

MANUAL DE INSTALACION DE METASPLOITABLE3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

MANUAL DE INSTALACION DE METASPLOITABLE3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

Objetivo general	6
Requisitos Previos	7
Paso 1: Clonar el repositorio oficial.....	7
Instalación de las maquinas a utilizar... ..	8
Instalación de los paquetes en virtualbox desde power Shell	8
Creación automáticamente	9
Imágenes de las maquinas corriendo al 100%	10
Conclusiones	12
Bibliografía	12
Morcor.....	12
Webgrafía	12

LISTA DE ILUSTRACIONES

Ilustración 1 creacion de la carpeta de metasploitable.....	7
Ilustración 2 accediendo a la carpeta de metasploitable3-workspace	8
Ilustración 3 Instalación de los paquetes.....	8
Ilustración 4 creación de las maquinas	9
Ilustración 5 metasploitable3-workspace_win2k8_1756799443609_27877.....	10
Ilustración 6 Metasploitable3-ub1404	11

Informe del Laboratorio #2 Manual de instalación de Metasploitable 3

Este informe presenta una guía detallada para la instalación de Metasploitable 3 en un entorno Windows, utilizando herramientas como VirtualBox, Vagrant, Packer y Git. El objetivo es documentar cada paso del proceso, desde la preparación del entorno hasta la construcción de la máquina virtual, asegurando que el lector pueda replicar la instalación de forma autónoma y confiable.

La implementación de este entorno vulnerable no solo facilita la exploración de técnicas ofensivas y defensivas en seguridad informática, sino que también promueve el desarrollo de habilidades críticas en análisis de servicios, detección de vulnerabilidades y aplicación de medidas de mitigación. En el marco del laboratorio académico, esta práctica se alinea con los objetivos formativos del programa de Ingeniería en Telecomunicaciones e Informática, fortaleciendo el dominio técnico en entornos controlados y éticamente responsables.

Objetivo general

Documentar el proceso de instalación de la máquina virtual vulnerable **Metasploitable 3** en un entorno Windows, con fines educativos y de práctica en hacking ético.

Requisitos Previos

Antes de iniciar el proceso, se deben instalar las siguientes herramientas:

Herramienta	Descripción	Enlace de descarga
VirtualBox	Plataforma de virtualización	virtualbox.org
Vagrant	Automatización de entornos virtuales	vagrantup.com
Packer	Generador de imágenes de máquina	packer.io
Git (<i>opcional pero recomendado</i>)	Control de versiones y clonación de repositorios	git-scm.com

Paso 1: Clonar el repositorio oficial

Abrir PowerShell o terminal y ejecutar: `mkdir metasploitable3-workspace` este comando nos crea una carpeta...

```
C:\Windows\System32>cd
C:\Windows\System32

C:\Windows\System32>cd..

C:\Windows>cd..

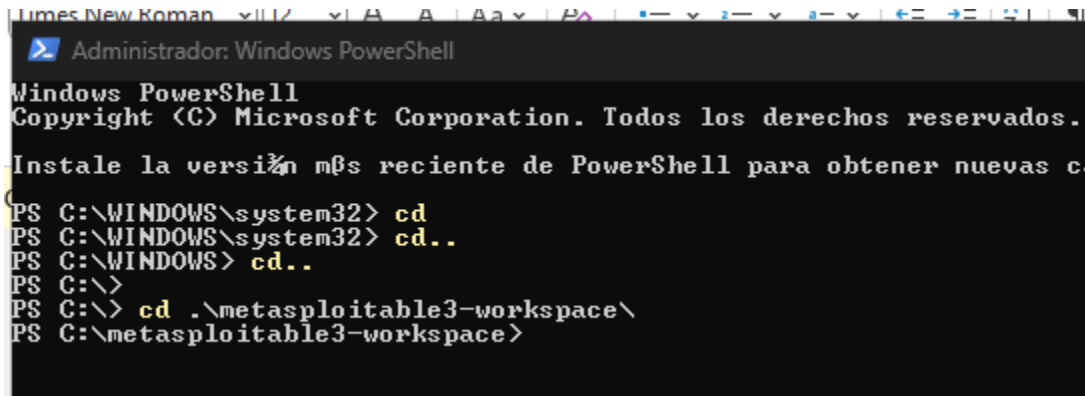
C:\>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\>mkdir metasploitable3-workspace
```

Ilustración 1 creacion de la carpeta de metasploitable

Instalación de las maquinas a utilizar...

