



INFORME 1

Juan Carlos Palacios Valencia

Manual de Metasploitable 3

Rafael Sandoval Morales

Docente

UNIVERSIDAD TECNOLÓGICA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTA DE INGENIERÍA

TELECOMUNICACIONES E INFORMÁTICA

SEMESTRE VIII

QUIBDÒ – CHOCÒ

AÑO 2025



Contenido

INTRODUCION	2
DESARROLLO (bits, 2023)	3
Paso 1 Descargar Vagrant (hashicorp, 2022)	3
Paso 2 Instalación de vagrant.....	3
Paso 3 instalación de Metasploitable 3 (Simonirwin-r7, 2016)	5
Paso 4 Configuración de red en Metasploitable 3	8
CONCLUSION.....	10
Bibliografía	10

INTRODUCION

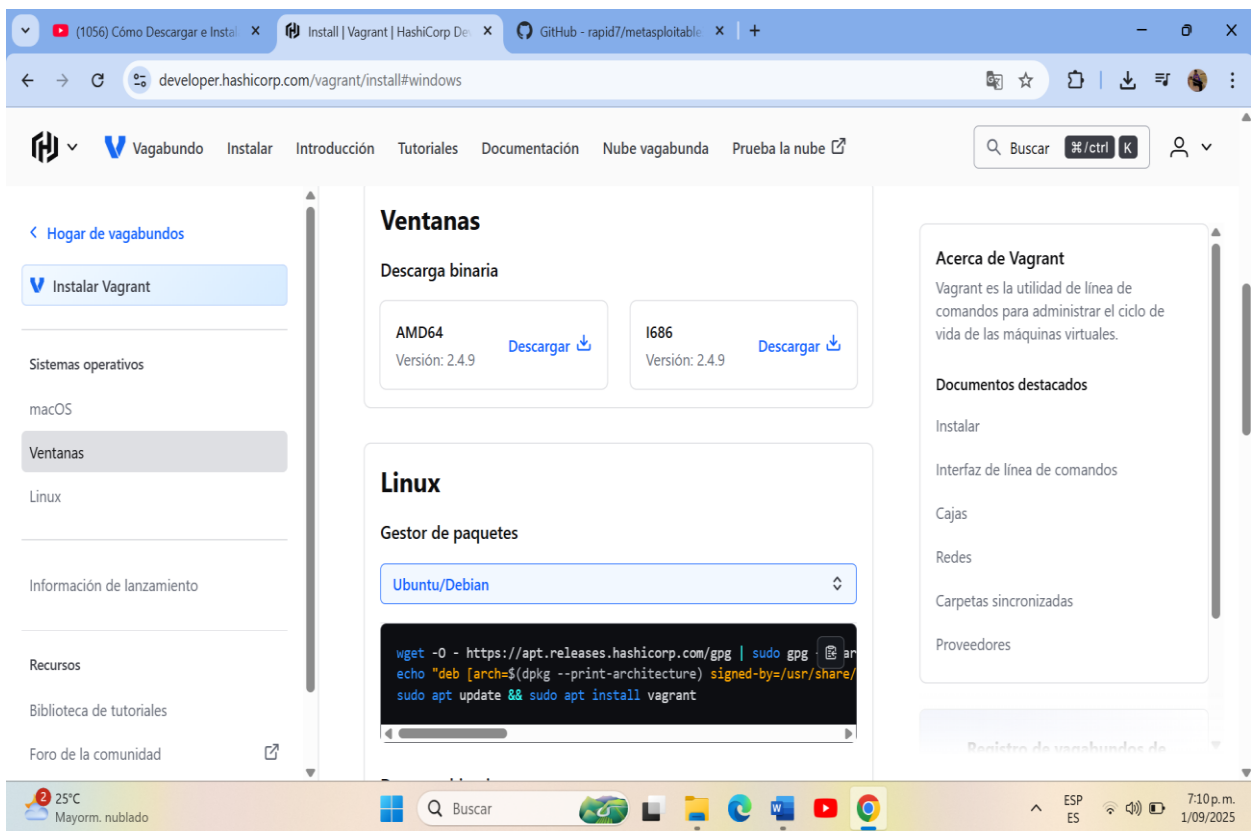
En el siguiente informe se realizó la instalación de metasploitable 3 que es un proyecto open soucer de seguridad informática que proporciona información acerca de vulnerabilidad de seguridad y ayuda en prueba de penetración. Esta instalación se hizo en virtual box que es una máquina virtual donde se pueden instalar otras máquinas virtuales, también se creo un manual de cómo hacer la instalación paso a paso integrando imágenes en tiempo real de la instalación.

