

### Colombia Hack Agent (CHackA)

[...]	Developer:	Jairo A. García H.	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB PARA INSTALAR METASPLOITABLE 2	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	<a href="https://github.com/chacka0101/HACKLABS">https://github.com/chacka0101/HACKLABS</a>	[...]
[...]	Publication Date:	30/Oct/2013	[...]

## HACKLAB PARA INSTALAR METASPLOITABLE 2

Resumen: Realizaremos la instalación y acceso a la plataforma de **METASPLOITABLE 2**.

Aplica para Instalar o subir en Máquinas Virtuales: **El HACKLAB se desarrolló con VMWARE Workstation PRO 14.**

¿Qué es **Metasploitable 2**?

Uno de los problemas que encuentra al aprender a usar un marco de explotación es tratar de encontrar y configurar objetivos para escanear y atacar. Afortunadamente, el equipo de Metasploit es consciente de esto y lanzó una máquina virtual de VMware vulnerable llamada "**Metasploitable 2**".

"**Metasploitable 2**" es una máquina virtual de Linux intencionalmente vulnerable que se puede usar para llevar a cabo entrenamientos de Hacking, probar herramientas de hacking y practicar técnicas comunes de PenTest. La máquina virtual se ejecutará en cualquier producto VMware reciente y otras tecnologías de visualización como VirtualBox. Puede descargar el archivo de imagen de "**Metasploitable 2**" desde acá:

Como recomendación NO exponga el "**Metasploitable 2**" a una red que no sea de confianza, use el modo NAT o solo en el host.

Una vez que haya descargado la VM "**Metasploitable 2**", extraiga el archivo zip, abra el archivo .vmx con el producto VMware de su elección y enciéndalo. Después de un breve tiempo, el sistema se iniciará y estará listo para la acción. El nombre de usuario es **msfadmin** y la contraseña predeterminada es **msfadmin**.



Colombia Hack Agent (CHACKA)

1. Descargar el “Metasploitable 2” de alguno de los dos (2) enlaces oficiales:

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

Registre sus datos y clic en Submit:

**RAPID7**

## Metasploitable - Virtual Machine to Test Metasploit

Download Metasploitable, 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.

Fill out the form to download the free version now – yours to keep, no expiration!

What is Metasploitable? How does it work?

chacka

chacka

chacka

CISO

chacka

chacka

chacka010@gmail.com

Colombia

Submit

Clic en “Download Metasploitable Now”:

**RAPID7**

## Metasploitable - Virtual Machine to Test Metasploit

Thank you for registering for Metasploitable

[Download Metasploitable Now](#)

Do you have a copy of Metasploit to use against Metasploitable?

Metasploit, backed by an open source community of 200,000 members, gives you that insight. It's the most popular penetration testing solution on the planet.

With an average of 1.2 exploits added each day, Metasploit allows you to find your weak point before a malicious attacker does.

