
# Installation Guide

# Table of Contents

# Installing the Metasploit Framework

Rapid7 provides open source installers for the Metasploit Framework on Linux, Windows, and OS X operating systems. The Metasploit installer ships with all the necessary dependencies to run the Metasploit Framework. It includes msfconsole and installs associated tools like John the Ripper and Nmap.

## Prerequisites and Requirements

The following sections provide information on the prerequisites and requirements that the system must meet before you can install the Metasploit Framework.

### Minimum System Requirements

- 2 GHz+ processor
- 1 GB RAM available
- 1 GB+ available disk space

### Supported Platforms

- Red Hat Enterprise Linux Server 5.10+
- Red Hat Enterprise Linux Server 6.5+
- Red Hat Enterprise Linux Server 7.1+
- Ubuntu Linux 10.04 LTS
- Ubuntu Linux 12.04 LTS
- Ubuntu Linux 14.04 LTS
- Kali Linux 2.0
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7
- Windows 8.1

### Disable Anti-virus Software

Anti-virus software detects that Metasploit Framework as malicious and may cause problems with the installation and runtime of Metasploit Framework. The Metasploit Framework exploits the same vulnerabilities that the anti-virus software detects. Therefore, when you install the Metasploit Framework, the anti-virus software interrupts the installation process and alerts you of the security risks that may infect the system.

If you intend to use the Metasploit Framework, you should disable any anti-virus software before you install Metasploit Framework. If you cannot disable the anti-virus software, you must exclude the Metasploit directory from the scan.

### Disable Firewalls

Local firewalls, including Windows Firewall, interfere with the operation of exploits and payloads. If you install the Metasploit Framework from behind a firewall, the firewall may detect the Metasploit Framework as malware and interrupt the download.

Please disable the local firewalls before you install or run Metasploit Framework. If you must operate from behind a firewall, you should download the Metasploit Framework from outside the network.

### Obtain Administrator Privileges

To install the Metasploit Framework, you must have administrator privileges on the system that you want to use to run the framework.

## Installation

The easiest way to get the Metasploit Framework is to download the installer from the Rapid7 site. Visit http://www.rapid7.com/products/metasploit/download.jsp to find and download the installer for your operating system.

The installer provides a self-contained environment for you to run and update the Metasploit Framework. This means that all the necessary dependencies are installed and configured for you during the installation process. If you prefer to install the dependencies manually, and configure the Metasploit Framework to use those dependencies, read https://community.rapid7.com/docs/DOC-1296.

When you launch the installer file, the installer prompts you to enter the following configuration options:

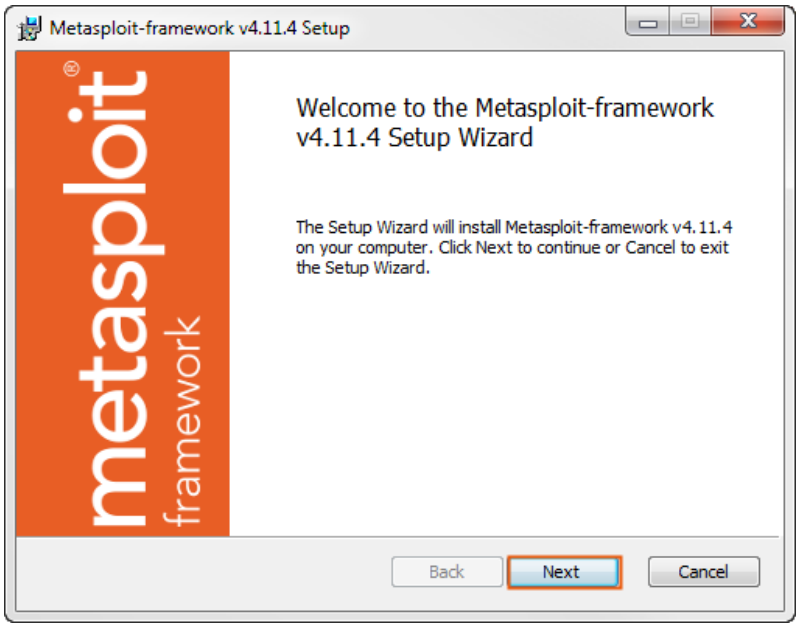
- The destination folder on the hard drive or external disk where you want to install the Metasploit Framework.

