Metasploit Pro
Getting Started Guide
# Table of Contents

## Metasploit Pro

- Getting Started Guide ................................................................. 1
- Welcome ......................................................................................... 4

## Getting Started Guide

- About This Guide ............................................................................ 5
  - Target Audience ........................................................................... 5
  - Organization .................................................................................. 5
  - Document Conventions ................................................................. 5
  - Support .......................................................................................... 5

- Warnings and Precautions ............................................................... 7

- Before You Begin ............................................................................ 8
  - System Requirements .................................................................... 8
  - Supported Operating Systems ...................................................... 8
  - User Accounts .............................................................................. 8
  - Setting Up a Target (Metasploit Vulnerable VMs) ......................... 9
    - System Requirements for Host and Guest Systems ..................... 10
    - Obtaining the Vulnerable VMs .................................................... 11
    - Setting Up the Vulnerable VMs .................................................... 11

## Metasploit Pro Interface Tour

- Navigational Tour .......................................................................... 12
- Projects Page Tour ......................................................................... 13
- Overview Page Tour ...................................................................... 13
- Hosts Page Tour ............................................................................ 14
- Sessions Page Tour ....................................................................... 15
- Campaigns Page Tour .................................................................. 16
- Web Apps Page Tour ..................................................................... 17
- Modules Page Tour ........................................................................ 18
- Reports Page Tour ......................................................................... 19
- Tags Page Tour ............................................................................... 20
- Reports Page Tour ........................................................................ 21
- Task Page Tour ............................................................................. 23

## Getting Started with Metasploit Pro

- Launching Metasploit Pro ............................................................... 24
  - Launching Metasploit Pro in Windows ......................................... 24
Welcome

Metasploit Pro is an easy-to-use penetration testing solution that provides network penetration testing capabilities, backed by the world’s largest fully tested and integrated public database of exploits. Built on feedback from the Metasploit user community, key security experts, and Rapid7 customers, Metasploit Pro enables organizations to take the next step forward in security.

Metasploit Pro was designed for corporate security professionals, security consulting practices, and existing Metasploit users. If you already use the open-source Metasploit Framework to develop and test exploit code, you will appreciate the increased execution and browsing functionality of Metasploit Pro.

In addition to the capabilities offered by the open source framework, Metasploit Pro goes above and beyond by delivering a full graphical user interface, automated exploitation capabilities, complete user action audit logs, customizable reporting, combined with an advanced penetration testing workflow. Metasploit Pro is fully supported by Rapid7 security and support specialists in addition to the large and growing Metasploit community.

Along with the full range of features available in Metasploit Express, Pro offers several additional features that make it a powerful and comprehensive penetration testing tool. Pro features include antivirus evasion, customized reporting, social engineering capabilities, Web application support, VPN Pivoting, and multi-user capabilities.

Metasploit Pro is a part of the Metasploit Project, the open-source penetration testing and development toolset for security professionals. The Metasploit Project was acquired by Rapid7 to continue the open-source community involvement, and to expand the project’s capability and ease-of-use.

Metasploit Pro can be installed on Windows and Linux machines and runs on almost any web browser, or you can continue to use the command line interface.
About This Guide

This Getting Started Guide provides comprehensive information and instructions for Metasploit Pro. The following sections will describe the audience, organization, and conventions used within this guide.

Target Audience

This guide is intended for IT and security professionals who are using Metasploit Pro as their penetration testing solution.

Organization

This guide is divided into the following chapters:

- About This Guide
- Before You Begin
- Getting Started with Metasploit Pro

Document Conventions

The following table lists the conventions and formats used within this guide.

<table>
<thead>
<tr>
<th>Table 1: Document Conventions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conventions</strong></td>
</tr>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td><strong>Code</strong></td>
</tr>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
</tr>
</tbody>
</table>

Support

We are dedicated to delivering superior support for our products. Use the Customer Center to ask questions and get assistance for Metasploit Pro. To log into the Customer Center, you will
need to use the email and password you entered to create your account when you purchased Metasploit Pro.

The Customer Center can be accessed at the URL below:

http://www.rapid7.com/customers/customer-login.jsp
Warnings and Precautions

Before installing Metasploit Pro, please read the following information:

- Antivirus (AV) software such as McAfee, Symantec, and AVG will cause problems with installation and at run-time. You **MUST** disable your AV before installing and using Metasploit Pro.

- Local firewalls, including the Windows Firewall, **MUST** be disabled in order to run exploits successfully. Alternatively, the "bind" connection type may be used, but some exploits still need to receive connections from the target host.