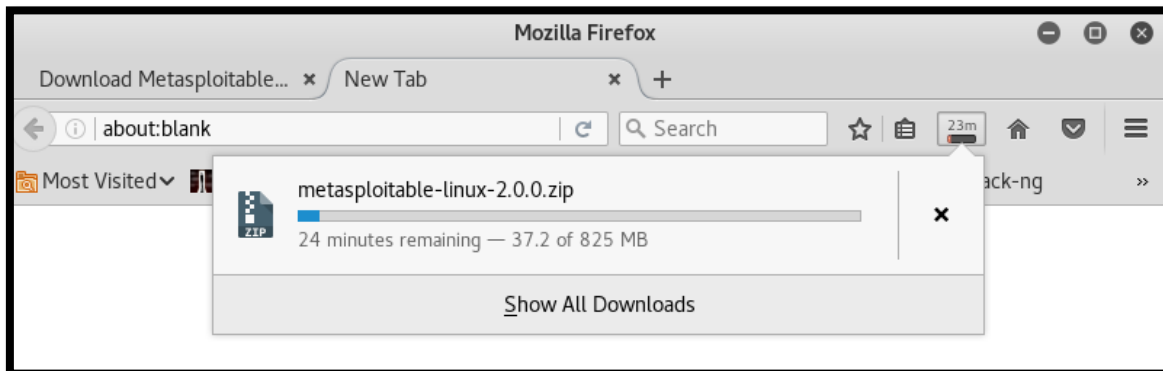
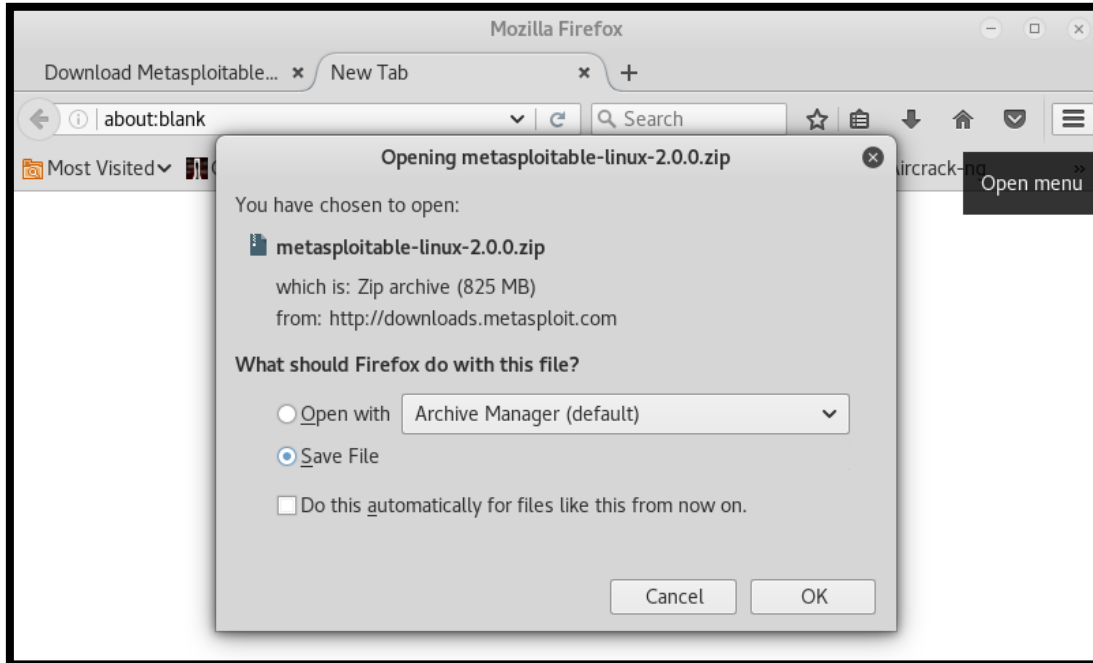
With Metasploit Pro you can:

- Conduct penetration tests 45% faster
- Validate vulnerabilities to prioritize remediation
- Manage phishing awareness to reduce user risk

**Free Metasploit Download**

Get your copy of the world's leading penetration testing tool

[Download Now](#)



Descomprimir el archivo .zip:

