

MANUAL DE INSTALACIÓN DE METASPLOITABLE 3

Autor: ROSA ELVIRA MONTH CORDOBA

Asignatura: Seguridad Informática y auditoria de redes

Docente: Rafael Sandoval Morales

Fecha: 02 de septiembre de 2025

Introducción

En este manual voy a explicar paso a paso cómo instalar **Metasploitable 3**, una máquina virtual creada que está diseñada con múltiples vulnerabilidades para que podamos practicar **pruebas de penetración (pentesting)** y aprender a usar **Metasploit Framework**.

La diferencia principal con **Metasploitable 2** es que la versión 3 **no viene lista para descargar como una imagen ISO**. En lugar de eso, nosotros debemos **construir la máquina desde cero** usando herramientas como **Vagrant**, **VirtualBox** y **Git**. Esto puede parecer complicado, pero siguiendo este manual podrás instalarla correctamente.

1. Requisitos Previos

Antes de empezar, debemos asegurarnos de que nuestro equipo cumple con las especificaciones necesarias y de tener instaladas las herramientas correctas.

Requisitos de hardware

- Procesador: **Mínimo 2 núcleos** (recomendado 4).
- Memoria RAM: **Mínimo 4 GB** (ideal 8 GB si usas varias máquinas).
- Disco duro: **Al menos 60 GB libres**.
- Virtualización: Debe estar habilitada en la **BIOS** (opciones **Intel VT-x** o **AMD-V**).

Requisitos de software

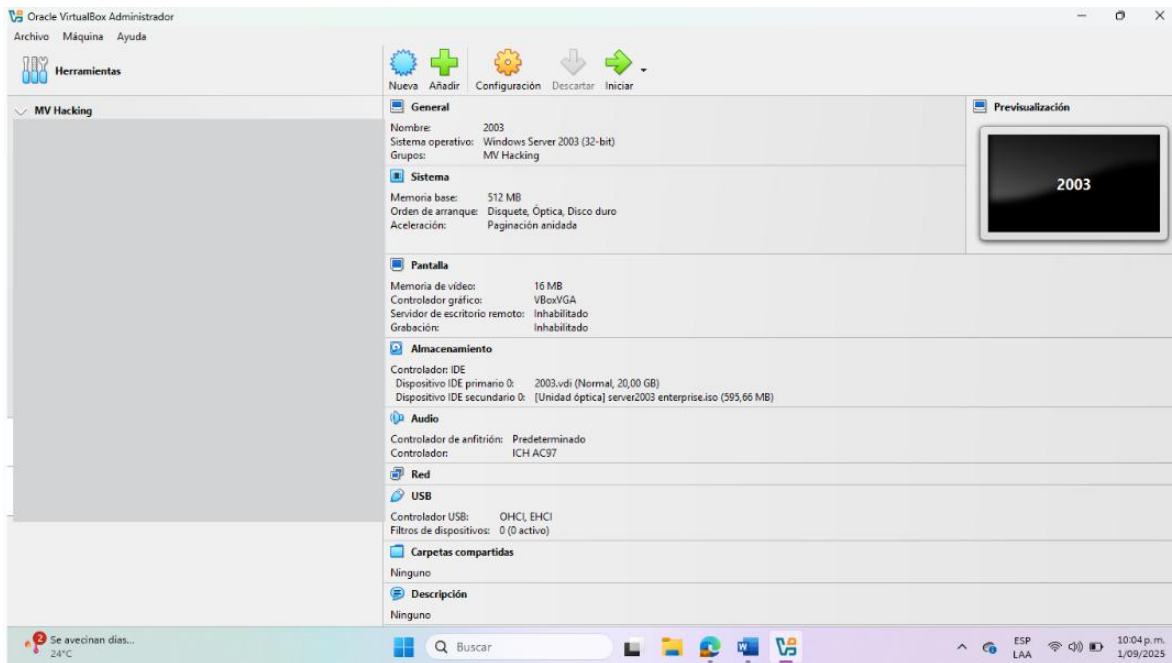
- **VirtualBox** → Para crear y administrar la máquina virtual.
- **Vagrant** → Para automatizar la construcción de la máquina.
- **Git** → Para descargar los archivos de instalación.
- **PowerShell** (en Windows) o **Terminal** (en Linux o Mac).

