Metasploit

Installation Guide
Release 4.4

RAPID7

TABLE OF CONTENTS

About this Guide

Target Audience 1
Organization 1
Document Conventions 1
Support 2
- Support for Metasploit Pro and Metasploit Express 2
- Support for the Metasploit Framework and Metasploit Community 2

Installing Metasploit

About the Installer 3
- Overview of the Installation Process 3
- Installed Programs 3
- Installer Size 4
- Bundled Packages 4

Prerequisites and Recommendations 5
- Minimum Hardware, Disk Space, and Memory Requirements 5
- Supported Platforms 5
- Disabling Antivirus Software 5
- Disabling Firewalls 5
- Authorized Usage 5

Windows Installation 6
- Installing on Windows 6

Linux Installation 10
- Installing on Linux 10
- Installing with the Linux Console 15

License Key Activation

Online Activation 19
Offline Activation 19

About this Guide

This guide provides information and instructions to help you install Metasploit. The following sections describe the audience, organization, and conventions used within this guide.

Target Audience

This guide is for IT and security professionals who use Metasploit as a penetration testing solution.

Organization

This guide includes the following chapters:

- About this Guide
- Installing Metasploit

Document Conventions

The following table describes the conventions and formats that this guide uses:

Convention	Description
Command	Indicates buttons, UI controls, and fields. For example, "**Click Projects > New Project**."
Code	Indicates command line, code, or file directories. For example, "Enter the following: `chmod +x Desktop/metasploit-3.7.1-linux-x64-installer`."
Title	Indicates the title of a document or chapter name. For example, "For more information, see the *Metasploit Pro Installation Guide*."
Note	Indicates there is additional information about the topic.

Support

Rapid7 and the community strive to provide you with a variety of support options. For a list of support options that are available, view the support section for the Metasploit product that you are using.

Support for Metasploit Pro and Metasploit Express

You can visit the Customer Center or e-mail the Rapid7 support team to obtain support for Metasploit Pro and Metasploit Express. To log in to the Customer Center, use the e-mail and password provided by Rapid7.

The following table describes the methods you can use to contact the Rapid7 support team.

Support Method	Contact Information
Customer Center	http://www.rapid7.com/customers/customer-login.jsp
E-mail	support@rapid7.com

Support for the Metasploit Framework and Metasploit Community

An official support team is not available for the Metasploit Framework or for Metasploit Community. However, there are multiple support channels available for you to use, such as the IRC channel and mailing list.

You can visit the Metasploit Community to submit your question to the community or you can visit the help page to view the support options that are available.

INSTALLING METASPLOIT

This chapter covers the following topics:

- **About the Installer** 3
- **Prerequisites and Recommendations** 5
- **Windows Installation** 6
- **Linux Installation** 10+

About the Installer

The standard Metasploit installer uses a graphical interface to guide you through the installation process. Installation is a simple process that guides you through a series of prompts to identify the location where you want to install Metasploit and the ports that you want Metasploit to use. After you define your installation preferences, the installer installs the dependencies and services that are necessary to run Metasploit.

Overview of the Installation Process

When you launch the installer, it prompts you to enter the following information:

- The destination folder on the hard drive or external disk where you want to install Metasploit.
- The port number that the bundled web server uses for SSL, Apache, and Mongrel access.
- The web server name that the installer uses to generate a self-signed SSL certificate specific to the installed device. The web server name can be any name and does not need to be a fully qualified domain.

The installation process can take between 5-20 minutes to complete.

Installed Programs

The following table describes the applications that the Metasploit installer installs:

Application	Description
Metasploit Web UI	A graphical user interface that provides the easiest way to work with Metasploit Pro, Metasploit Express, and Metasploit Community. Use a web browser, like Firefox, Chrome, or Internet Explorer, to launch the Metasploit Web UI.

Application	Description
Metasploit Console	A command line interface that provides the look and feel of the Metasploit Framework Console, or msfconsole, with the added features of Metasploit Pro. The Metasploit Console provides you with Metasploit Pro commands that you can use to easily perform tasks, social engineering attacks, report generation, and bruteforce attacks.
Framework Console	A command line interface that provides access to the Metasploit Framework. The Framework Console is also referred to as msfconsole. The Framework console provides you with access to modules, which you can use to perform tasks like scans, exploits, SQL injections, and bruteforce attacks.
Framework MSFGUI	A graphical interface that provides you with access to the Metasploit Framework. You can use MSFGUI to easily access modules, plugins, and the database. MSFGUI provides
Armitage	A graphical interface that visually streamlines the features within the Metasploit Framework, such as host discovery, pivoting, client and server side exploitation, and privilege escalation.
Framework IRB	A Ruby interpreter shell that you can use to input Ruby commands and to create Metasploit scripts.

Installer Size

The size of the Windows installer is 90 MB, and the Linux binary files are 80 MB.

Bundled Packages

The installer bundles and includes the following packages:

- Ruby
- Perl
- Python
- Java
- PostgreSQL
- PacketFu
- GNU Public License
- Lesser GNU Public License

- OpenSSL
- SSHkey

Prerequisites and Recommendations

The following sections describe the system requirements and prerequisites that you must meet to install and run Metasploit.

Minimum Hardware, Disk Space, and Memory Requirements

- 2 GHz+ processor
- 2 GB RAM available
- 500MB+ available disk space
- 10/100 Mbps network interface card

Supported Platforms

- Windows XP SP2+, Vista, 7, 2003 Server SP+1, 2008
- Red Hat Enterprise Linux 5.x-x86 and x86_64
- Ubuntu Linux 8.08+

Disabling Antivirus Software

Antivirus software detects Metasploit as malicious and may cause problems with the installation and runtime of Metasploit. Before you install Metasploit, disable any antivirus software that your system uses.