DESARROLLO (bits, 2023)

Paso 1 Descargar Vagrant (hashicorp, 2022)

Para la instalación de metasploitable 3 debemos instalar vagrant que es un software open source para entornos virtuales, como lo descargamos.

- Ingresamos a la página oficial de vagrant <https://developer.hashicorp.com/vagrant/install#windows>
- Elegimos el sistema operativo que estamos utilizando
- Luego nos aparecerán 2 versiones binaria de las cuales vamos a descargar AMD64 versión 2.4.9

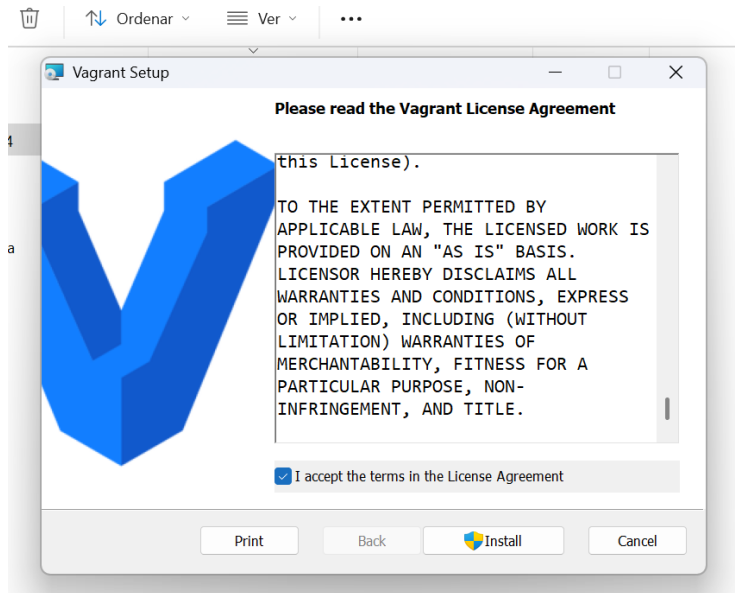


Paso 2 Instalación de vagrant

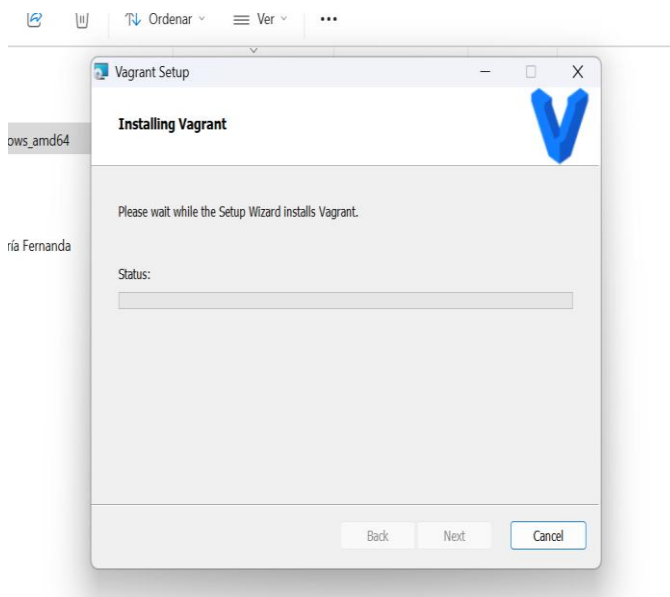
Al completar la descarga de vagrant pasamos a la instalación como:

- Abrimos el archivo

- aceptamos los términos y condiciones del producto
- y le damos instalar



Y comenzará la instalación inmediata, solo queda esperar el tiempo de cargar.