2. Instalación de Herramientas Necesarias

Para instalar Metasploitable 3, primero necesitamos configurar el entorno de trabajo.

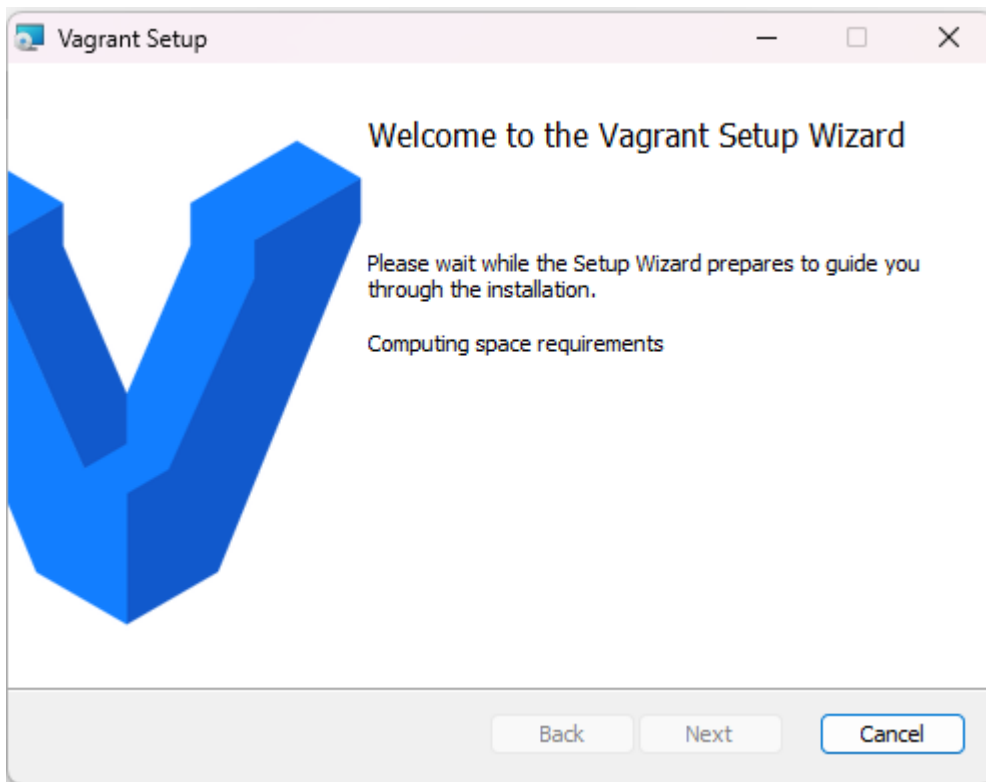
Instalar VirtualBox

1. Descargamos VirtualBox desde la página oficial:
<https://www.virtualbox.org/wiki/Downloads>
2. Ejecutamos el instalador y dejamos las opciones por defecto.
3. Al finalizar, abrimos VirtualBox para confirmar que se instaló correctamente.