Disabling Firewalls

Local firewalls, including the Windows Firewall, interfere with the operation of exploits and payloads. Please disable the local firewalls before you install or run Metasploit.

Note: If you must use a firewall, you can use the bind connection type for exploits; however, most exploits may still need to receive connections from the target host.

Authorized Usage

You should run Metasploit on machines that you have permission to test on or machines that you own. It is illegal to use this software for criminal activity. Use Metasploit responsibly.

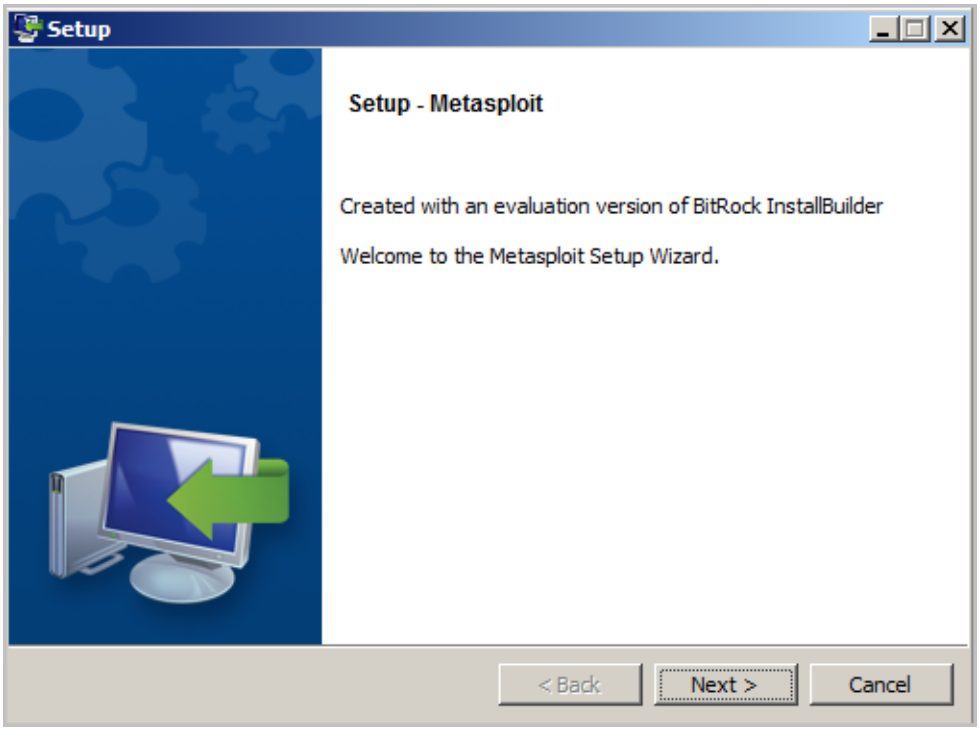
Windows Installation

The following section provides instructions for installing Metasploit on Windows operating systems.

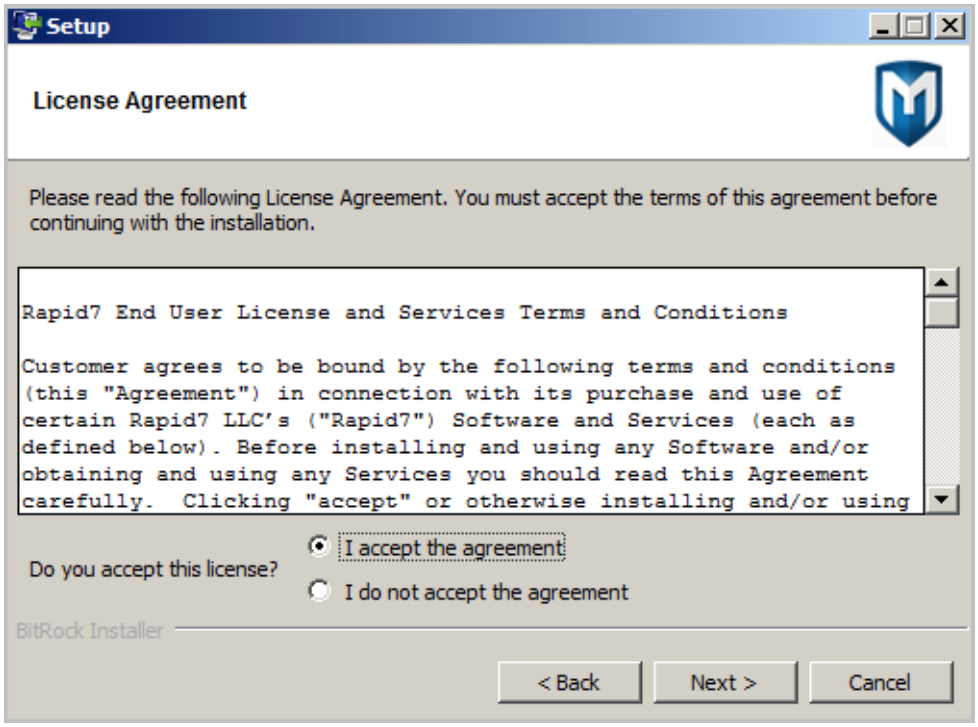
Note: On Windows 7, it can take up to 10 minutes before the installation window appears.