Luego de haber terminado la carga de instalación nos vamos a terminales de Windows para verificar que se instaló correctamente, ponemos el comando **vagrant --help** y nos muestra el pack de las variables de entorno.

```

Microsoft Windows [Versión 10.0.26100.4946]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\super> vagrant --help
Usage: vagrant [options] <command> [<args>]

-h, --help            Print this help.

Common commands:
autocomplete  manages autocomplete installation on host
box           manages boxes: installation, removal, etc.
cloud         manages everything related to Vagrant Cloud
destroy       stops and deletes all traces of the vagrant machine
global-status outputs status Vagrant environments for this user
halt          stops the vagrant machine
help          shows the help for a subcommand
init          initializes a new Vagrant environment by creating a Vagrantfile

tfile
login
package  packages a running vagrant environment into a box
plugin   manages plugins: install, uninstall, update, etc.
port     displays information about guest port mappings
powershell connects to machine via powershell remoting
provision provisions the vagrant machine
push     deploys code in this environment to a configured destination

on
rdp      connects to machine via RDP
reload  restarts vagrant machine, loads new Vagrantfile configuration
ion

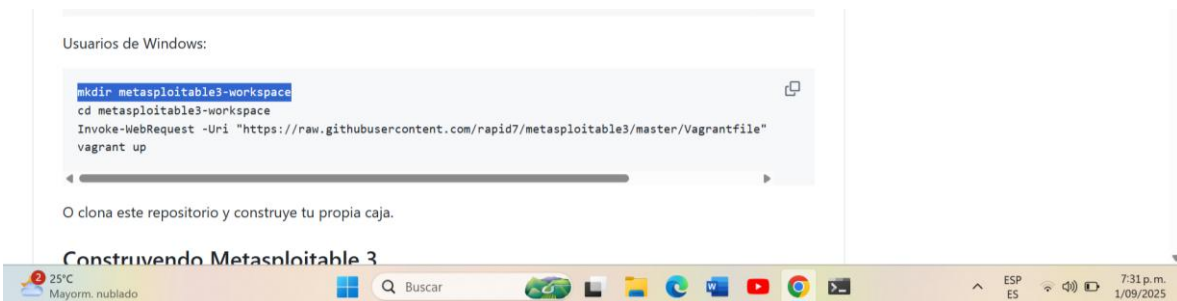
```

Paso 3 instalación de Metasploitable 3 (Simonirwin-r7, 2016)

Para la instalación de metasploitable 3 se deben seguir los siguientes pasos:

- ingresar la página github <https://github.com/rapid7/metasploitable3>
- estando en la página bajamos hasta llegar a metasploitable 3 y copiamos uno a uno los comandos para Windows en terminal.

Así se instalaría metasploitable 3. A continuación se mostrarán los comandos utilizados para la instalación.