- The RPC service (:50505) on Metasploit Pro runs as ROOT, so any Metasploit Pro account has privileged access to the system on which it runs. In malicious hands, this can lead to system or network damage. Please protect the service accordingly.

- Metasploit Pro is intended only for authorized users. Run Metasploit Pro only on machines you own or have permission to test. Using this software for criminal activity is illegal and could result in jail time.

- Local firewalls, including the Windows Firewall, will need to be disabled in order to run exploits successfully. Alternatively, the "bind" connection type may be used, but some exploits still need to receive connections from the target host.
Before You Begin

Before you get started, you must have Metasploit Pro installed on your system. For more information on installing Metasploit Pro, please see the Metasploit Pro Installation Guide.

System Requirements

- 2 GHz+ processor
- 2 GB RAM available (increase accordingly with VM targets on the same device)
- 500MB+ available disk space
- 10/100 Mbps network interface card

Supported Operating Systems

- Windows XP SP2+
- Windows Vista
- Windows 7
- Windows 2003 Server SP1+
- Windows 2008 Server
- RHEL 5+
- Ubuntu 8.08+

User Accounts

Before you can get started, you will need to create a user account, which will be used to access the system.

The first time you launch Metasploit Pro, you will be prompted to create a new user account. For each instance of Metasploit Pro, you can have up to three user accounts associated with it.

To create a new user:

1. Enter your desired username in the **Username** field.
2. Enter your first and last name in the **Full name** field.
3. Enter a strong password in the **Password** field. Strong passwords are recommended because Metasploit Pro runs as root. Use mixed case, punctuation, numbers, and at least 6 characters. Re-enter the password in the Password confirmation field.
4. Re-enter your password in the **Password** confirmation field.
5. Click **Save Changes**.
Setting Up a Target (Metasploit Vulnerable VMs)

You will need to configure a target network before penetration testing can begin. Rapid7 provides vulnerable virtual machines you can install as a guest system on your local machine for testing purposes. The Metasploitable and UltimateLAMP vulnerable VMs are Ubuntu machines running vulnerable services and containing weak accounts.

The Metasploitable VM focuses on network-layer vulnerabilities, while the UltimateLAMP VM is primarily focused on web vulnerabilities.

If you’re familiar with VMWare and have a workstation or, server already installed, that can be used as a VM host. Alternatively, you can get the free VMWare Player here: http://www.vmware.com/products/player/.

The Metasploitable vulnerable VM runs the following services:

- FTP
- Secure Shell
- Telnet
- DNS
- Apache
- Postgres 8.3
- MySQL
- Tomcat 5.5
- DistCC

The Metasploitable VM also contains a weak system account with the username user and the password user. Several vulnerable applications have been installed on the VM.

The UltimateLAMP VM runs the following services:

- Postfix
- Apache
- MySQL

Additionally UltimateLAMP runs older and vulnerable versions of the following applications:

- Wordpress
- TextPattern
- Sereditpity
- MediaWiki
- TikiWiki
- PHP Gallery
- Moodle
- PHPWebSite
- Joomla
- eGroupWare
- Drupal
- Php Bulletin Board
- Sugar CRM
- Owl
- WebCalendar
- Dot Project
- PhpAdsNew
- Bugzilla
- OsCommerce
- ZenCart
- PhpMyAdmin
- Webmin
- Mutillidae 1.5 (OWASP Top 10 Vulns)

The UltimateLAMP VM’s default credentials are: ‘root’: ‘vmware’. Each application is available by browsing to :80 on the VM’s assigned IP address.

**System Requirements for Host and Guest Systems**

For a typical host system that will run Metasploit Pro and VMware, we recommend a 2GHz or faster processor and a minimum of 3GB of memory.

VMware Player requires approximately 150MB of disk space to install the application on the host, and at least 1GB of disk space is recommended for each guest operating system. For more details on minimum PC requirements, see the VMware Player Documentation.

You must have enough memory to run the host operating system, in addition to the memory required for each guest operating system and the memory required for Metasploit Pro. Please see your guest operating system and application documentation for their memory requirements.

The vulnerable VM requires VMWare 6.5 or above and approximately 1.5GB of disk space to run properly.
Obtaining the Vulnerable VMs

To access and download the UltimateLAMP and Metasploitable VMs, visit http://www.metasploit.com/community/ for the public BitTorrent link. An HTTP download is available from within the customer portal. An up-to-date README file is also available with the VMs.