Installing on Windows

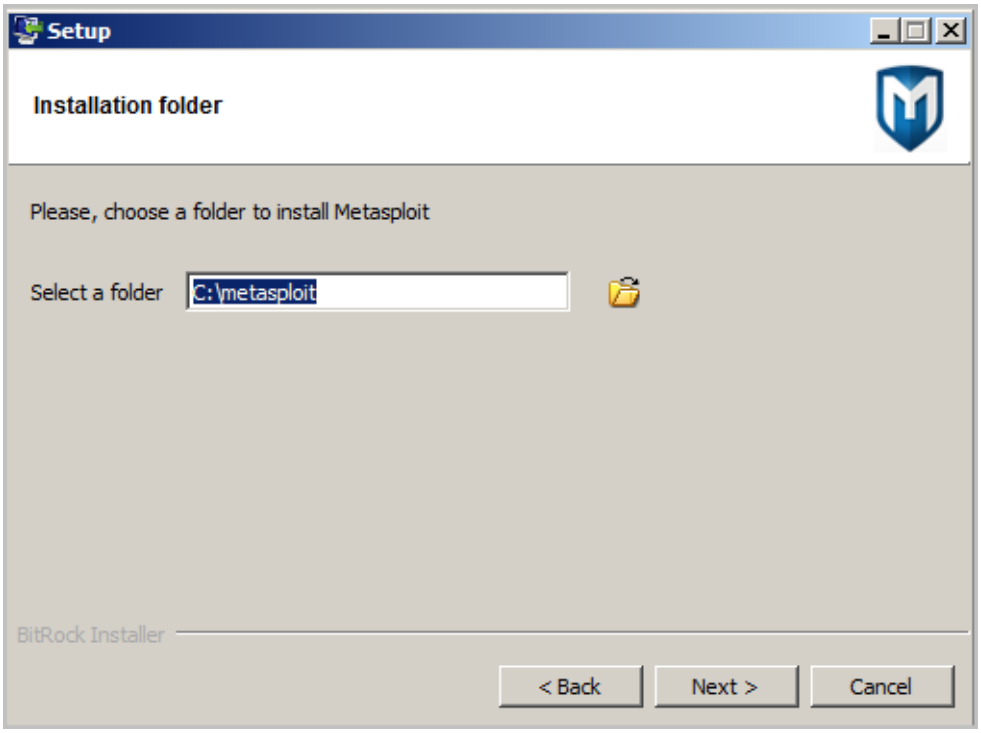
1. Visit http://www.metasploit.com/download/ and download the Windows installer. Save the installer file to a location like the Desktop.
2. Locate the Windows installer file and double-click the installer icon. When you see the security warnings about anti-virus software and firewalls, click **OK**.
3. When the Setup screen appears, click **Next** to continue.



4. Accept the license agreement and click **Next**.



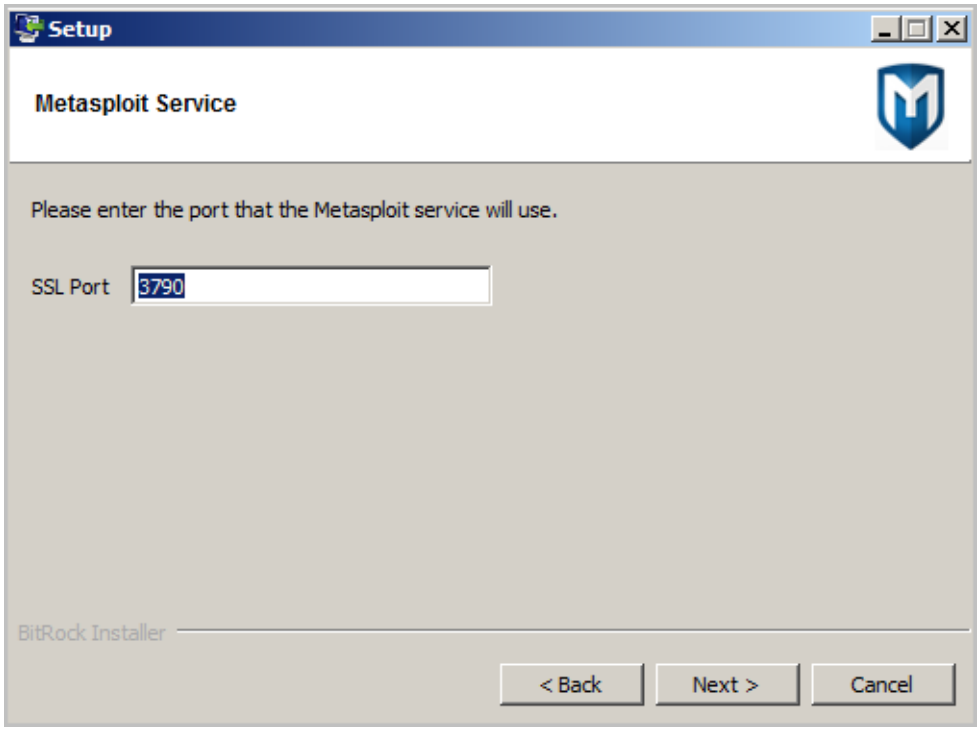
5. On the next screen, you can choose to install Metasploit **i**n the default `c:\metasploit` folder or you can click the folder icon to choose a different directory or hard drive. The directory you choose must be empty.Click **Next** to continue.