Con este comando `mkdir metasploitable3-workspace` vamos a crear un directorio con el nombre de la máquina vulnerable.

```
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\super> mkdir metasploitable3-workspace

Directorio: C:\Users\super

Mode                LastWriteTime         Length Name
----                -
d-----          1/09/2025   7:33 p. m.         metasploitable3-workspace

PS C:\Users\super> |
```

Con este otro comando **cd metasploitable3-workspace** hacemos un cambio de directorio a esta máquina vulnerable.

```
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\super> mkdir metasploitable3-workspace
mkdir : Ya existe un elemento con el nombre especificado: C:\Users\super\metasploitable3-workspace.
En línea: 1 Carácter: 1
+ mkdir metasploitable3-workspace
+ ~~~~~
+ CategoryInfo          : ResourceExists: (C:\Users\super\metasploitable3-workspace:String) [New-Item], IOExceptio
n
+ FullyQualifiedErrorId : DirectoryExist,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Users\super> cd metasploitable3-workspace
PS C:\Users\super\metasploitable3-workspace> ls
PS C:\Users\super\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploit
able3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\Users\super\metasploitable3-workspace> ls

Directorio: C:\Users\super\metasploitable3-workspace

Mode                LastWriteTime         Length Name
----                -
-a-----          1/09/2025   8:03 p. m.         2297 Vagrantfile

PS C:\Users\super\metasploitable3-workspace> vagrant up
```

Y luego con el comando **Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"** instalaremos el vagrantfile.

```

n
+ FullyQualifiedErrorId : DirectoryExist,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Users\super> cd metasploitable3-workspace
PS C:\Users\super\metasploitable3-workspace> ls
PS C:\Users\super\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploit
able3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\Users\super\metasploitable3-workspace> ls

Directorio: C:\Users\super\metasploitable3-workspace

Mode                LastWriteTime         Length Name
----                -
-a----             1/09/2025   8:03 p. m.           2297 Vagrantfile

PS C:\Users\super\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/v
irtualbox/unknown/vagrant.box
Progress: 13% (Rate: 3024k/s, Estimated time remaining: 0:31:23)

```

Ya para finalizar utilizamos el comando **vagrant up** y se comienzan hacer automáticamente las configuraciones.

```

n
+ FullyQualifiedErrorId : DirectoryExist,Microsoft.PowerShell.Commands.NewItemCommand

PS C:\Users\super> cd metasploitable3-workspace
PS C:\Users\super\metasploitable3-workspace> ls
PS C:\Users\super\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploit
able3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\Users\super\metasploitable3-workspace> ls

Directorio: C:\Users\super\metasploitable3-workspace

Mode                LastWriteTime         Length Name
----                -
-a----             1/09/2025   8:03 p. m.           2297 Vagrantfile

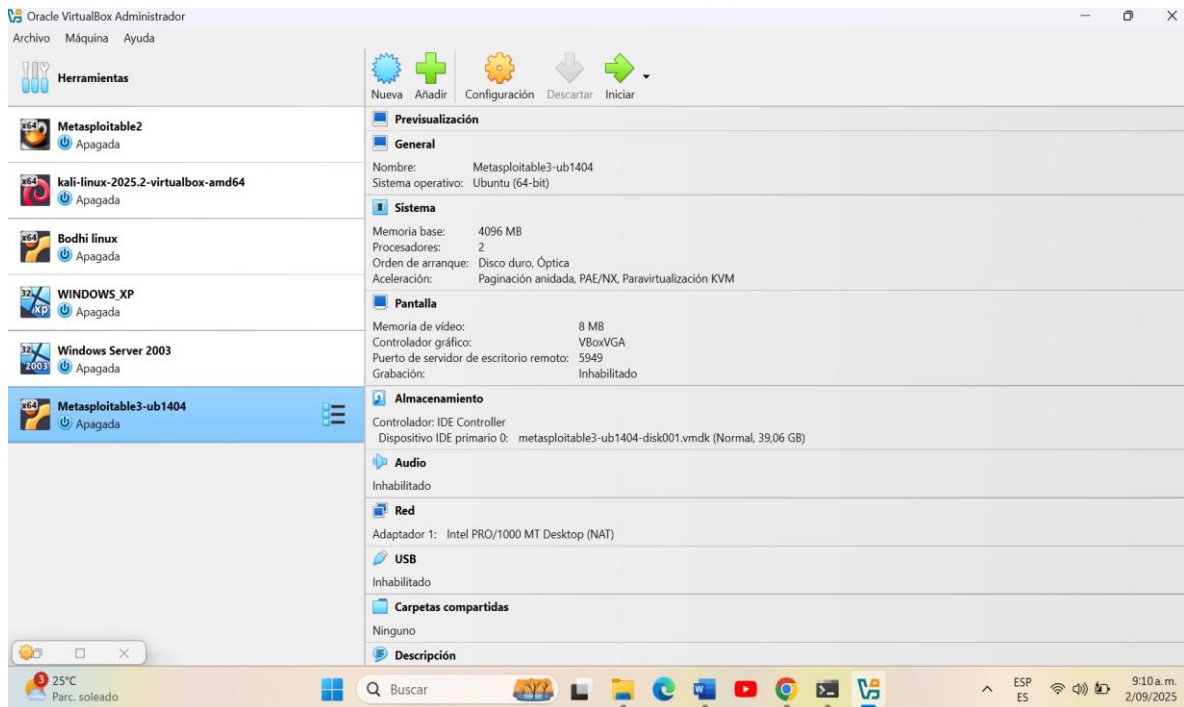
PS C:\Users\super\metasploitable3-workspace> vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Box 'rapid7/metasploitable3-ub1404' could not be found. Attempting to find and install...
ub1404: Box Provider: virtualbox
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/v
irtualbox/unknown/vagrant.box
Progress: 13% (Rate: 3024k/s, Estimated time remaining: 0:31:23)