Setting Up the Vulnerable VMs

You will need to download and install the vulnerable VM in your local machine as a guest system. The virtual device is approximately 600MB and will take about 10 minutes to download on a modern cable connection.

Once the VM is available on your desktop, open the device and run with VMWare Player. Alternatively, you can also use VMWare Workstation or VMWare Server. Once you have a vulnerable machine ready, it’s time to begin your penetration test on Metasploit Pro. You will need to log into your Metasploit Pro account to get started.
Metasploit Pro Interface Tour

The following sections will provide you with a quick tour of the different areas within the user interface.

Navigational Tour

Figure 1: Navigational Overview

There are five main areas of the interface that you can use to navigate through your project:

1. **Main Menu** – The Main menu enables you to manage your project settings, user account settings, and administration duties.

2. **Task Tabs** – The Task tabs enable you to navigate between individual Task pages. Task pages include Hosts, Sessions, Campaigns, Web Apps, Modules, Reports, and Tasks.

3. **Navigational Breadcrumbs** – The navigational breadcrumbs enable you to move between Task pages. Typically, there will be three breadcrumbs listed (Home > Project Name > Task Page). Click on Home to access the Projects page.

4. **Dashboard** – The Dashboard provides you with a graphical breakdown of the services, operating systems and session statuses running on the system. Additionally, you can run any of the main tasks from the Dashboard – including scans, exploits, and campaigns.

5. **Task Panes** – There are four Task panes that will always be visible to you from the Overview page: Discovery, Penetration, Web Apps, and Social Engineering. The Task buttons listed within each Task pane will apply that particular task to the entire project.
Projects Page Tour

To access the Project page, you can either click on the Home link located in the breadcrumbs or you can select Projects > Show All Projects from the Main menu.

The Projects page has several notable areas:

1. **Navigational breadcrumbs** – Use the Home link to access the Projects page.
2. **Projects** – All projects are listed on the Projects page. Simply click on a project name to open it.
3. **Host/Session status** – Quickly view host and session statuses directly on the Projects page.
4. **New project** – All new projects are created through this page.
5. **Settings** – All project settings can be modified through this page; this includes project names, project descriptions, network ranges, and user access.
6. **Delete projects** – Easily delete any unnecessary projects directly from the Projects page.
7. **Global search** – Search for any host in any project to which you have access.

Overview Page Tour

The Overview page for each project is a high-level view of the penetration testing progress. There are shortcuts on the Overview page you can use to initiate or review the basic testing stages for the project. All penetration testing stages - including discovery, penetration, web scanning, and social engineering - can be initiated from this page.
Figure 3: Overview Page

The Overview page includes the following notable areas:

1. **Discovery** – Run a discovery scan, data import, or NeXpose scan directly from the Discovery pane.
2. **Penetration** – Bruteforce or exploit target hosts directly from the Penetration pane.
3. **Web App** – Run a web scan directly from the Web Apps pane.
4. **Social Engineering** – Create a new Campaign from the Web Apps pane.
5. **Recent Events** – Lists a log of recent activity on the system; use the Show link to view more details on the event.

**Hosts Page Tour**

The Hosts page contains a detailed, sortable list of the live hosts that were identified during the scan process.
The **Hosts** page has the following notable areas:

1. **Manage hosts** – Create and delete hosts.
2. **Run scans** – Discover hosts by running a discovery scan, NeXpose scan, Web scan, or by importing your own scan data.
3. **Exploit hosts** – Use bruteforce or automated exploits to gain access to target hosts.
4. **Search** – Use keywords to search for a host.

### Sessions Page Tour

The **Sessions** page lists the open and closed sessions (persistent connections) that were opened during the bruteforce or exploitation of a host. Sessions are also opened when a background module, such as a browser exploit, succeeds in exploiting a client system.
Figure 5: Sessions Page

The Sessions page has the following notable areas:

1. **Collect Evidence** – Collect system data from exploits on target systems.
2. **Cleanup Sessions** – Close any active sessions.
3. **Interact with Sessions** – Click on a session name to view the options for each session. These options will allow you to interact with an active session (e.g., collect system data, access file systems, create Proxy/VPN Pivots, etc.).
4. **View Closed Sessions** – Click on a session name to see its details; this includes the event type and any session data.

