Colombia Hack Agent (CHackA)

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

HACKLAB PARA INSTARLAR 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:

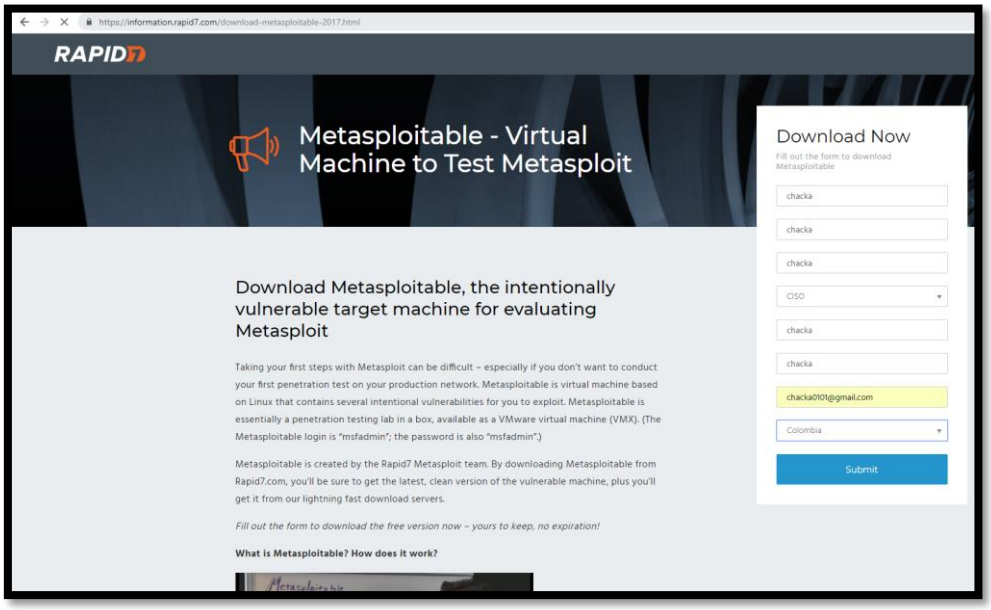
Como recomendación NO exponga el "**Metasploitable 2**" a una red que no sea de confianza, use el modo NAT o solo en el host.

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**.

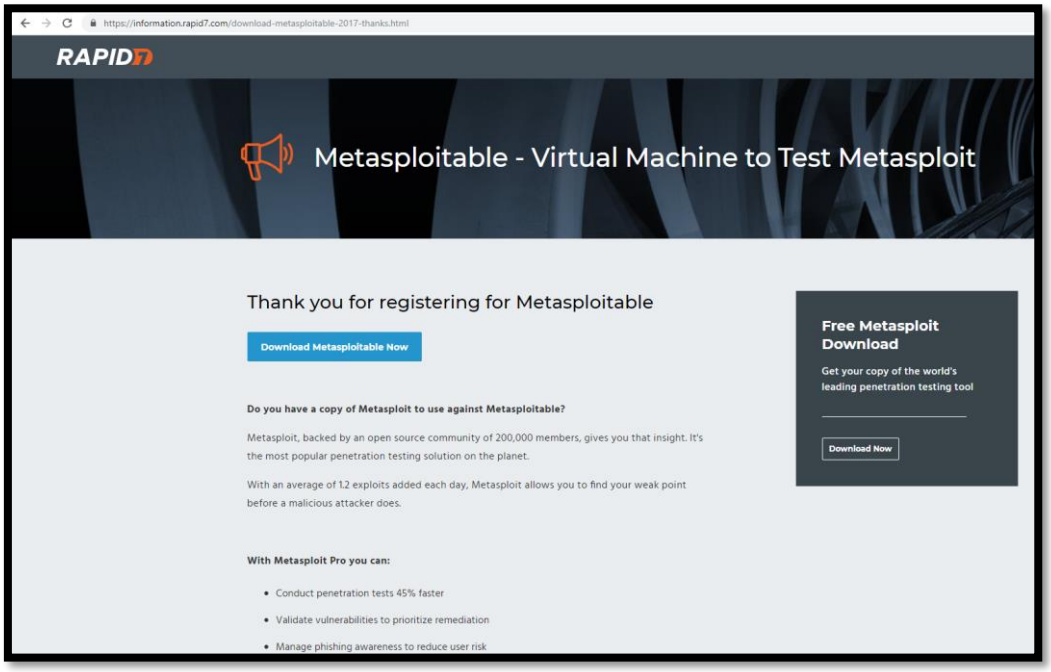
1. Descargar el **"Metasploitable 2"** de alguno de los dos (2) enlaces oficiales:

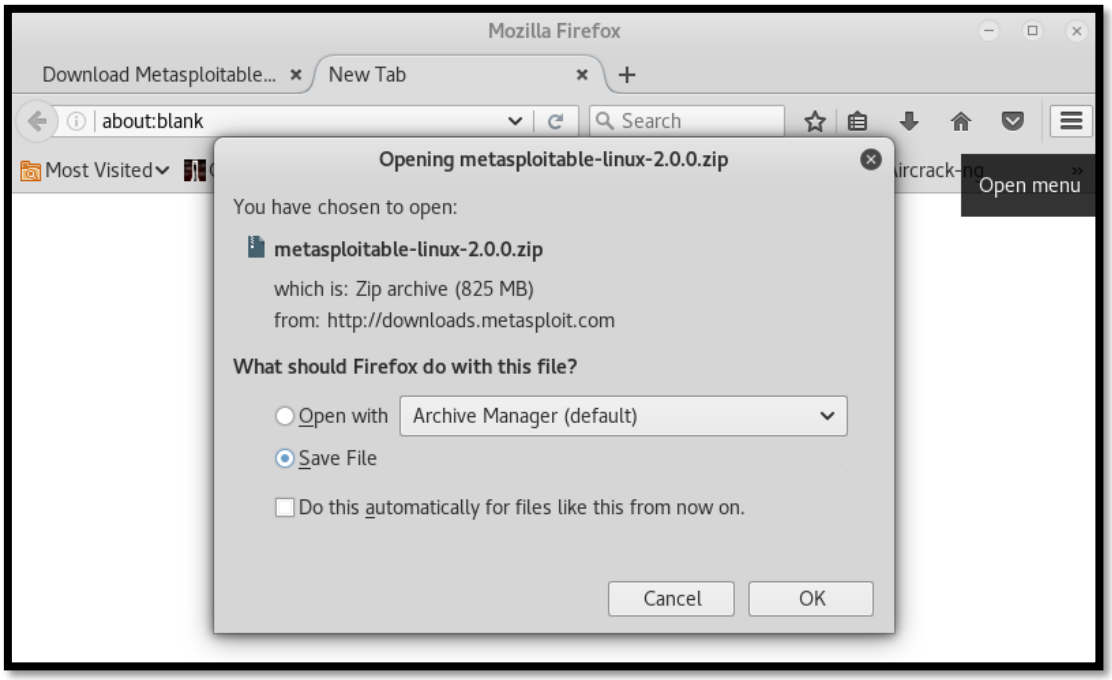
- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

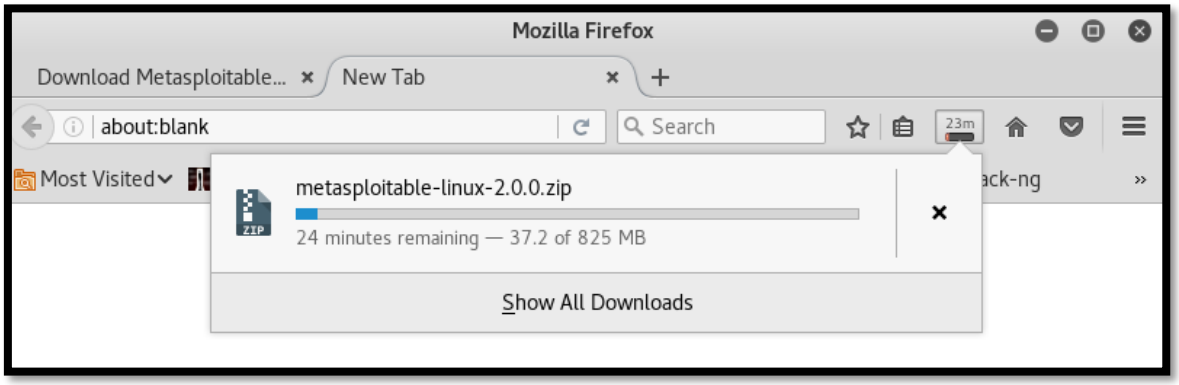
Registre sus datos y clic en Submit:



Clic en "Download Mestasploitable Now":





