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

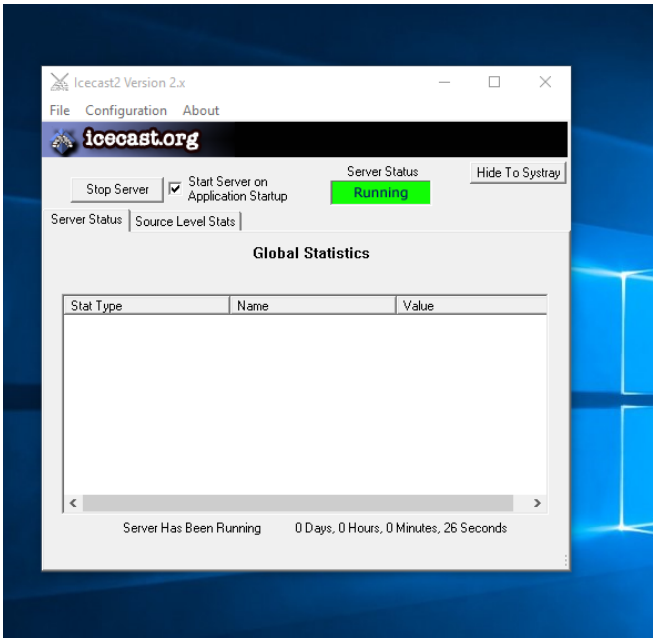

Fig.1 Attivazione server Icecast

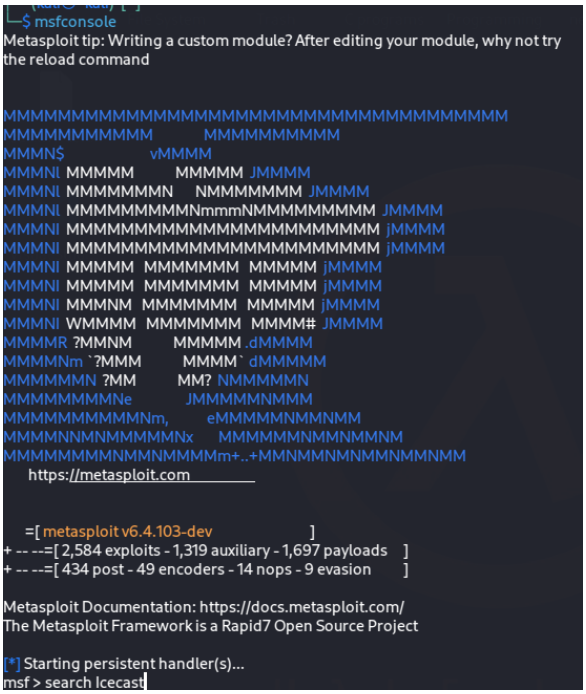

Fig.2 Avvio Metasploit

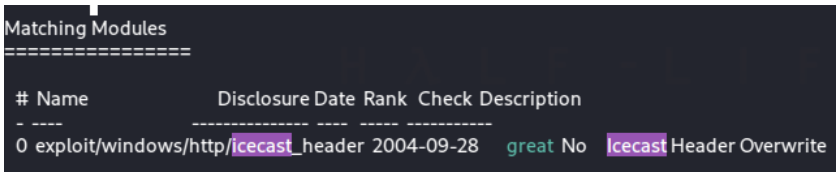

Fig.3 Ricerca modulo Icecast

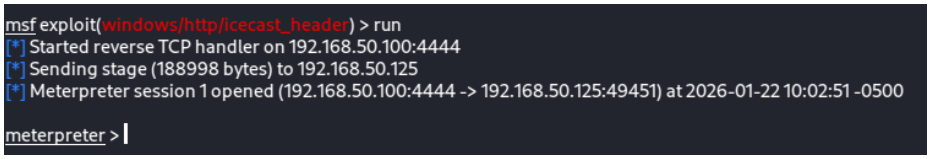

Fig.4 Lancio exploit

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

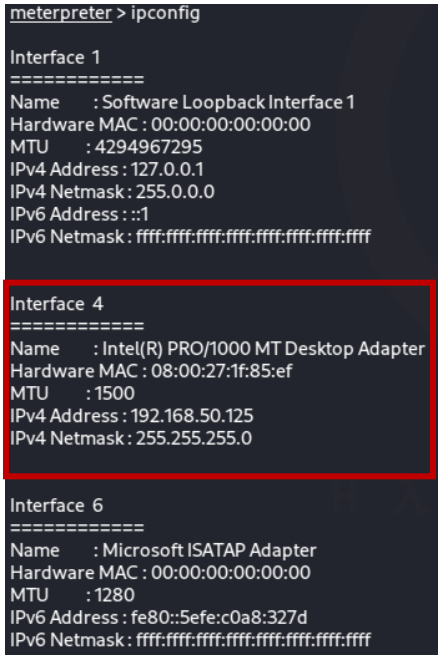

Fig.5 Verifica indirizzo IP

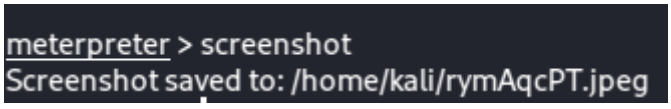

Fig.6 Comando screenshot

*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.