Instalar Vagrant

1. Descargamos Vagrant desde:
<https://developer.hashicorp.com/vagrant/downloads>
2. Instalamos con las configuraciones predeterminadas.
3. Verificamos que se haya instalado ejecutando en la terminal:
4. `vagrant -v`



```
C:\WINDOWS\system32\cmd. X + v
Microsoft Windows [Versión 10.0.26100.4946]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Ingro>vagrant -v
Vagrant 2.4.9

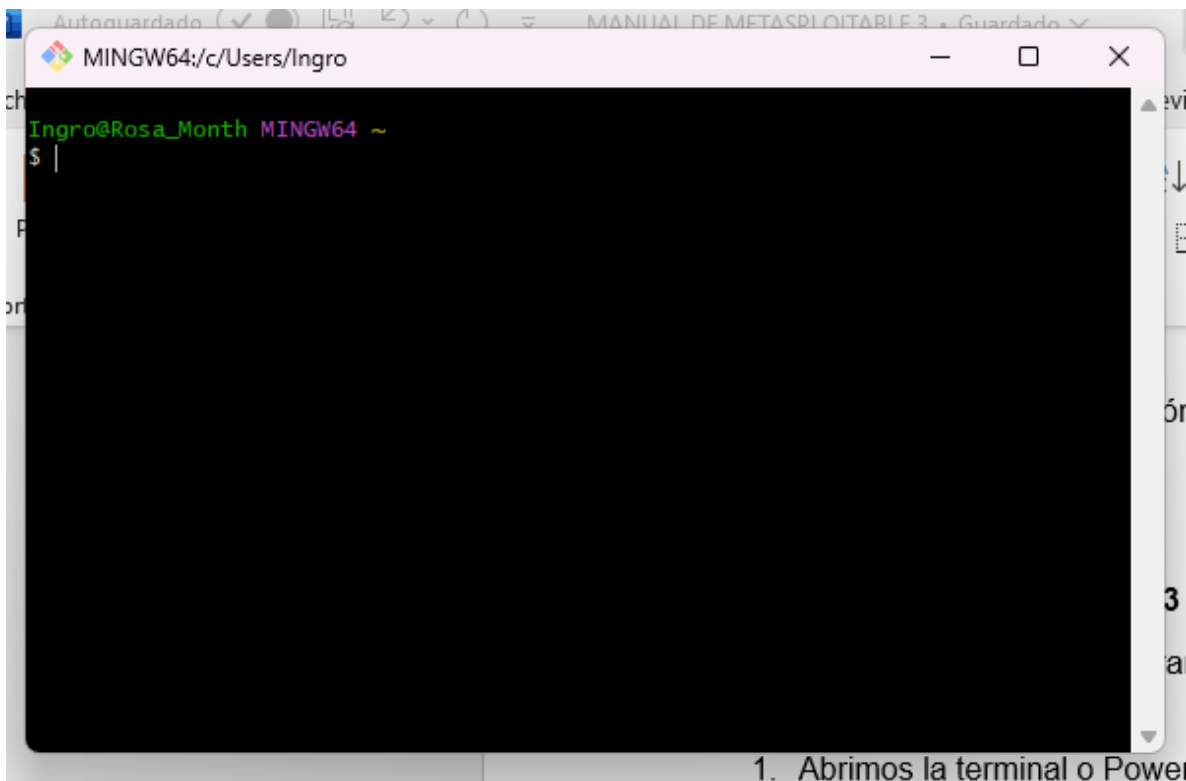
C:\Users\Ingro>
```

Si aparece un número de versión, significa que está funcionando.

Instalar Git

1. Descargamos Git desde:
<https://git-scm.com/downloads>
2. Lo instalamos aceptando la configuración predeterminada.

3. Para confirmar la instalación:
4. `git --version`



1. Abrimos la terminal o Power

3. Descarga de Metasploitable 3

Una vez tengamos todas las herramientas instaladas, descargamos los archivos necesarios desde GitHub.

1. Abrimos la terminal o PowerShell.
2. Ejecutamos:
3. `git clone https://github.com/rapid7/metasploitable3.git`
4. Entramos a la carpeta descargada:
5. `cd metasploitable3`

Explicación: Aquí obtenemos todos los scripts y configuraciones que permiten a Vagrant crear la máquina Metasploitable 3 desde cero.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\Ingro> git clone https://github.com/rapid7/metasploitable3.git
Cloning into 'metasploitable3'...
remote: Enumerating objects: 4985, done.
remote: Counting objects: 100% (79/79), done.
remote: Compressing objects: 100% (31/31), done
Receiving objects: 7% (349/4985), 140.01 KiB |
Receiving objects: 8% (399/4985), 140.01 KiB |
Receiving objects: 9% (449/4985), 140.01 KiB |
Receiving objects: 10% (499/4985), 140.01 KiB |
Receiving objects: 11% (549/4985), 140.01 KiB |
Receiving objects: 11% (571/4985), 140.01 KiB |
Receiving objects: 12% (599/4985), 140.01 KiB |
Receiving objects: 13% (649/4985), 140.01 KiB |
Receiving objects: 14% (698/4985), 140.01 KiB |
Receiving objects: 15% (748/4985), 140.01 KiB |
Receiving objects: 16% (798/4985), 356.01 KiB |
Receiving objects: 17% (848/4985), 356.01 KiB |
Receiving objects: 18% (898/4985), 356.01 KiB |
Receiving objects: 19% (948/4985), 356.01 KiB |
Receiving objects: 20% (997/4985), 356.01 KiB |
| 284.00 KiB/s
| 4.96 MiB/s, done.
Resolving deltas: 100% (2473/2473), done.
Updating files: 100% (502/502), done.
PS C:\Users\Ingro> cd metasploitable3
PS C:\Users\Ingro\metasploitable3> |
```

4. Construcción de la Máquina Virtual

Con todo listo, ahora vamos a **crear** la máquina vulnerable.

1. Dentro de la carpeta metasploitable3, ejecutamos:

2. vagrant up
3. Este comando hace todo el trabajo:
 - Descarga la imagen base del sistema operativo.
 - Instala los programas vulnerables.
 - Configura la red y los recursos.
4. Este proceso puede tardar **entre 30 y 90 minutos** dependiendo de la velocidad de tu internet y tu computadora.