6. Enter the SSL Port number that the Metasploit service uses. By default, the Apache

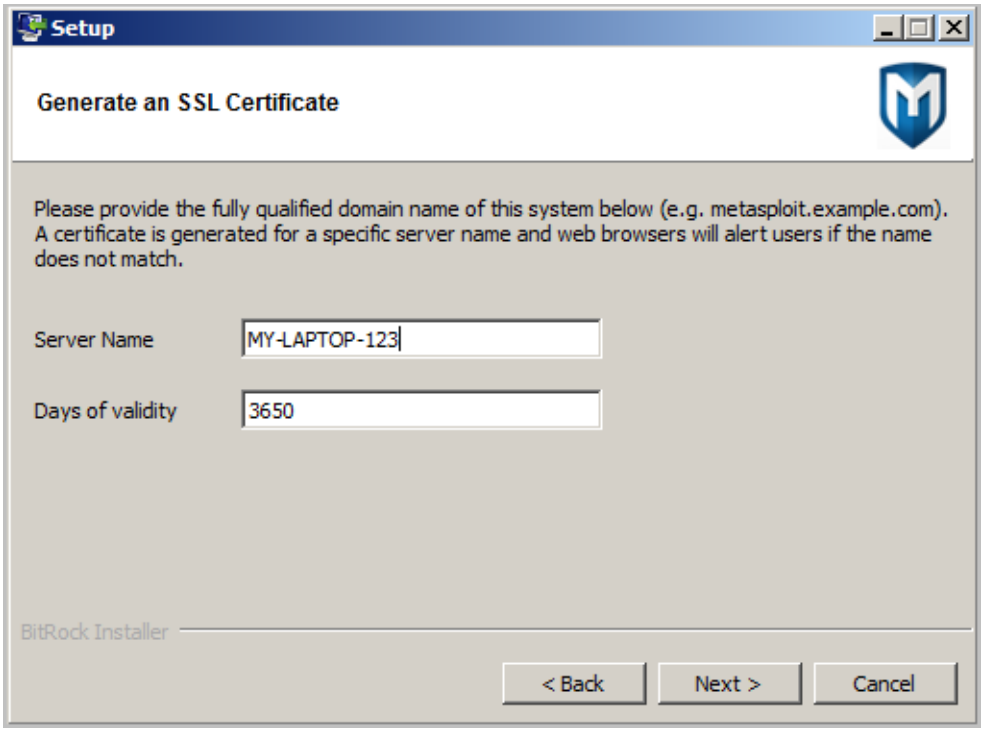
server uses port 3790 for HTTPS. Click **Next** to continue.

Note: If the port is already bound to another process, you will receive an error that states that the installer was unable to bind to the port number. You can use `netstat` to determine if a process is listening on that port and kill the process, or you can enter another port number such as `8080` or `442`. If the suggested port is in use, enter a new port until you resolve the issue.

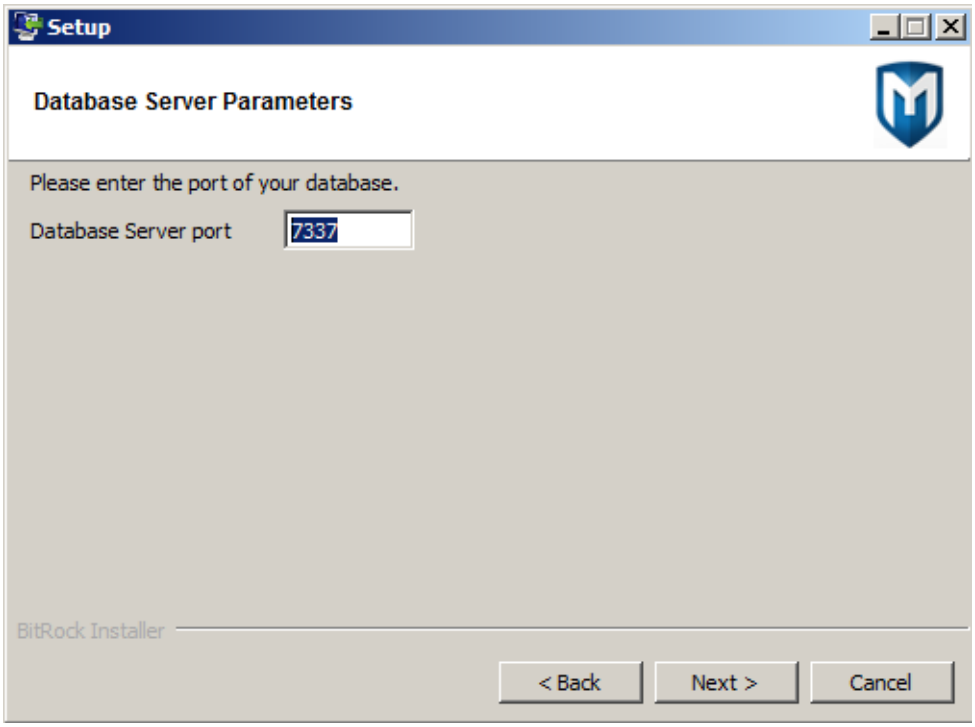


7. Enter the web server name that you want to use to generate the SSL certificate.

This enables the browser to match the information.