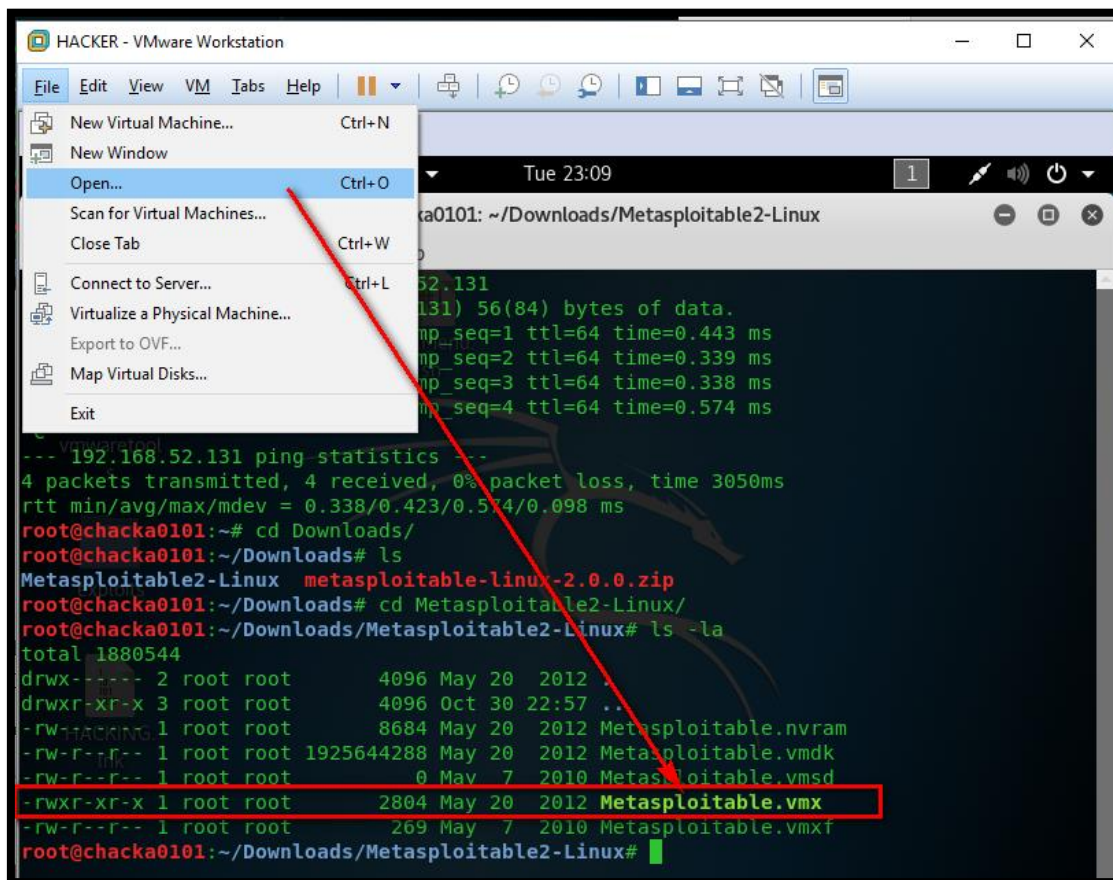
```
root@chacka0101:~/Downloads# ls
metasploitable-linux-2.0.0.zip
root@chacka0101:~/Downloads# unzip metasploitable-linux-2.0.0.zip
Archive:  metasploitable-linux-2.0.0.zip
  creating:  Metasploitable2-Linux/
  inflating:  Metasploitable2-Linux/Metasploitable.nvram
  inflating:  Metasploitable2-Linux/Metasploitable.vmdk
  extracting:  Metasploitable2-Linux/Metasploitable.vmsd
  inflating:  Metasploitable2-Linux/Metasploitable.vmx
  inflating:  Metasploitable2-Linux/Metasploitable.vmx
root@chacka0101:~/Downloads# ls -la
total 844828
drwxr-xr-x  3 root root    4096 Oct 30 22:57 .
drwxr-xr-x 23 root root    4096 Oct 30 14:46 ..
drwx-----  2 root root    4096 May 20 2012 Metasploitable2-Linux
-rw-r--r--  1 root root 865084584 Oct 30 22:48 metasploitable-linux-2.0.0.zip
root@chacka0101:~/Downloads#
```



Colombia Hack Agent (Chacka)

```
root@chacka0101:~/Downloads# cd Metasploitable2-Linux/
root@chacka0101:~/Downloads/Metasploitable2-Linux# ls -la
total 1880544
drwx----- 2 root root      4096 May 20  2012 .
drwxr-xr-x  3 root root      4096 Oct 30  22:57 ..
-rw-----  1 root root     8684 May 20  2012 Metasploitable.nvram
-rw-r--r--  1 root root 1925644288 May 20  2012 Metasploitable.vmdk
-rw-r--r--  1 root root           0 May  7  2010 Metasploitable.vmsd
-rwxr-xr-x  1 root root      2804 May 20  2012 Metasploitable.vmx
-rw-r--r--  1 root root       269 May  7  2010 Metasploitable.vmxr
root@chacka0101:~/Downloads/Metasploitable2-Linux#
```

