HOW TO INSTALL METASPLOIT ONTO MAC OS X PLATFORM
by Leo Ni

INTRODUCTION:

Metasploit is an open-source Framework, providing information security professionals with a powerful tool in developing and executing exploit code against a remote target machine, and it is becoming well known for anti-forensic, penetration testing and evasion domains.

On the official website of Metasploit (URL: http://www.metasploit.com/download/), there are three installations available for download:

- Windows
- Linux 32-Bits
- Linux 64-Bits

Loosely translated, the operating systems being supported are:

- Windows XP, 2003, Vista, 2008 Server, and Windows 7
- Red Hat Enterprise Linux 5.x, 6.x - x86 and x86_64
- Ubuntu Linux 8.04, 10.04 - x86 and x86_64

Since Apple Mac OS X is built on FreeBSD, Metasploit should be able to run on Mac OS X, if we properly configure it. This article introduces the step-by-step working level instructions on how to install Metasploit on Mac OS X.

INSTALLATION PROCEDURES:

1. Preparations

1)   Before we start installing Metasploit Framework, we need to make sure the system has already installed Apple's Development Tool XCode. At the time when I am writing this article, the Mac OS X version I am using with is Mac OS X Lion (version 10.7.4), and XCode 4.5.2.

2)   XCode can be downloaded and installed at Apple's Developer website (https://developer.apple.com/). Or, it can be directly obtained from Apple's App Store, which is free to download.

3) After downloading and installation of XCode, launch XCode and select from menu XCode -> Preferences -> then click on download tab and make sure "Command Line Tools" has been installed.
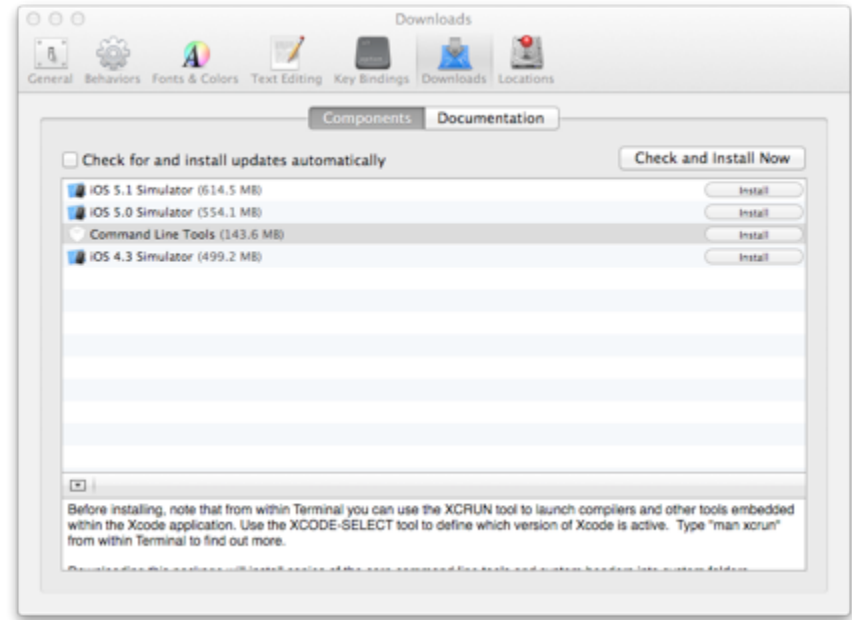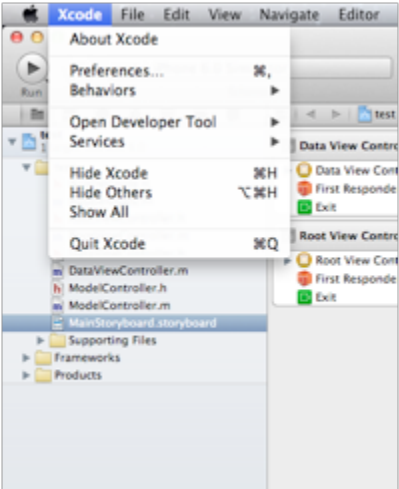
2. Installation Steps:

There are totally four major steps in installing Metasploit Framework:

1) Install MacPorts
2) Install Ruby and RubyGem
3) Install PostgreSQL Database (Optional)
4) Install Metasploit Framework

1) Install MacPorts

a) MacPorts is a powerful package, which is free for download and install, and it allows the installation of a number of packages by entering the command by using "sudo port install <packagename>" in the Terminal, which will then download, if necessary, compile and install the requested software, while also installing any required dependencies automatically.
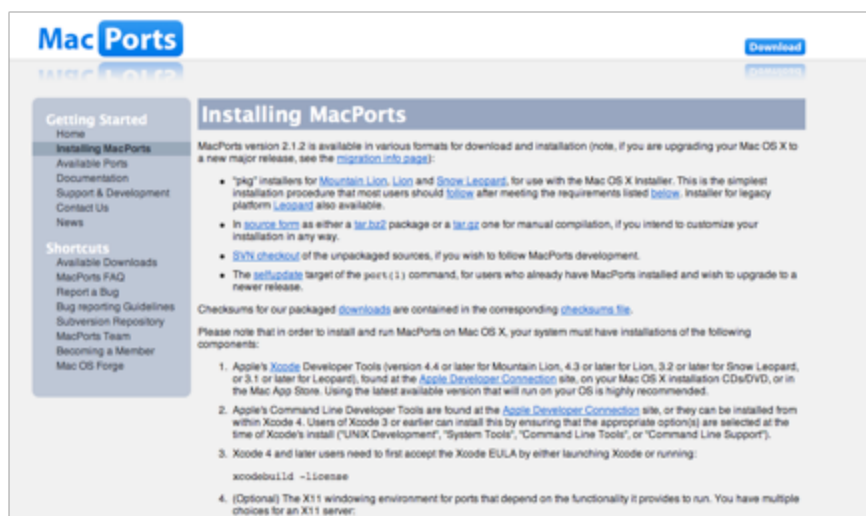
b) MacPorts can be downloaded from website

http://www.macports.org/install.php

c) Update MacPorts by using below command in the Terminal window:

port selfupdate

2) Install Ruby and RubyGem

Ruby and RubyGem packages are the essential components that Metasploit framework required to run,

since Metasploit framework was re-written in Ruby programming language.

