LAB

8

Introduction To Metasploit Framework

By the end of this section, you should be able to:

- To understand the usage of Metasploit Framework
- Demonstrate the basic usage of Metasploit Framework

8.1 Metasploit Framework

Metasploit is one of the most powerful and widely used tools for penetration testing. Detail information and resources can be found www.metasploit.com. Metasploit have two versions: commercial and free edition. As an ethical hacker, who is often doing penetration testing will use Metasploit as the tool to do a proof of concept on the vulnerabilities found during the penetration testing exercise. In this lab session students are shown the usage of Metasploit community version that is available in the Kali Linux Distribution.

The Metasploit Framework is far more than just a collection of exploits–it is also a solid foundation that enables the user to build upon and easily customize to meet the user needs. This allows user to concentrate on the unique target environment and not have to reinvent the wheel. Metasploit is one of the single most useful security auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an

extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

The Metasploit framework is an open-source exploitation framework that is designed to provide security researchers and pen testers with a uniform model for rapid development of exploits, payloads, encoders, NOP generators, and reconnaissance tools. Figure 1 Illustrated Metasploit Framework architecture.

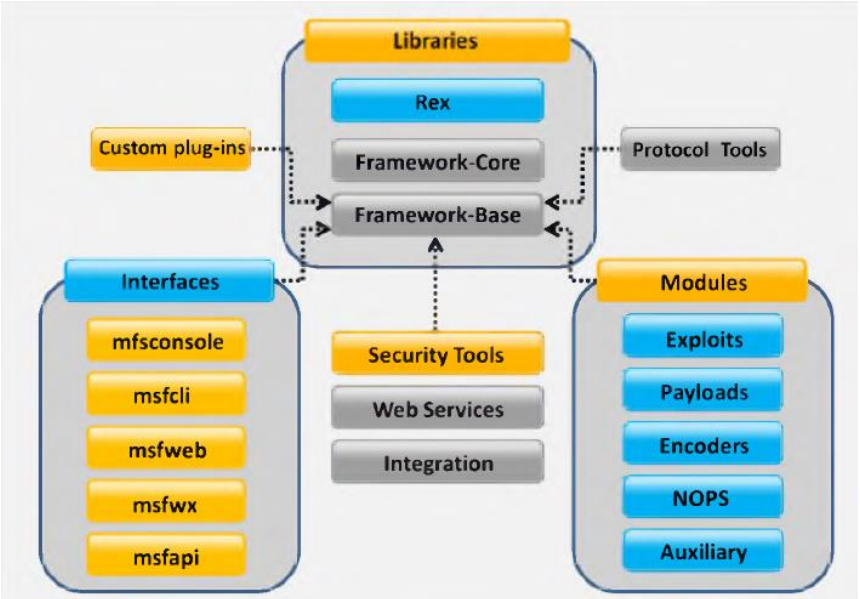

Figure 1: Metasploit Architecture

Figure 1 shows that Metasploit framework was designed to be as modular as possible in order to encourage the reuse of code across various projects. The framework itself is broken down into a few different pieces, the most low-level being the framework core. The framework core is responsible for implementing all of the

required interfaces that allow for interacting with exploit modules, sessions, and plugins. It supports vulnerability research, exploit development, and the creation of custom security tools.

Task 1

Introduction to Metasploit Framework.

1. To start Metasploit framework open Kali and open a terminal and type

   ```
   #> msfconsole
   ```

   msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an “all-in-one” centralized console and allows you efficient access to virtually all of the options available in the MSF.
2. Once you open msfconsole you will have a terminal showing the CLI of Metasploit framework. To start using MSF you can type help to get more information on command you can use in the MSF
3. The list of basic command that can be used are:-
   a. Info
   b. Show
   c. Search
      - There are a number of show commands you can use but the ones you will use most frequently are show auxiliary, show

exploits, show payloads, show encoders, and show nops.

d. use
e. set
f. sessions
g. back
h. exploit
i. exit

Task 2

Scanning in Metasploit Framework.

1. Scanning can also be done directly in MSF. To start this exercise make sure you have set the network environment. You need :-
    a. A kali VM set to NAT
    b. A Windows 7 VM set to NAT and being installed with Wireshark
    c. Metasploitable 2 VM set to NAT

2. NMAP can also be apply in msf just type the command:-

```
#msfconsole>nmap [nmap command] [Target's IP address]
```

3. Another option to do a port scanning is by using the auxiliary module of MSF. To use this feature you can start by type the command:-

```
#msfconsole> search type: auxiliary  portscan
```

4. A list of portscan method is displayed on the terminal
5. To use a particular portscan, type the command

```
#msfconsole>use
auxiliary/scanner/portscan/tcp
```

6. This command let user to do a TCP port scan on the target, you will also see the prompt change to

```
#msfconsole auxiliary(scanner/portscan/tcp)>
```

7. This prompt inform the user that they are using the auxiliary module of MSF and in the process to execute a TCP port scan. To see the options/information you required to run the scanning, type in the command

```
#.....> show options
```

8. This command shows you the options/information you need to provide in order to run the scanning, the information such as the NIC/interface, port number, thread and target's IP address.

9. To set the options/information required, use the command "`set`"

```
#...>set INTERFACE eth0
    *scanning done on NIC
#...>set PORTS 20-100
   *scanning port 20 to 100
#...>set RHOSTS [Target IP address] *To scan a range of IP just type in the subnet address e.g 192.168.2.0/24
#...>set THREADS 50
```

10. To check in the information you have entered use command "`show options`" again
11. To execute the scanning, type in the command:-

```
#...>run
```

12. The output of the scanning will be displayed on the terminal, listing the open and closed port.

- **For a step by step demonstration, please refer to the video manual prepared by your instructor.**

Review Question

 ***Do your scanning using the zenmap tool and compare the output between the zenmap output and MSF auxiliary module.***

 ***on your target device, capture the network traffic using wireshark, can you describe the network traffic activity***

 ***In the auxiliary module in the MSF, there are other method you can used other than scanning. Choose one method and describe what it is use for?***