! If you are a Kali Linux 2.0 user, Metasploit Framework is already pre-installed and updated monthly. You can use this installer if you want to receive updates more frequently.

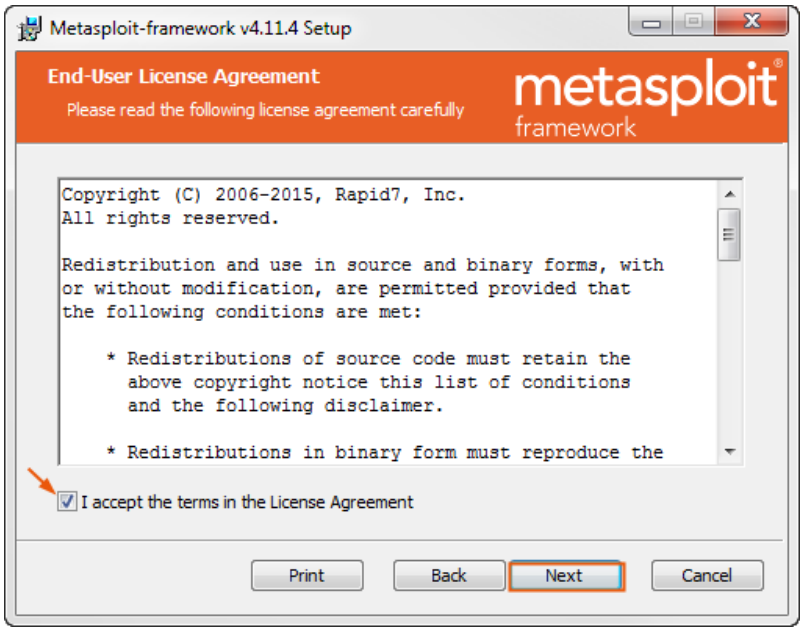
! Rapid7 no longer supports the pre-installed Metasploit Community edition on Kali Linux 1.0/

### Installing the Metasploit Framework on Windows

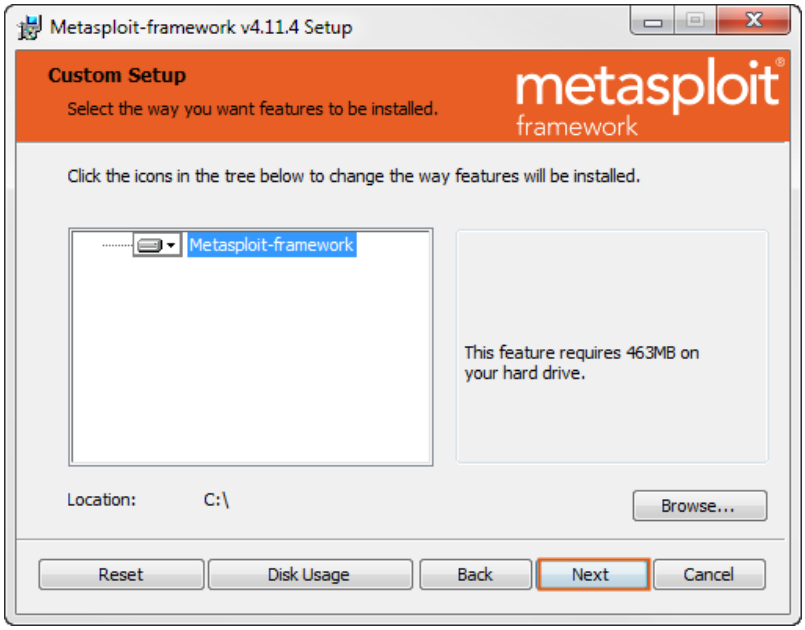
1. Visit http://windows.metasploit.com/metasploitframework-latest.msi to download the Windows installer.
2. After you download the installer, locate the file and double-click the installer icon to start the installation process.
3. When the Setup screen appears, click **Next** to continue.



