uso.

Sería mejor si también hubieras utilizado el exploit **ms17_010_eternalblue** para obtener acceso a la VM de destino .

En las siguientes salas, abordaremos Metasploit y sus componentes con más detalle. Al completar este módulo, comprenderá a fondo las capacidades de Metasploit .

P: No se necesita respuesta

R: No se necesita respuesta

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>