```
PS C:\Users\Ingro> cd metasploitable3
PS C:\Users\Ingro\metasploitable3> vagrant up
```

Consejo:

Si durante la instalación te sale un error, usa:

vagrant destroy

vagrant up --provision

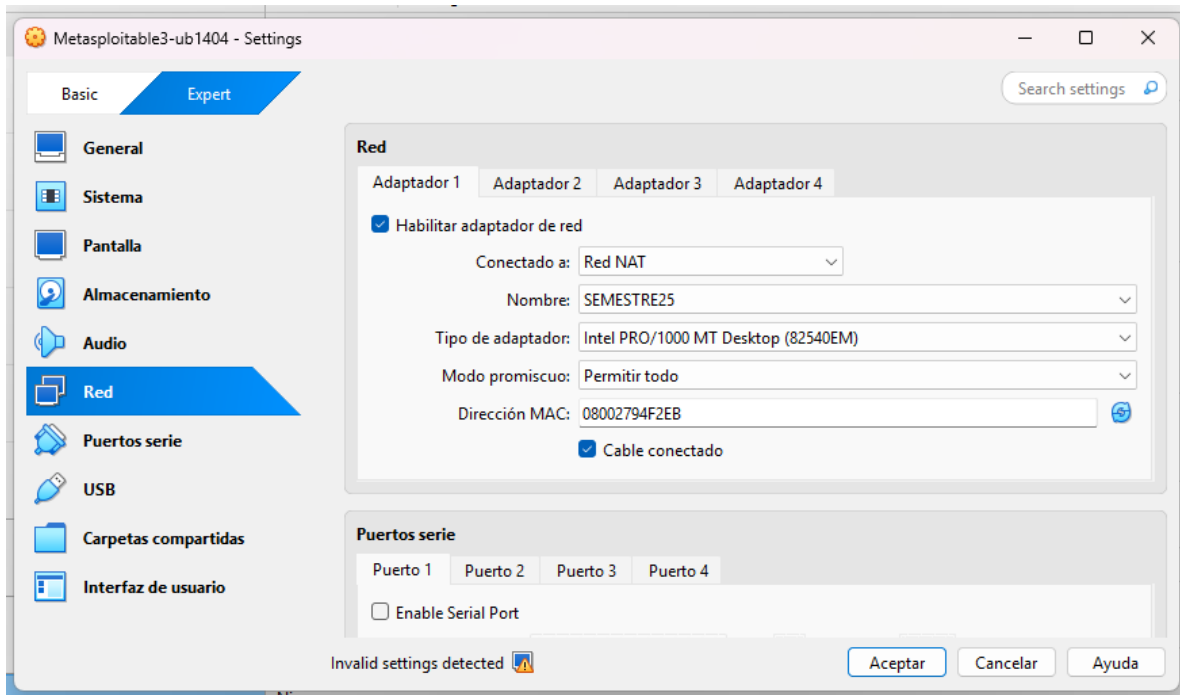
Esto reinicia la construcción desde cero.

5. Configuración de Red

Para que podamos acceder a la máquina Metasploitable 3 desde otras máquinas virtuales (por ejemplo, Kali Linux), debemos configurar su red.

Modo recomendado: Host-Only Adapter

1. Abrimos **VirtualBox**.
2. Seleccionamos la máquina metasploitable3.
3. Vamos a **Configuración** → **Red**.
4. En el **Adaptador 2**, elegimos **Adaptador solo-anfitrión**.
5. Esto nos permitirá conectarnos a Metasploitable 3 desde nuestra máquina física o desde otras VMs.



6. Acceso a Metasploitable 3

Después de construir la máquina, podemos acceder de dos formas:

Opción 1: Acceso por SSH

`vagrant ssh`

Con esto entramos directamente al sistema.