Luego ejecutamos Power Shell (en modo administrador), ya que esta nos permite instalar de manera correcta las dependencias y los programas a utilizar...



```

Administrator: Windows PowerShell

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

Instale la versión más reciente de PowerShell para obtener nuevas características.
(Ejecute el comando 'Get-Command -Syntax' para obtener más información.)

PS C:\WINDOWS\system32> cd
PS C:\WINDOWS\system32> cd..
PS C:\WINDOWS> cd..
PS C:\>
PS C:\> cd .\metasploitable3-workspace\
PS C:\metasploitable3-workspace>
  
```

Aquí copiamos los siguientes comandos:

`Invoke-WebRequest -Uri`

`"https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"`

Y con este último: `vagrant up` es que nos instalara todo metasploitable3 y las demás maquinas que necesitamos



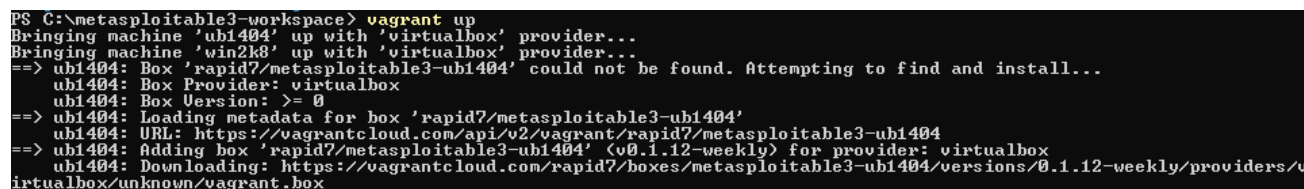
```

PS C:\> cd .\metasploitable3-workspace\
PS C:\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\metasploitable3-workspace> vagrant up
  
```

Ilustración 2 accediendo a la carpeta de metasploitable3-workspace

Instalación de los paquetes en virtualbox desde power Shell

Eso demora bastante, aun apenas están descargando los paquetes, una vez descargados adjuntare imágenes y pruebas de ellas

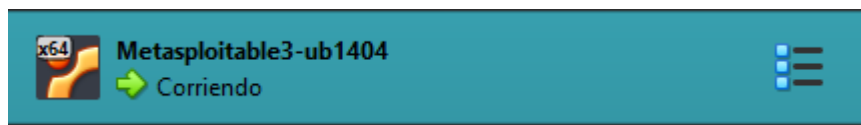


```

PS C:\metasploitable3-workspace> vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Box 'rapid7/metasploitable3-ub1404' could not be found. Attempting to find and install...
ub1404: Box Provider: virtualbox
ub1404: Box Version: >= 0
==> ub1404: Loading metadata for box 'rapid7/metasploitable3-ub1404'
ub1404: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-ub1404
==> ub1404: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
ub1404: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekly/providers/virtualbox/unknown/vagrant.box
  
```

Ilustración 3 Instalación de los paquetes

Creación automática



```
win2k8>
==> win2k8: Successfully added box 'rapid7/metasploitable3-win2k8' <v0.1.0-weekly> for 'virtualbox'!
==> win2k8: Importing base box 'rapid7/metasploitable3-win2k8'...
Progress: 20%
```

Ilustración 4 creación de las maquinas

Aquí lo que podemos observar es como automáticamente metasploitable3 se va creando por medio de la power Shell