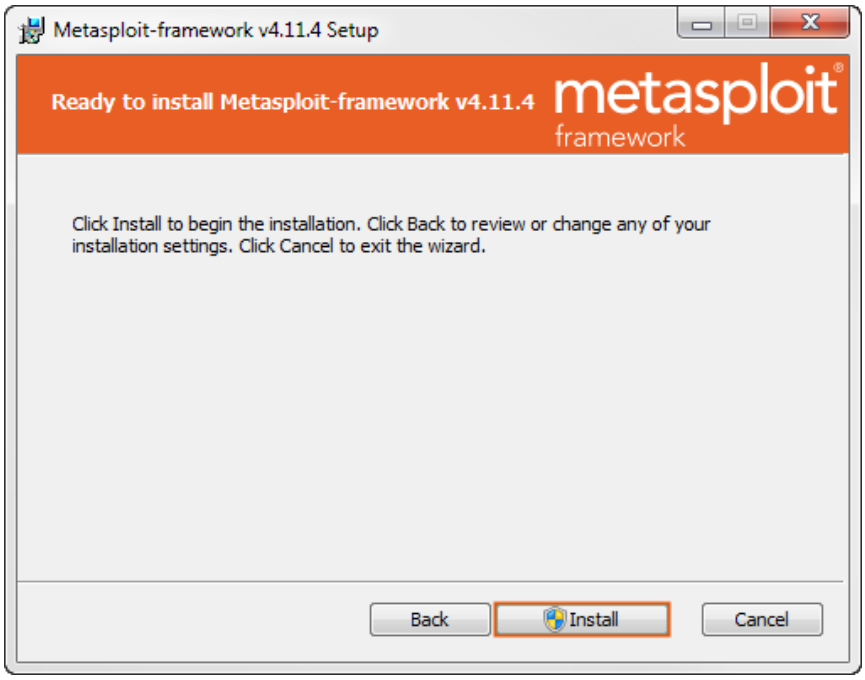
4. Read the license agreement and select the **I accept the license agreement** option. Click **Next** to continue.




5. Browse to the location where you want to install the Metasploit Framework. By default, the framework is installed on the `C:\Metasploit-framework`. Click **Next** to continue.



6. Click **Install**.




7. The installation process can take 5-10 minutes to complete. When the installation completes, click the **Finish** button.

To launch msfconsole after the installation completes, run the following from the command line:

```
$ msfconsole.bat
```

### Installing the Metasploit Framework on Linux

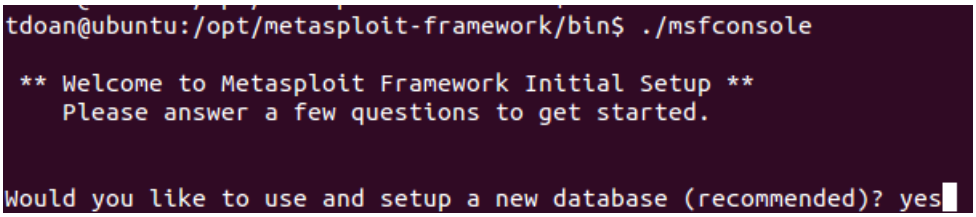
1. Open the terminal.
2. Enter the following command to add the build repository and install the Metasploit Framework package:

```
curl https://raw.githubusercontent.com/rapid7/metasploit-
omnibus/master/config/templates/metasploit-framework-
wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall &&
./msfinstall
```

After the installation completes, open a terminal window and type the following to start msfconsole:

```
$ ./msfconsole
```

The prompt asks you if you want to use and set up a new database. Type 'y' or 'yes' to run the initial configuration script to create the initial database.




If all goes well, the console starts and displays the following:

```
Creating database at /Users/joesmith/.msf4/db
Starting Postgresql
Creating database users
Creating initial database schema

** Metasploit Framework Initial Setup Complete **

[*] Starting the Metasploit Framework console...-[*] The initial module
cache will be built in the background, this can take 2-5 minutes...
/

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
=[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]
+ -- --=[ 1454 exploits - 827 auxiliary - 229 post ]
+ -- --=[ 376 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf >
```

To check to see if the database was set up, run the following command:

```
$ db_status
```