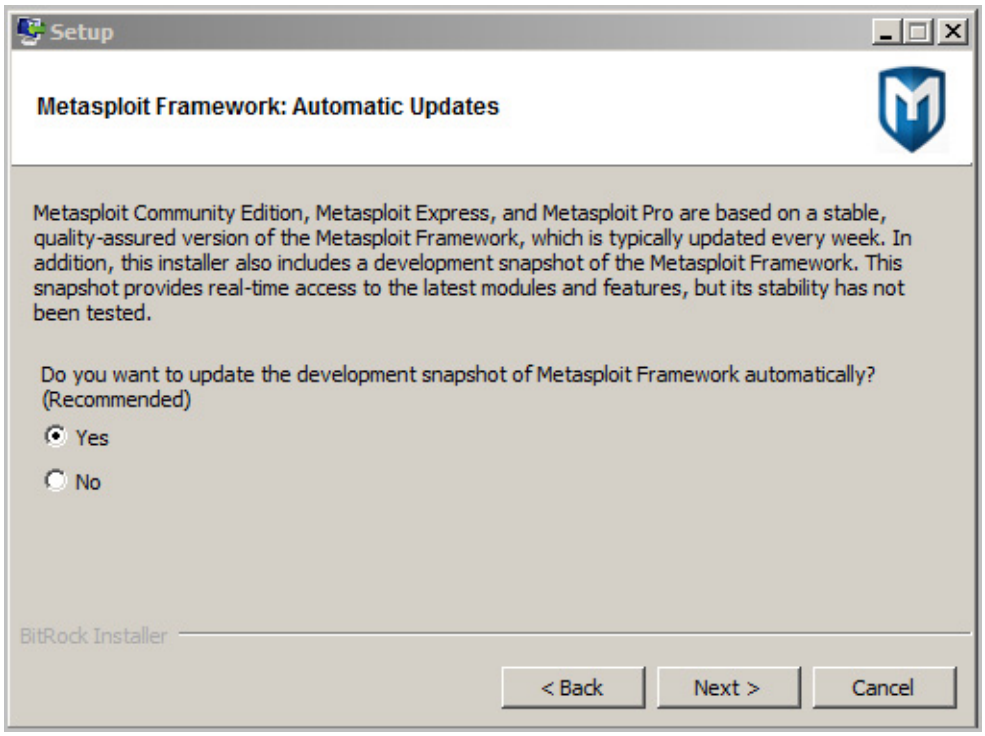


8. Enter the number of days the certificate will be valid in the **Days of validity** field.
9. Enter the port that you want the PostgreSQL database to use. The default server port is 7337. Click **Next** to continue.



10. Enter a port for the Thin server. The default Thin server port is 3001. Click **Next** to continue.

11. Select **Yes** to enable automatic updates for the Metasploit Framework. Click **Next** to continue.



12. The installer is ready to install Metasploit and all its bundled dependencies. Click **Next** to continue.
13. When the installation completes, click the **Finish** button.

After the installation completes, a window appears and prompts you to launch the Metasploit Web UI. At this point, you should launch the Metasploit Web UI to create a user account and to activate your license key. You do not need to restart your system to launch Metasploit for the first time.

Linux Installation

The following sections provide instructions for installing Metasploit on Linux operating systems. Before you install Metasploit, note that the 32-bit installer is not compatible with 64-bit Linux operating systems.

Installing on Linux

1. Visit http://www.metasploit.com/download/ and download the Linux 32 bit or 64 bit installer. Save the installer file to a location like the desktop.
2. Open a terminal.
3. Change the mode of the installer to be executable. To do this, choose one of the options below:

•For 64-bit systems:

```
chmod +x desktop/metasploit-latest-linux-x64-installer.run
```

•For 32-bit systems:

```
chmod +x desktop/metasploit-latest-linux-x32-installer.run
```

4. Run the installer. To do this, choose one of the options below:

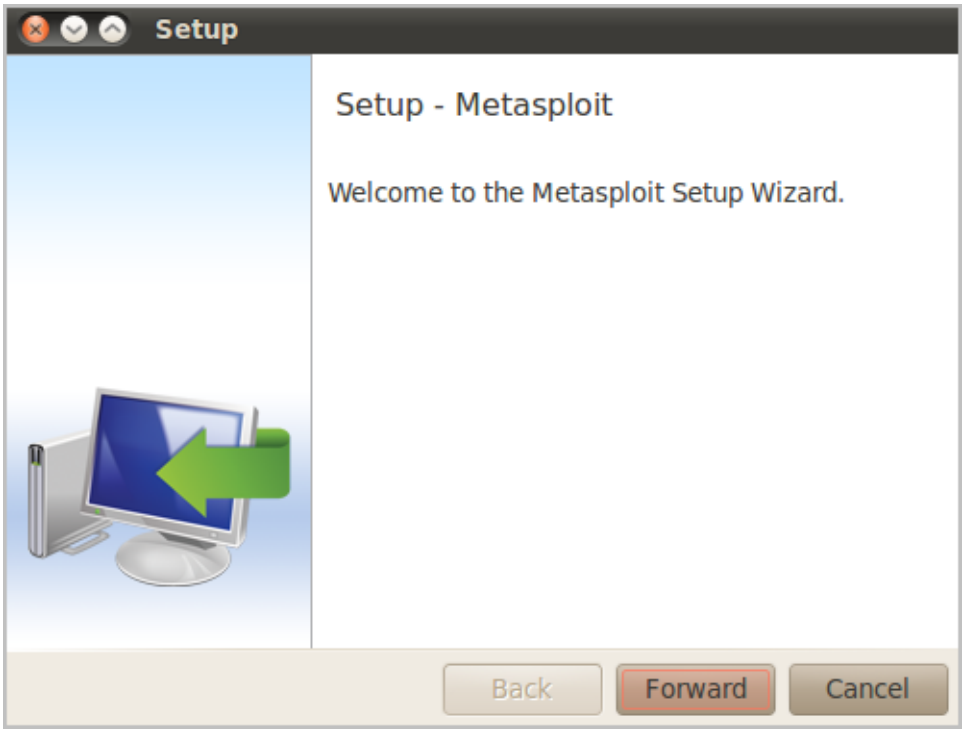
•For 64-bit systems:

```
sudo desktop/metasploit-latest-linux-x64-installer.run
```

•For 32-bit systems:

```
sudo desktop/metasploit-latest-linux-x32-installer.run
```