Imágenes de las maquinas corriendo al 100%

1) metasploitable3-workspace_win2k8_1756799443609_27877

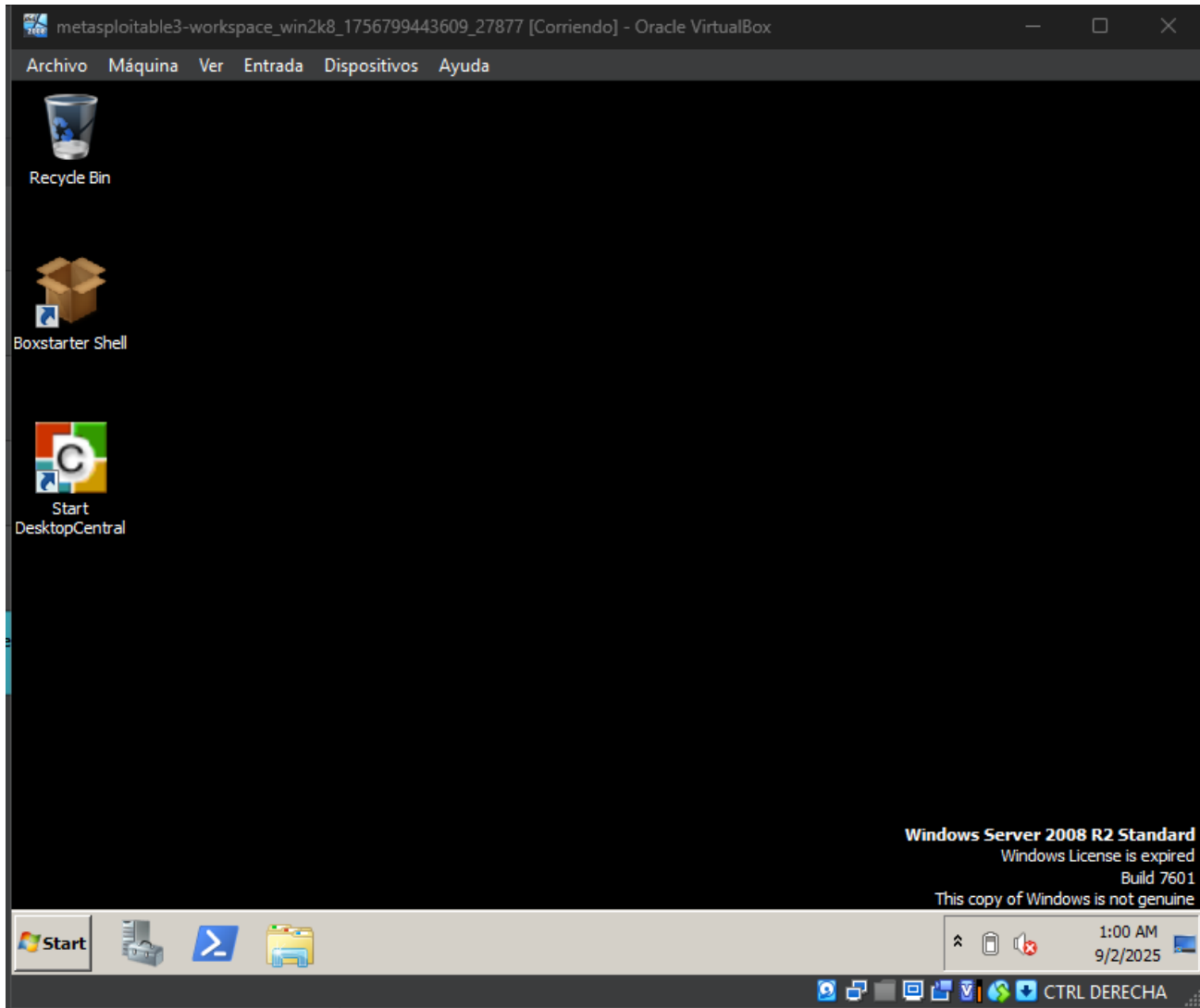


Ilustración 5 metasploitable3-workspace_win2k8_1756799443609_27877

2) Metasploitable3-ub1404

```

Metasploitable3-ub1404 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

collisions:0 txqueuelen:1000
RX bytes:6471708 (6.4 MB)  TX bytes:43567 (43.5 KB)

eth1  Link encap:Ethernet  HWaddr 08:00:27:15:6a:e7
      inet addr:172.28.128.3  Bcast:172.28.128.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe15:6ae7/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:56 errors:0 dropped:0 overruns:0 frame:0
      TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:11269 (11.2 KB)  TX bytes:11452 (11.4 KB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:65536  Metric:1
      RX packets:494 errors:0 dropped:0 overruns:0 frame:0
      TX packets:494 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:176204 (176.2 KB)  TX bytes:176204 (176.2 KB)

veth62b6a4c Link encap:Ethernet  HWaddr ba:19:69:22:b3:77
          inet6 addr: fe80::b819:69ff:fe22:b377/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:13777 (13.7 KB)

vagrant@metasploitable3-ub1404:~$ _

```

Ilustración 6 Metasploitable3-ub1404

Conclusiones

La instalación de Metasploitable3 en Windows requiere una preparación cuidadosa del entorno y ajustes técnicos precisos. A pesar de los errores iniciales, se logró identificar y corregir los conflictos de versión y rutas, permitiendo avanzar con éxito en la construcción de la máquina virtual

Bibliografía

Morcor

Webgrafía

Metasploitable3 [GitHub - rapid7/metasploitable3](https://github.com/rapid7/metasploitable3): Metasploitable3 is a VM that is built from the ground up with a large amount of security vulnerabilities.

Ia.

<https://chatgpt.com/>