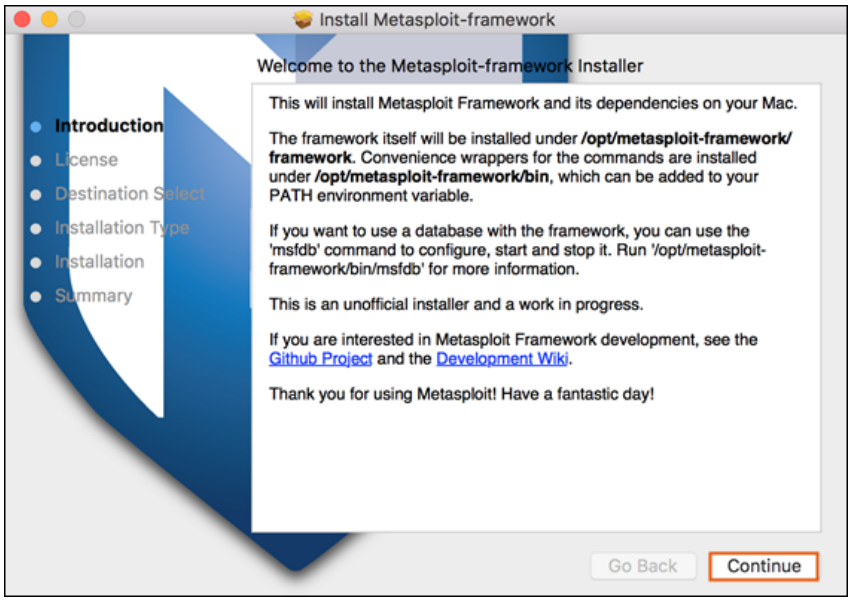
If the Metasploit Framework successfully connected to the database, the following status displays:

```
[*] postgresql connected to msf
```

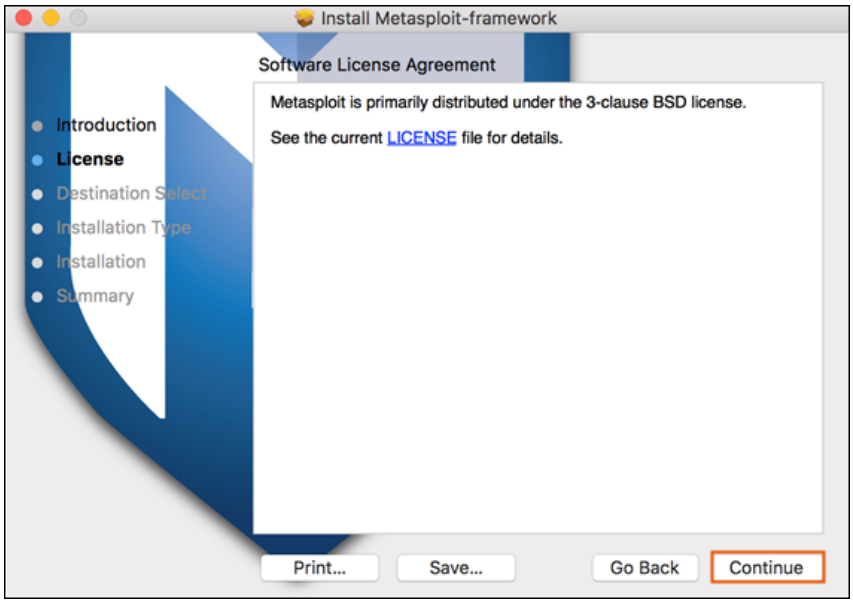
### Installing Metasploit Framework on OSX

1. Visit http://osx.metasploit.com/metasploitframework-latest.pkg to download the OSX package.
2. After you download the package, locate the file and double-click the installer icon to start the installation process.

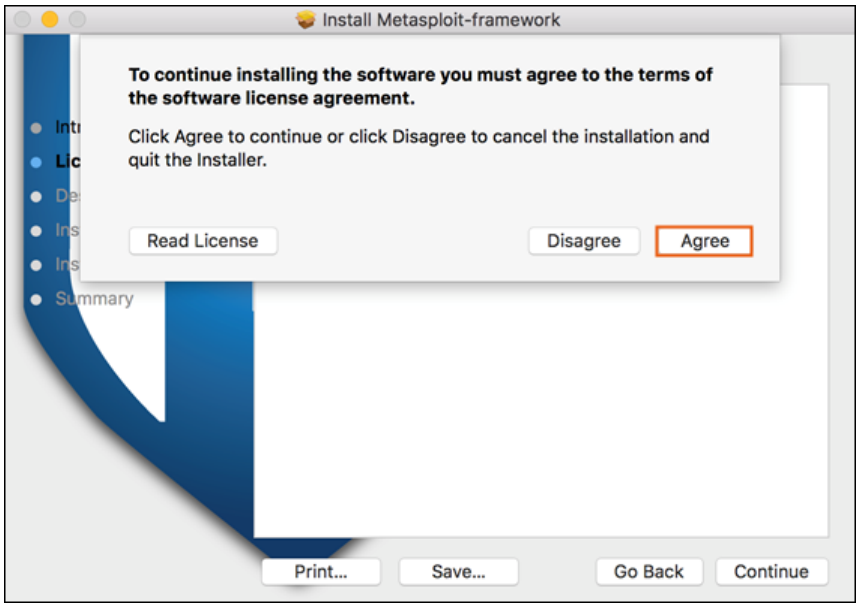
3. When the Welcome screen appears, click **Continue**.