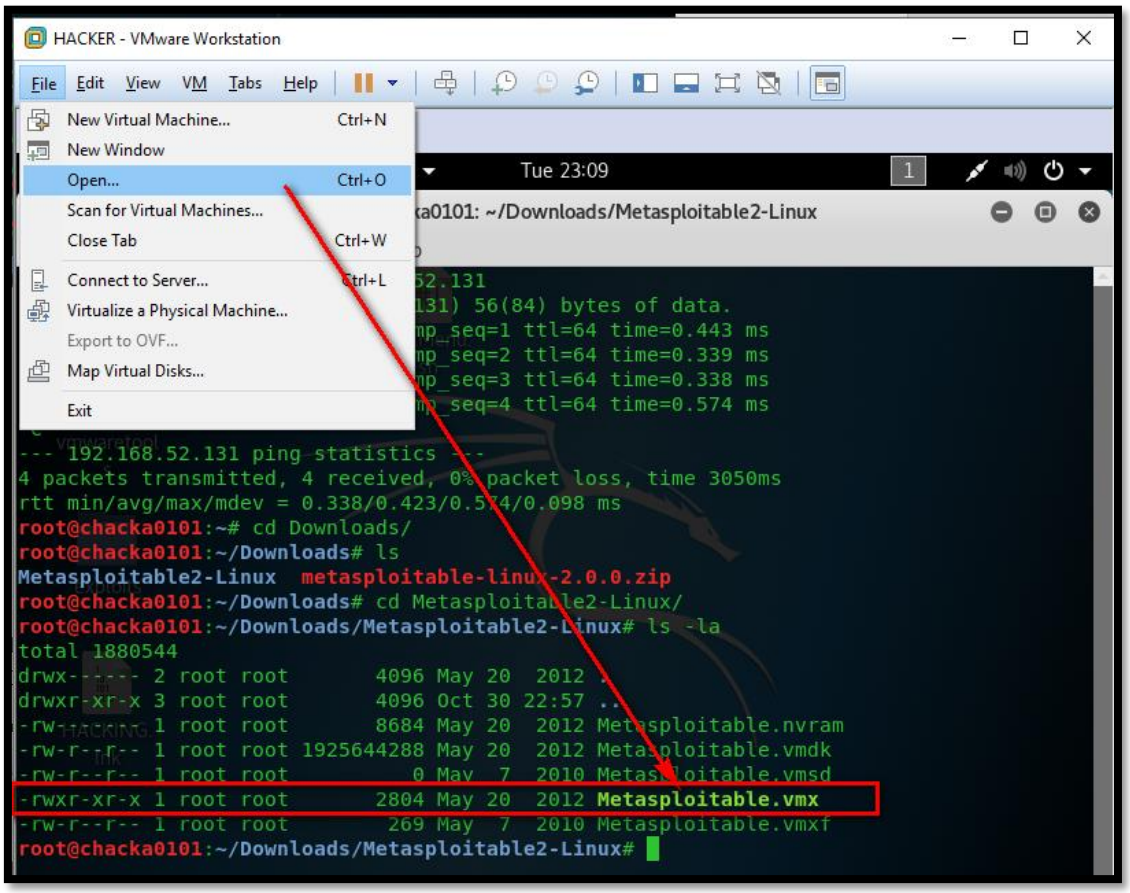


Descomprimir el archivo .zip:

```
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.vmxf
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#
```

