Report: Ottenimento di una sessione Meterpreter su Windows 10 tramite vulnerabilità Icecast

---

1. Introduzione

Lo scopo di questo laboratorio è dimostrare come una **vulnerabilità presente in un servizio di rete** possa essere sfruttata per ottenere accesso remoto a un sistema target.
In particolare, l'attività si concentra sull'ottenimento di una **sessione Meterpreter** su un sistema **Windows 10**, sfruttando una vulnerabilità nota del servizio **Icecast**, installato e attivo sulla macchina vittima.

---

2. Ambiente di laboratorio

L'ambiente utilizzato è composto da:

- **Macchina attaccante**:
  Sistema Linux con framework **Metasploit** installato
- **Macchina vittima**:
  - Sistema operativo: Windows 10
  - Servizio vulnerabile: Icecast
  - Configurazione di rete: rete locale di laboratorio

---

3. Descrizione del servizio Icecast e della vulnerabilità

Icecast è un server di streaming audio/video open-source.
Alcune versioni presentano **vulnerabilità di sicurezza** che permettono a un attaccante remoto di eseguire codice arbitrario sul sistema che ospita il servizio.

Nel contesto del laboratorio, tale vulnerabilità consente:

- l’iniezione di codice malevolo,
- l’esecuzione di un payload,
- l’apertura di una sessione remota sul sistema target.

Questa tipologia di vulnerabilità evidenzia l’importanza di:

- mantenere i servizi aggiornati,
- limitare l’esposizione dei servizi di rete,
- applicare patch di sicurezza.

---

4. Ottenimento della sessione Meterpreter

Sfruttando la vulnerabilità del servizio Icecast, è stato possibile ottenere una **sessione Meterpreter** sulla macchina Windows 10.

Meterpreter è un payload avanzato che permette:

- l’interazione con il sistema compromesso,
- l’esecuzione di operazioni di post-exploitation,
- la raccolta di informazioni sul sistema.

Il successo dell’operazione è confermato dall’apertura di una sessione attiva associata al target.

---

5. Attività di post-exploitation

Una volta ottenuto l’accesso al sistema, sono state eseguite alcune operazioni di post-exploitation richieste dalla traccia.

5.1 Identificazione dell’indirizzo IP della vittima

Attraverso le funzionalità di enumerazione fornite da Meterpreter, è stato possibile analizzare la configurazione di rete del sistema compromesso.

In particolare, sono state individuate:

- le interfacce di rete attive,
- l'indirizzo IP assegnato alla macchina vittima.

Questa informazione conferma:

- l'identità del target,
- la corretta riuscita dello sfruttamento,
- la posizione del sistema all'interno della rete di laboratorio.

5.2 Acquisizione di uno screenshot del desktop

Meterpreter fornisce funzionalità per interagire con la sessione grafica del sistema compromesso.
Poiché sulla macchina Windows 10 era presente una sessione desktop attiva, è stato possibile acquisire uno **screenshot dello schermo**.

Lo screenshot ottenuto mostra:

- il desktop del sistema vittima,
- la barra delle applicazioni,
- la conferma dell'accesso interattivo al sistema.

Questa operazione dimostra l'impatto concreto della vulnerabilità, in quanto un attaccante potrebbe:

- monitorare le attività dell'utente,
- raccogliere informazioni sensibili,
- compromettere la privacy.

---

6. Risultati ottenuti

Gli obiettivi del laboratorio sono stati raggiunti con successo:

- Ottenimento di una sessione Meterpreter su Windows 10
- Identificazione dell'indirizzo IP della macchina vittima
- Acquisizione di uno screenshot del desktop

Questi risultati dimostrano l'efficacia dello sfruttamento della vulnerabilità Icecast in un contesto controllato.

---

7. Considerazioni di sicurezza

Il laboratorio evidenzia come un servizio vulnerabile possa rappresentare un grave rischio per la sicurezza di un sistema. In uno scenario reale, un attaccante potrebbe sfruttare tale accesso per:

- installare malware persistente,
- esfiltrare dati sensibili,
- muoversi lateralmente nella rete.

Per mitigare questi rischi è fondamentale:

- aggiornare regolarmente i servizi,
- limitare l'esposizione delle porte,
- utilizzare firewall e sistemi di monitoraggio,
- adottare il principio del **least privilege**.

---

8. Conclusioni

L’attività svolta ha permesso di comprendere l’intero processo di sfruttamento di una vulnerabilità, dalla compromissione iniziale fino alle fasi di post-exploitation.

Il laboratorio sottolinea l’importanza della **sicurezza dei servizi di rete** e fornisce una dimostrazione pratica dell’impatto che una vulnerabilità non mitigata può avere su un sistema Windows.