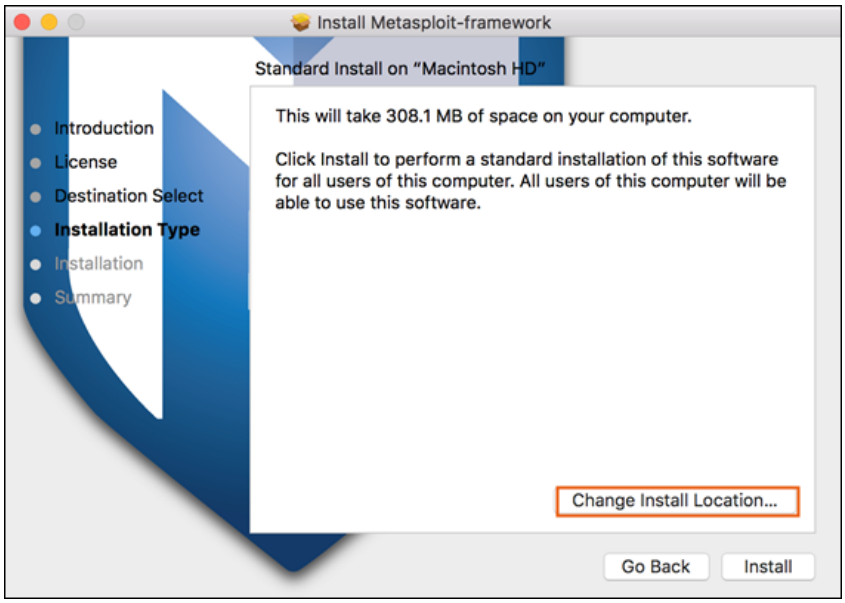

4. Read the license agreement and click **Continue**.



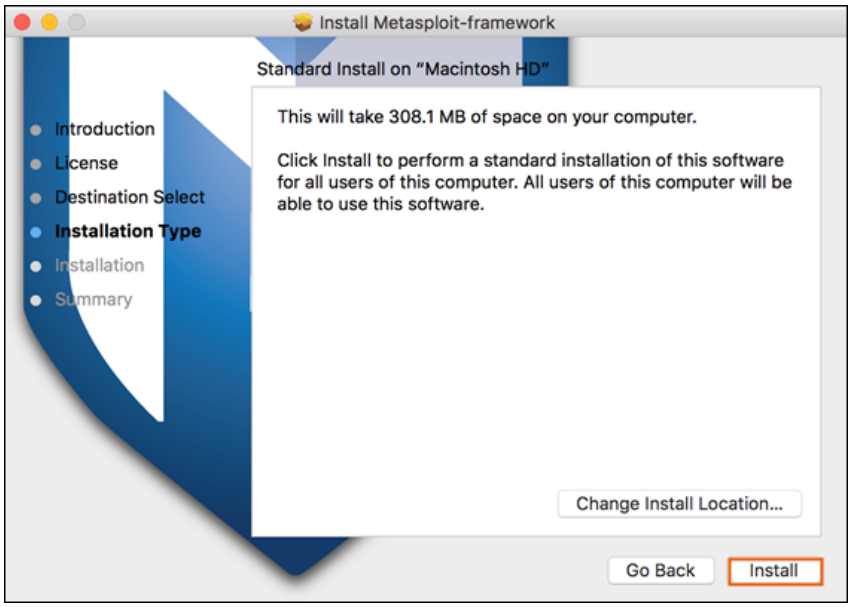
5. Agree to the license agreement to continue with the installation process.