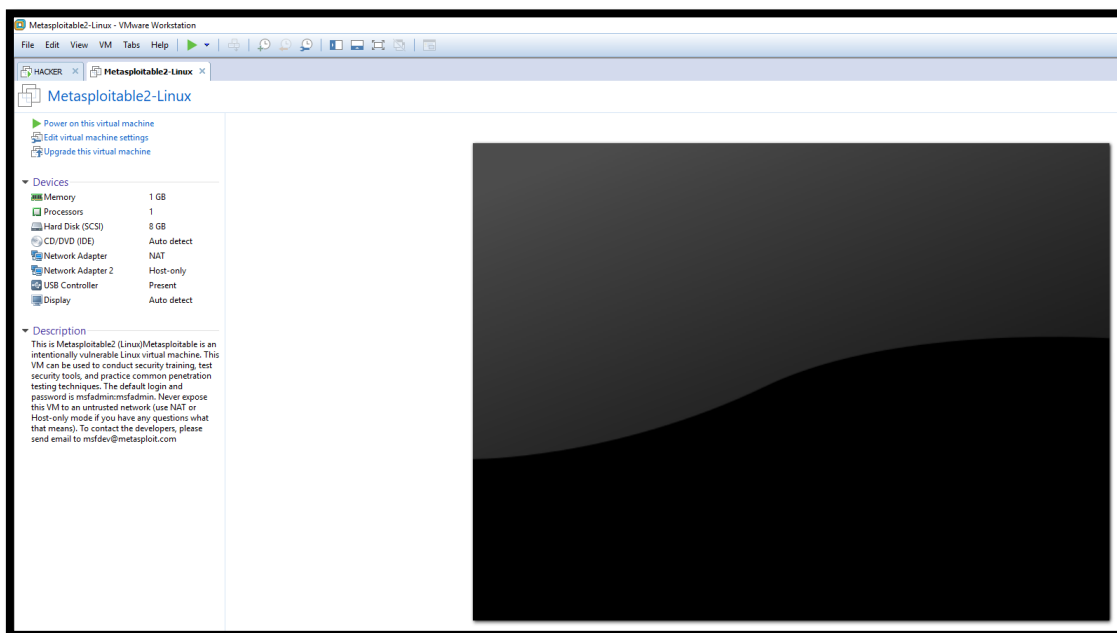
En la máquina virtual, clic en "File", luego "Open", luego seleccionar "Metasploitable.vmx":