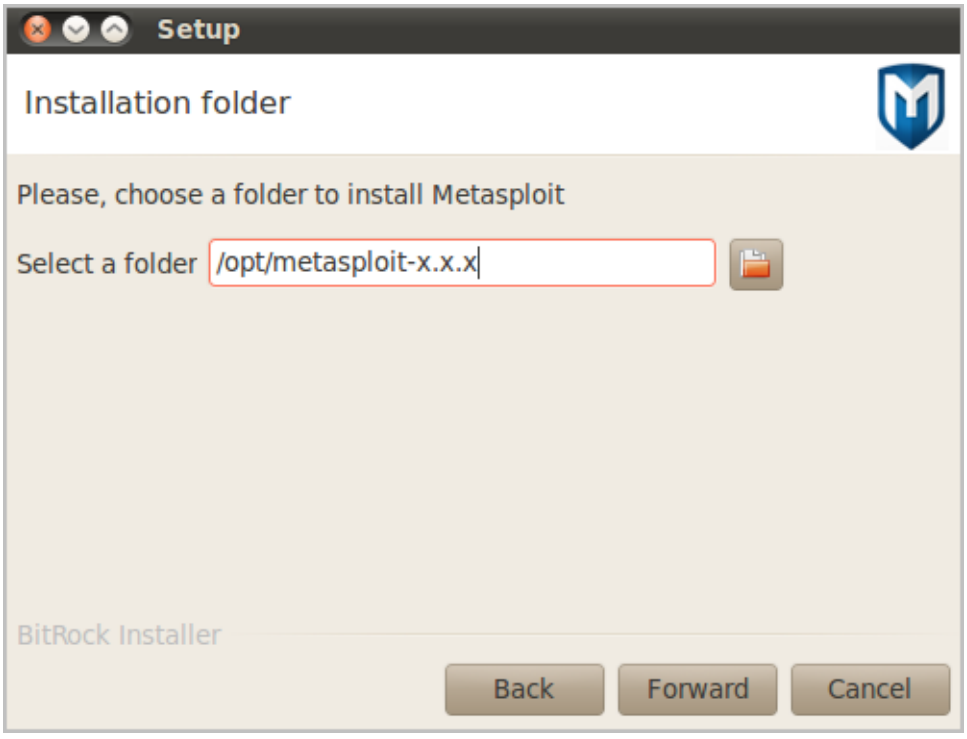
5. If the password prompt appears, enter your sudo password. The setup window appears.



6. Click **Forward** to start the installation process.

7. Accept the license agreement and click **Forward**.

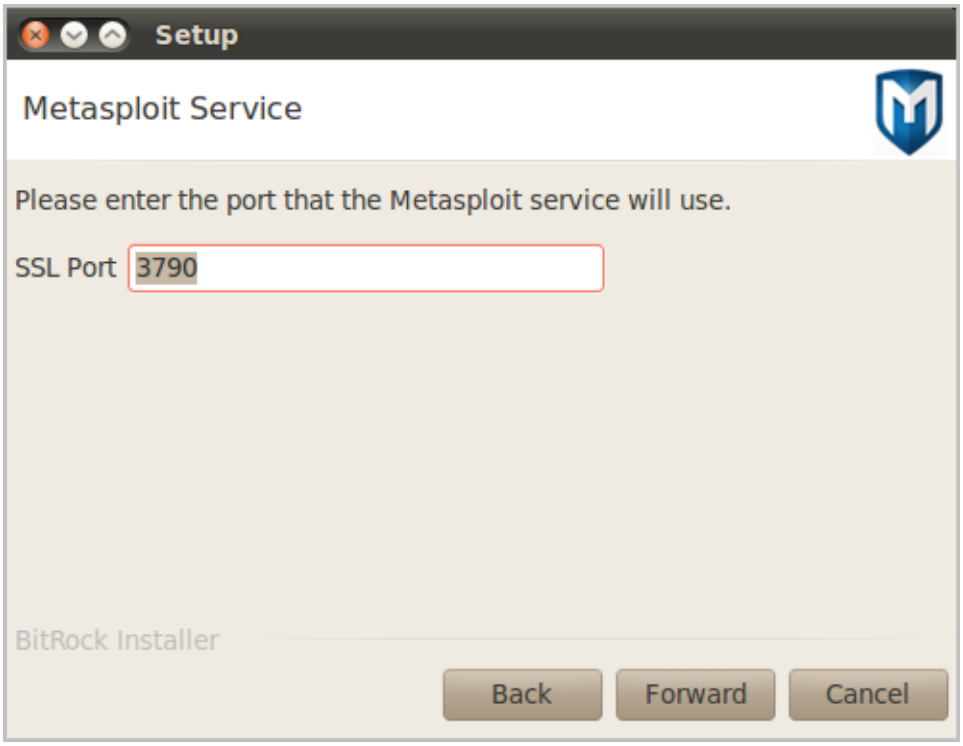
8. Choose an installation folder and click **Forward**.



9. Select **Yes** to register Metasploit as a service (recommended). Click **Forward** to

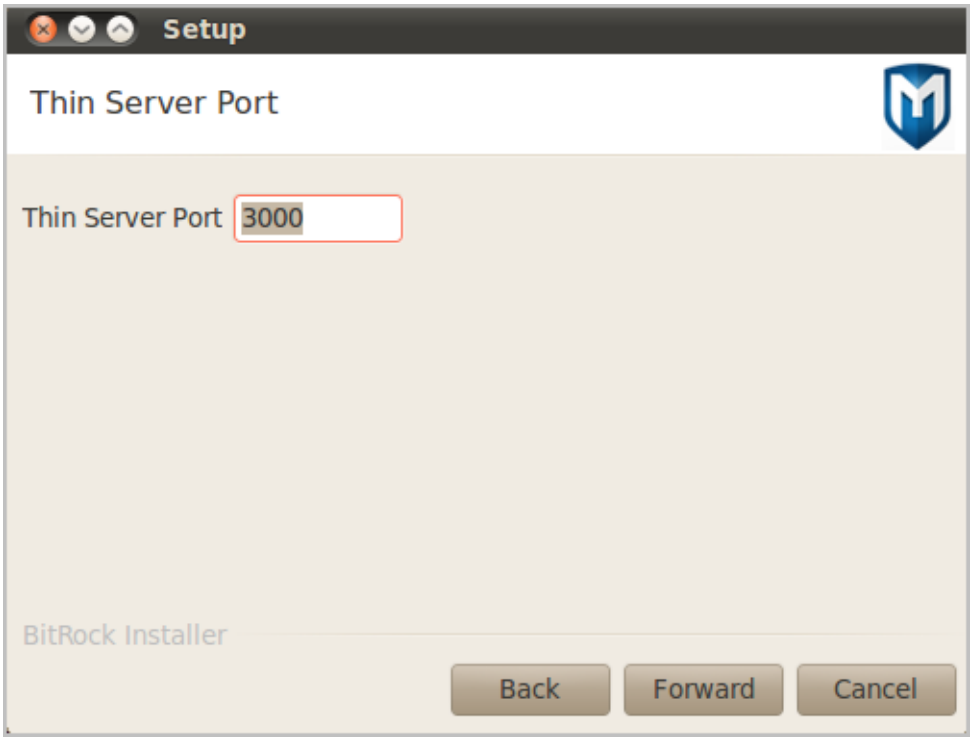
continue.