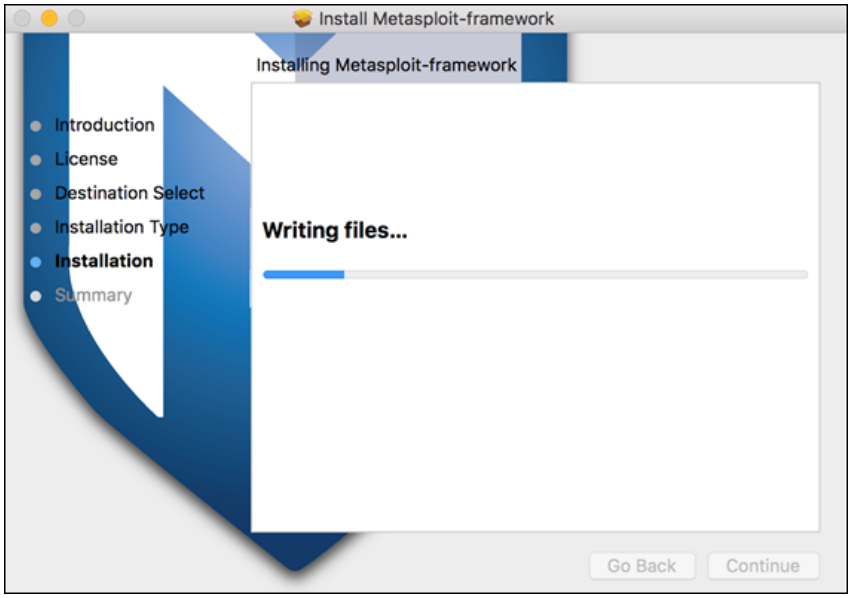

6. Browse to the location where you want to install the Metasploit Framework if you want to change the default installation location.



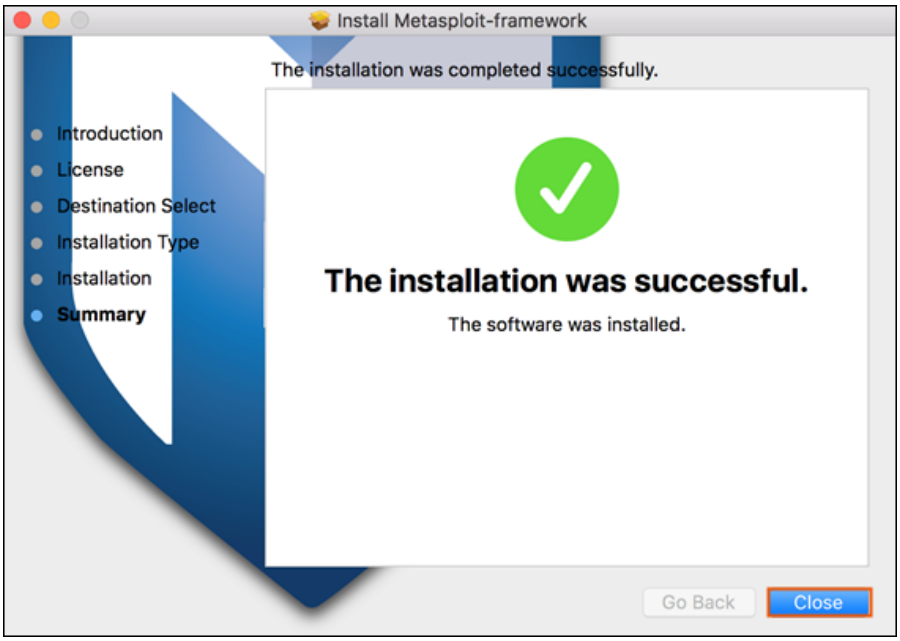
7. Click **Install** when you are ready to install the Metasploit Framework.




8. The installation process can take 5-10 minutes to complete.




9. When the installation completes, click the **Close** button.




## Managing the Database

If you did not opt to create a database when msfconsole loaded for the first time, you can use the msfdb script to configure postgresql to run as your local user and store the database in `~/.msf4/db/`.

To enable and start the database, run the following command:

```
$ msfdb init
```

After the database starts, you can use any of the following commands to manage the database:

- `msfdb reinit`: Deletes and reinitializes the database.
- `msfdb delete`: Deletes the database.
- `msfdb start`: Starts the database.
- `msfdb stop`: Stops the database.
- `msfdb status`: Shows the database status.