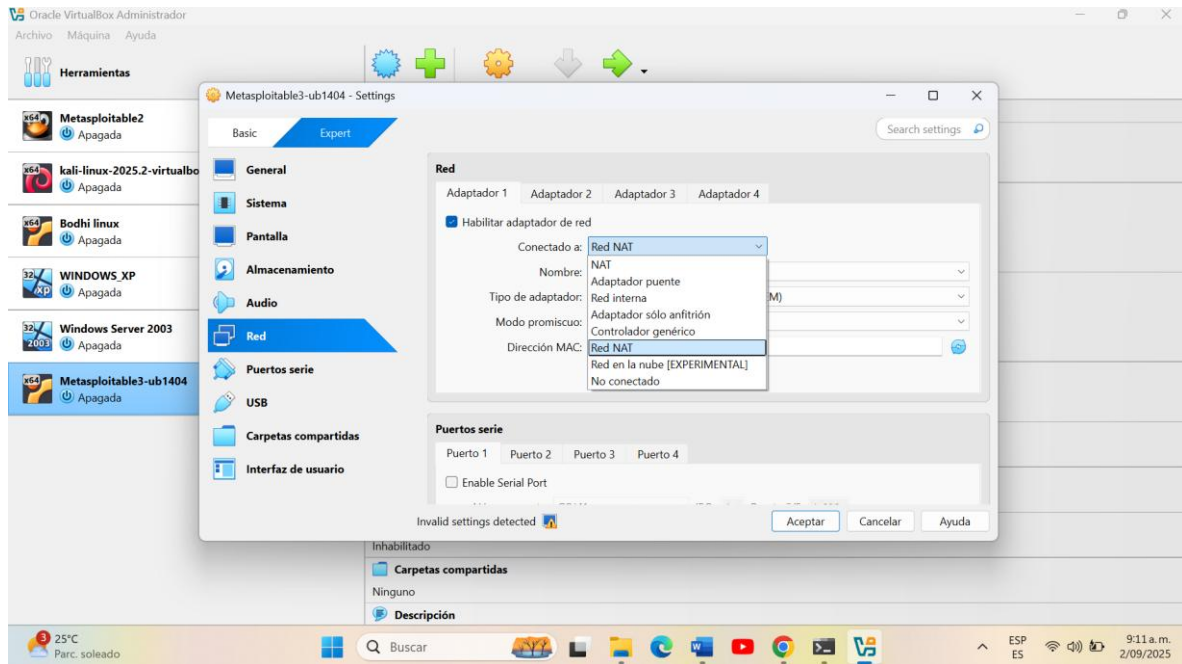
```

Paso 4 Configuración de red en Metasploitable 3

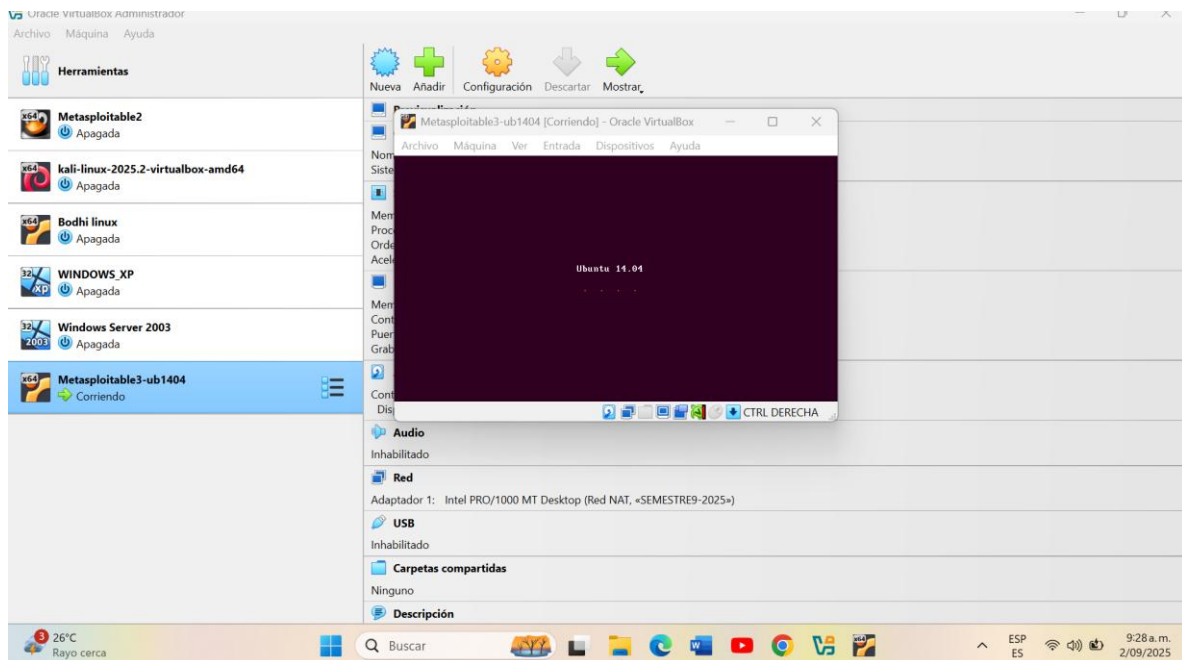
Cuando ya termina la carga de la instalación abrimos Virtual Box y nos aparecerá la máquina de metasploitable 3 ya creada, debemos configurar la red para que tenga visibilidad frente a las otras máquinas, como se hace:

- Ingresamos a configuraciones
- Red
- Seleccionamos Red Nat
- Aceptar





Ya con la configuración completada ponemos a correr el programa.





CONCLUSION

Se instalo con éxito el metasploitable 3 en la maquina virtual box con el manual que se elaborado en el taller.

Bibliografía

bits, C. (22 de junio de 2023). *contando bits*. Obtenido de contando bits :
<https://www.youtube.com/watch?v=0Uibljlllk>

hashicorp. (12 de diciembre de 2022). *hashicorp*. Obtenido de hashicorp:
<https://developer.hashicorp.com/vagrant/install#windows>

Simonirwin-r7. (10 de septiembre de 2016). *gihtub.com*. Obtenido de gihtub.com:
<https://github.com/rapid7/metasploitable3>