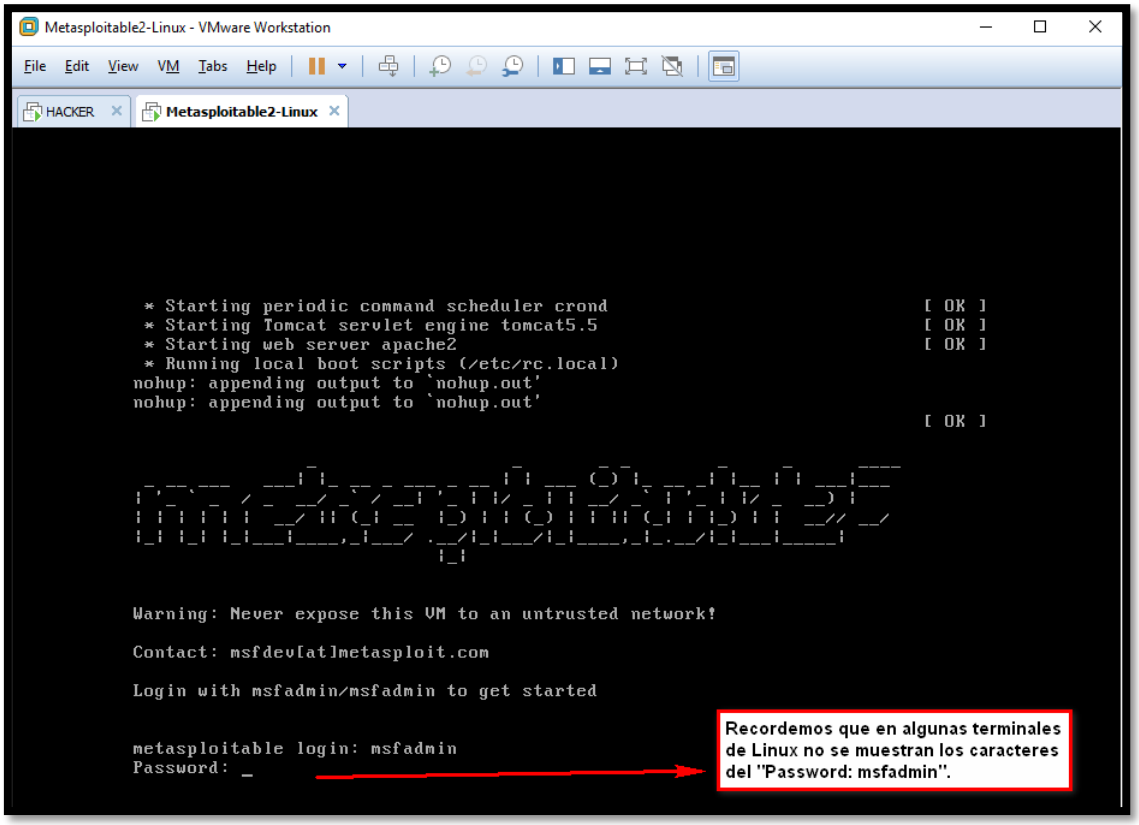
```
root@chacka0101:~/Downloads# cd Metasploitable2-Linux/
root@chacka0101:~/Downloads/Metasploitable2-Linux# ls -la
total 1880544
drwx------ 2 root root       4096 May 20  2012 .
drwxr-xr-x 3 root root       4096 Oct 30 22:57 ..
-rw------- 1 root root       8684 May 20  2012 Metasploitable.nvram
-rw-r--r-- 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.vmxf
root@chacka0101:~/Downloads/Metasploitable2-Linux#
```

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



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:~$
```

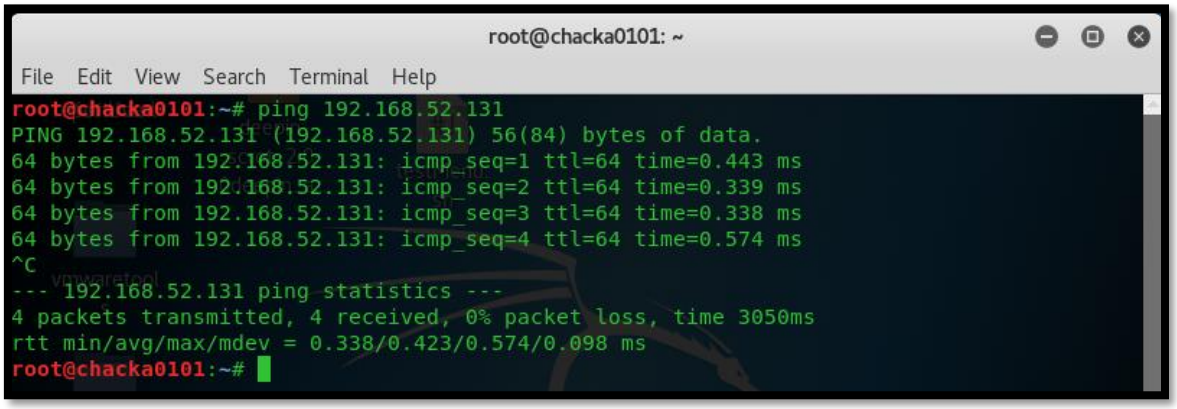
5. Identificamos la dirección IP del **"Metasploitable 2"** con el fín de brindarles dicha IP a las personas que atacarán el **"Metasploitable 2"**.

```
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:~$
```

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



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-