10. Enter the port number that you want the Metasploit service to use. The default port is 3790. Click **Forward** to continue.

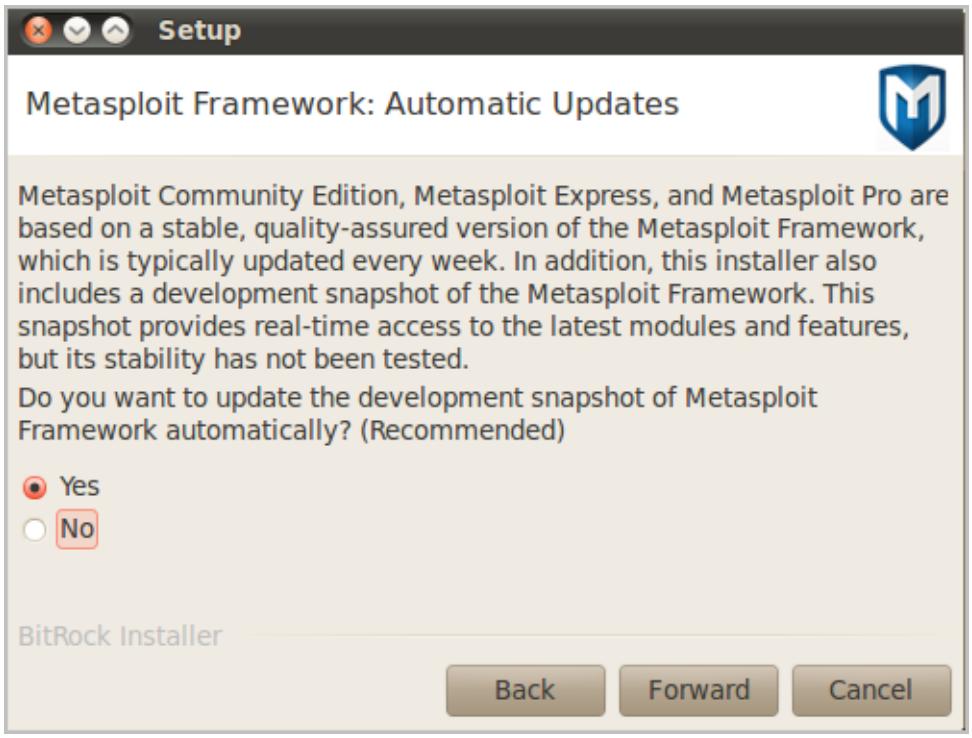


11. Enter the server name that will be used to generate the SSL certificate.

12. Enter the number of days that you want the SSL certificate to remain valid. Click **Forward** to continue.
13. Enter the port for the thin server. By default, this port is 3000. Click **Forward** to continue.



14. Select **Yes** if you want the development snapshot automatically updated. Click Forward to continue.



15. The **Ready to Install** window appears. Click **Forward** to start the installation process.
16. Click **Forward** to continue.

After the installation completes, a window appears and prompts you to launch the Metasploit Web UI. At this point, you should launch the Metasploit Web UI to create a user account and to activate your license key. You do not need to restart your system to launch Metasploit for the first time.

Installing with the Linux Console

If you install Metasploit on a server, such as Ubuntu Server, you need to use the Linux Console to run the Metasploit installation process.

Note: Before you install Metasploit, note that the 32-bit installer is not compatible with 64-bit Linux operating systems.

1. Open the Linux console.
2. Download the installer and save it to your system. To do this, choose one of the options below:

•For 64-bit systems:

```
wget http://downloads.metasploit.com/data/releases/metasploit-
latest-linux-x64-installer.run
```

•For 32-bit systems:

```
wget http://downloads.metasploit.com/data/releases/metasploit-
latest-linux-x32-installer.run
```

3. Change the mode of the installer to be executable. To do this, choose one of the options below:

•For 64-bit systems:

```
chmod +x ./metasploit-latest-linux-x64-installer.run
```

•For 32-bit systems:

```
chmod +x ./metasploit-latest-linux-x32-installer.run
```

Note: If you do not have root privileges, you do need to use sudo. For example, `sudo chmod +x ./metasploit-latest-linux-x64-installer.run`.

4. Run the installer. To do this, choose one of the options below:

•For 64-bit systems:

```
./metasploit-latest-linux-x64-installer.run
```

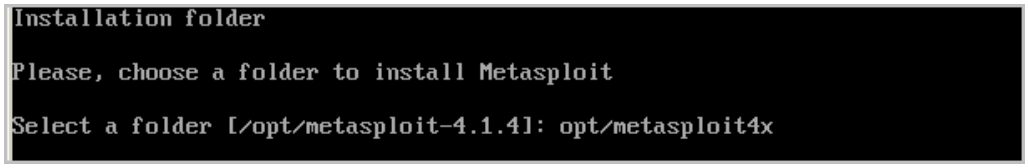
•For 32-bit systems:

```
./metasploit-latest-linux-x32-installer.run
```

Note: If you do not have root privileges, you need to use sudo. For example, `sudo ./metasploit-latest-linux-x64-installer.run`.