a)   After MacPorts and XCode have been configured, we can go ahead to install a new version of Ruby and RubyGems with the following command:

$sudo port install ruby19 +nosuffix

b)   This will install the Ruby package onto folder /opt/local/. We need to verify that our environment variables are set correctly such that /opt/local/bin is listed before /usr/bin.

3)   Install PostgreSQL Database (Optional):

a)   In order to take full advantages of the features of Metasploit Framework, we need to install a database system and connect Metasploit Framework to that database system.

b)   PostgreSQL is the ideal candidate on Mac OS X. Most importantly, it is an object-relational database management system (ORDBMS) available for many platforms including Linux, FreeBSD, Solaris, Microsoft Windows and Mac OS X. And Metasploit Framework fully supports connecting to it

c)   To download PostgreSQL Database, below is the GUI based link

http://www.enterprisedb.com/products-services-training/pgdownload#osx

d)   During installation, PostgreSQL will ask you to set admin password. Please memorize the password and it will be re-used in the future

4)   Install Metasploit Framework

Now it is time for us to install the Metasploit Framework.

a)   In terminal window, run below command to download and install Metasploit Framework

sudo svn co https://www.metasploit.com/svn/framework3/trunk/ /opt/local/msf/

b)   Create links to our newly installed Metasploit applications

*sudo ln -s /opt/local/msf/msf* /opt/local/bin*

Until this step, the basic installation is done. Now we are going to do setup works to configure our Metasploit.

3.   Post-Installation Configurations:

In order to take advantage of its full features of Metasploit, connecting to database is required. Thus, below steps
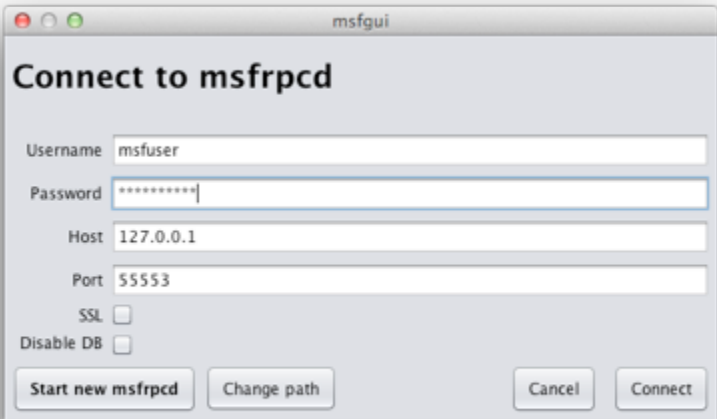
demonstrate how to set up a Database together with user name and password in PostgreSQL.

In PG Admin III, create a database called "metasploitdb" and a user name called "msfuser" with password "msfpassword", then assign "msfuser" to "metasploitdb".
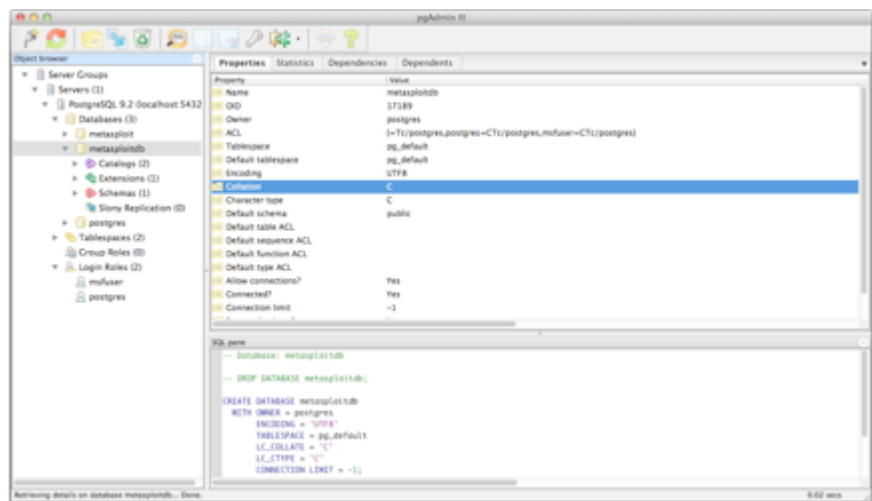
4. Launch Metasploit:

1) In the Terminal window, type "msfgui" command to launch Metasploit application on Mac OS X

2) In the msfgui login window, input username as "msfuser" with password "msfpassword" and make sure Host and Port Number are consistent with environment settings (In this case, we are using 55553 as default port number and host name as itself "127.0.0.1")

3) msfgui main window appear and now you can start enjoying Metasploit.

msfgui

File View Exploits Auxiliary Payloads History Post-Exploit Console Database Plugins Help

Jobs | Sessions | Hosts | Clients | Services | Vulns | Notes | Loots | Creds | Events

Host	Created	Updated	Name	Critical	Username	Info