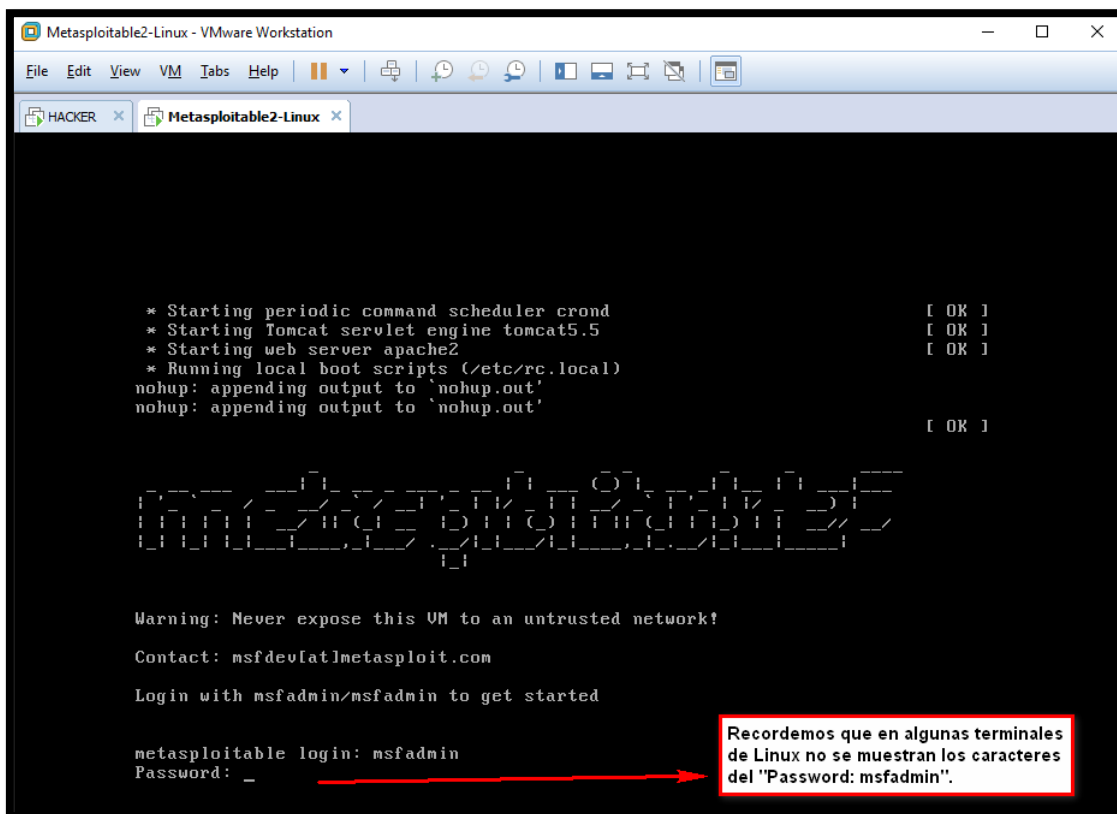


Colombia Hack Agent (CHACKA)

2. Configuramos la máquina virtual para que tenga 1 GB de RAM, recomendado para el "Metasploitable 2", luego ejecutamos la máquina virtual:



3. Ingresamos con el nombre de usuario es **msfadmin** y la contraseña predeterminada es **msfadmin**.



4. Configuramos la conexión de red para que el "Metasploitable 2" tenga conexión de red:

```
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:~$ ping google.com
PING google.com (172.217.30.206) 56(84) bytes of data:
64 bytes from bog02s08-in-f14.1e100.net (172.217.30.206): icmp_seq=1 ttl=128 tim
e=56.8 ms
64 bytes from bog02s08-in-f14.1e100.net (172.217.30.206): icmp_seq=2 ttl=128 tim
e=55.5 ms
^64 bytes from bog02s08-in-f14.1e100.net (172.217.30.206): icmp_seq=3 ttl=128 t
ime=55.8 ms

--- google.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 2998ms
rtt min/avg/max/mdev = 55.585/56.106/56.892/0.597 ms
msfadmin@metasploitable:~$
```

5. Identificamos la dirección IP del "Metasploitable 2" con el fin de brindarles dicha IP a las personas que atacarán el "Metasploitable 2".

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1a:b4:d1
          inet addr:192.168.52.131  Bcast:192.168.52.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1a:b4d1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13088 (12.7 KB)  TX bytes:11810 (11.5 KB)
          Interrupt:18 Base address:0x2000

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:16436  Metric:1
          RX packets:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35929 (35.0 KB)  TX bytes:35929 (35.0 KB)

msfadmin@metasploitable:~$
```





Colombia Hack Agent (Chacka)

6. Por último, hacemos un ping desde la máquina del Kali Linux al "Metasploitable 2":

```
root@chacka0101: ~  
File Edit View Search Terminal Help  
root@chacka0101:~# ping 192.168.52.131  
PING 192.168.52.131 (192.168.52.131) 56(84) bytes of data:  
64 bytes from 192.168.52.131: icmp_seq=1 ttl=64 time=0.443 ms  
64 bytes from 192.168.52.131: icmp_seq=2 ttl=64 time=0.339 ms  
64 bytes from 192.168.52.131: icmp_seq=3 ttl=64 time=0.338 ms  
64 bytes from 192.168.52.131: icmp_seq=4 ttl=64 time=0.574 ms  
^C  
--- 192.168.52.131 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3050ms  
rtt min/avg/max/mdev = 0.338/0.423/0.574/0.098 ms  
root@chacka0101:~#
```

7. Todo está listo para iniciar ataques desde KALI LINUX:



Agradecimientos a:

- Rapid7 - <https://metasploit.help.rapid7.com/docs/metasploitable-2>
- VMware - <https://www.vmware.com/>
- Kali Linux - <https://www.kali.org/>

-END-