5. The Welcome screen appears. Press **Enter** to continue.
6. The License Agreement appears in multiple parts. Read the license agreement and continue to press **Enter** until you read all of the License Agreement.
7. Type `Y` to accept the license agreement and press type y.
8. Enter the folder where you want to install Metasploit. For example, you can enter the default path `/opt/metasploit-4` or enter a different path.
9. Type `Y` to install Metasploit as a service.This adds an init script that calls

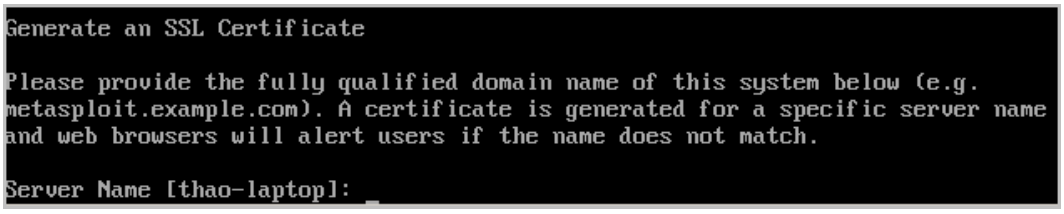
`$INSTALLERBASE/ctlscript.sh`.



10. Enter a port for the Metasploit service. The default port is 3790.

    Note: If there is a conflict during the port configuration, a dialog appears and requests an alternative configuration for the service script, Mongrel server, Postgres database server, or Apache web server to use. The install prompts you to enter another port until the conflict is resolved. The Metasploit Framework can only be installed once on each computer, therefore, you must uninstall the Metasploit Framework before you install an different version.

11. Enter the server name that will be used to generate an SSL certificate, and enter the number of days that the certificate will be valid.



12. Enter the port for the Thin Server. The default Thin Server port is 3000. If you install Metasploit on a server, the installer does not prompt you to enter a port for the Thin Server.

13. Type `Y` to enable automatic updates for the Metasploit Framework.
14. The installer is ready to install Metasploit and all its bundled dependencies. Type `Y` to continue the installation.

To launch the Metasploit web interface to activate your license key, open a web browser and go to `https://localhost:3790` or `https://<IP address>:3790`. If you changed the port that the Metasploit service uses, specify that port instead of the default port 3790.

Creating a User Account

When you initially launch the Metasploit web interface, it will prompt you to create a user account. If you do not have access to a web browser, you can use the createuser script to create a user.

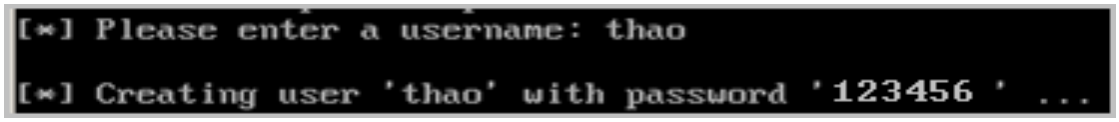
To run this script, enter the following command:

```
./createuser
```

Creating a Password for a User Account

After you create a user, the system returns a password for the user account. Please copy the password. You will need the password to log in to the commercial Metasploit editions.

The following image shows the password that the console returns:



License Key Activation

Activation is the process that validates the authenticity of your license key and determines the Metasploit edition that you can access. If your Metasploit environment has access to the internet, you can activate your license key directly from the Metasploit web interface with the license key provided by Rapid7. If you do not have access to the internet, you must contact Rapid7 for an offline activation key and perform an offline activation.

Online Activation

1. Open Metasploit Pro in a web browser. For example, enter `https://localhost:3790` if you installed Metasploit Pro on your local system or enter `https://<IP address>:3790` if you installed Metasploit Pro in location other than your local system, such as a virtual machine.

   Note: `3790` is the default port that the Metasploit service uses. If you assigned the Metasploit service to a different port during the installation process, use that port instead.

2. If you receive a warning about the trustworthiness of the security certificate, select that you understand the risks and want to continue to the website. The wording that the warning displays depends on the browser that you use.
3. When the web interface for Metasploit Pro appears, the **New User Setup** page displays. Follow the onscreen instructions to create a user account for Metasploit Pro. Save the user account information so that you can use it later to log in to Metasploit Pro.
4. After you create a user account, the **Activate Metasploit** page appears. Enter the license key that you received from Rapid7 in the **Product Key** field.

   Note: If you need to use an HTTP proxy to reach the internet, you can select the HTTP proxy option and provide the information for the HTTP proxy server that you want to use.

5. Activate the license key.

After you activate the license key, the **Projects** page appears. Visit the Metasploit Pro Getting Started Guide for more information on how to create a project.

Offline Activation

To perform an offline activation, you must contact Rapid7 Support for an offline activation key. When you receive the zip file that contains the offline activation key, you save the zip file to a location on your system. You do not need to unzip the contents of the file.

1. Open Metasploit Pro in a web browser. For example, enter `https://localhost:3790` if you installed Metasploit Pro on your local system or enter `https://<IP address>:3790` if you installed Metasploit Pro in location other than your local system, such as a virtual machine.

   Note: `3790` is the default port that the Metasploit service uses. If you assigned the Metasploit service to a different port during the installation process, use that port instead.

2. If you receive a warning about the trustworthiness of the security certificate, select that you understand the risks and want to continue to the website. The wording that the warning displays depends on the browser that you use.
3. When the web interface for Metasploit Pro appears, the **New User Setup** page displays. Follow the onscreen instructions to create a user account for Metasploit Pro.
4. After you create a user account, the **Activate Metasploit** page appears. Locate and click the link to the **Offline Activation** form.
5. Browse to the location of offline activation files.
6. Select the zip file and click **Open**.
7. Activate Metasploit Pro.

After you activate the license key, the **Projects** page appears. Visit the Metasploit Pro Getting Started Guide for more information on how to create a project.