```
PS C:\Users\Ingro\metasploitable3>
PS C:\Users\Ingro\metasploitable3> vagrant ssh
This command requires a specific VM name to target in a multi-VM environment.
PS C:\Users\Ingro\metasploitable3>
```

Opción 2: Acceso por VirtualBox

- Abrimos **VirtualBox**.
- Seleccionamos la máquina **Metasploitable 3**.
- Usuario por defecto:
- `vagrant`
- Contraseña por defecto:
- `Vagrant`

```
Ubuntu 14.04 LTS ubuntu tty1
ubuntu login: vagrant
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vagrant@ubuntu:~$
```

7. Verificación de Instalación

Para asegurarnos de que todo funciona correctamente:

1. Obtenemos la dirección IP de Metasploitable 3:
2. ip addr

```

metasploitable3-ub1404_1756833137535_25139 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:42:51:79 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:2:8991:b368:e1fd:f7/64 scope global temporary dynamic
        valid_lft 86301sec preferred_lft 14301sec
    inet6 fd17:625c:f037:2:a00:27ff:fe42:5179/64 scope global dynamic
        valid_lft 86301sec preferred_lft 14301sec
    inet6 fe80::a00:27ff:fe42:5179/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gr
oup default
    link/ether 02:42:4e:49:c5:bb brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:4eff:fe49:c5bb/64 scope link
        valid_lft forever preferred_lft forever
5: veth40c1394: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master
docker0 state UP group default
    link/ether 02:ca:84:ac:3b:70 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::ca:84ff:feac:3b70/64 scope link
        valid_lft forever preferred_lft forever
vagrant@ubuntu:~$

```

3. Desde nuestra máquina anfitriona, hacemos un escaneo rápido con Nmap:
4. `nmap -sV <IP_Metasploitable3>`
5. Si vemos muchos puertos abiertos, la instalación fue exitosa.

```

Setting up nmap (6.40-0.2ubuntu1) ...
Processing triggers for libc-bin (2.19-0ubuntu6) ...
vagrant@ubuntu:~$ nmap -sV 10.10.10.9

Starting Nmap 6.40 ( http://nmap.org ) at 2025-09-02 17:25 UTC
Nmap scan report for ubuntu (10.10.10.9)
Host is up (0.00039s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: UBUNTU)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: UBUNTU)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          Unreal ircd
8080/tcp  open  http         Jetty 8.1.7.v20120910
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=9/2%Time=68B72890%P=x86_64-pc-linux-gnu%r(NULL,
SF:2C,"SSH-2\0-OpenSSH_6\6\1p1\0Ubuntu-2ubuntu2\13\r\n");
Service Info: Host: irc.TestIRC.net; OS: Unix

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
vagrant@ubuntu:~$

```

8. Problemas Comunes y Soluciones

Problema	Causa	Solución
Error en vagrant up	Falta de dependencias	Actualiza Vagrant y VirtualBox
No hay conexión de red	Configuración incorrecta	Cambia a Host-Only Adapter
Máquina lenta	Pocos recursos	Asigna más CPU y RAM
Error al descargar archivos	Internet lento	Usa una VPN o cambia de red

Conclusión

Como estudiante, mi experiencia instalando **Metasploitable 3** fue un reto al principio, ya que requiere varias herramientas y configuraciones. Sin embargo, siguiendo estos pasos logré crear mi laboratorio de pruebas para practicar **pentesting** y **explotación de vulnerabilidades** de forma segura.

Ahora puedo usar Metasploitable 3 junto con **Kali Linux** y otras máquinas para simular ataques reales y aprender cómo proteger sistemas.