**Campaigns Page Tour**

Metasploit Pro organizes social engineering into what are known as Campaigns. These Campaigns provide a way to send client-side attacks and phishing attacks, allowing you to test users and client systems.
Figure 6: Campaigns Page

From the **Campaigns** page, you can perform several actions:

1. **New Campaign** – Create a new Campaign.
2. **Delete Campaign** – Delete existing Campaigns that are no longer necessary.
3. **Campaign details** – Click on the Campaign name to see an overview of the Campaign and click on the Email Template name to see the template used with the Campaign.

**Web Apps Page Tour**

Metasploit Pro provides you with complete visibility and control over the scanning, auditing, and exploitation of active Web applications.
Figure 7: Web Apps

From the **Web Apps** page, you can perform several actions:

1. **Delete applications/websites** – Remove any applications or websites you no longer need.
2. **Perform a Web scan** – Search for any active content or Web forms on target hosts.
3. **Import** – Import data for your Web Apps. Supported file types include:
   - Metasploit PWDump Export
   - Metasploit Zip Export
   - Metasploit XML
   - NeXpose Simple XML
   - NeXpose XML Export
   - NetSparker XML
   - Nessus XML (v1 & v2)
   - Qualys XML
   - Retina XML
   - IP Address List
   - Amap Log
   - Nmap XML
   - Libpcap
4. **Perform a Web Audit** – Search for vulnerabilities on any found active content or Web forms.
5. **Exploit Web Apps** – Run exploits on vulnerabilities found on target systems.

**Modules Page Tour**

The **Modules** page provides a way to search, view, and execute standard auxiliary or exploit modules.
From the **Modules** page, you can perform several actions:

1. **Search for an exploit module, post module, or auxiliary module** – Run a search based on the module’s name, path, platform, type, and other parameters.

2. **Look at totals** - Review statistics about the total number of modules, and the breakdown between exploit vs. auxiliary and server-side vs. client-side modules.

3. **Manually launch an exploit** - Select a module from the list of filtered module search results to configure for a manual attack.

### Reports Page Tour

The Reports page provides a list of live HTML reports and generated reports. The generated reports are static reports that can be exported and saved.
From the **Reports** page, you can:

1. View an instant report - Click a report type from the **Live Reports** section.
2. Create a custom report - Configure and view a live report with specific options by clicking on the **Customized** reports.
3. Create a PDF report or in another format - Click **Generate a Report** and select the **PDF** option or any of the other available formats (XML, Word, ZIP, etc.).
4. Upload a custom report template – You can upload a custom template that references any fields in the database and contains a custom logo, which will be used on every generated report. The custom template must be in JRXML (Jasper) format. For more details on creating a JRXML file, see [http://jasperforge.org/projects/jasperreports](http://jasperforge.org/projects/jasperreports)

**Tags Page Tour**

The **Tags** page provides a list of all current tags and the ability to modify properties of tags.
Figure 10: Tags Page

From the Tags page, you can:

1. Apply changes to your Host Tags – Make your modifications to the Host Tag and then click the **Update** button to apply changes to it.

2. Remove Host Tags – Click the **Delete** button to permanently remove the Host Tag.

3. Modify the attributes for a Host Tag – Choose to include the Host Tag in report summaries, report details, and/or critical findings.

4. Delete hosts from the Host Tag – Deselect hosts to remove them from the Host Tag.

**Reports Page Tour**

The **Reports** page provides a list of live HTML reports and generated reports. The generated reports are static reports that can be exported and saved.
Figure 11: Reports page

From the Reports page, you can:

1. View an instant report - Click a report type from the Live Reports section.
2. Create a PDF report or in another format - Click Generate a Report and select the PDF option or any of the other available formats (XML, Word, ZIP, etc.).
3. Generate a PCI Findings Report – Click Generate PCI Findings to generate an appendix for your penetration test based on PCI standards.
4. Export data from the penetration test – Click Export Data to generate all the data found during the penetration test. Select whether the report will be downloadable as a PDF, XML, RTF, ZIP, PWDump, or Replay file.
5. Download or delete existing reports – Click the Download button to view an existing report or Delete to permanently remove a report from the system.
6. Upload a custom report template – You can upload a custom template that references any fields in the database and contains a custom logo, which will be used on every generated report. The custom template must be in JRXML (Jasper) format. For more details on creating a JRXML file, see http://jasperforge.org/projects/jasperreports
Task Page Tour

The **Tasks** page is a real-time log of user-initiated activities (e.g., discovery, bruteforce, exploit, and cleanup), their completion status, and the duration of completed tasks. There are essentially two Task pages: the main task page that shows a list of the completed and running tasks and the individual task page that shows the detailed progress of a task.

![Individual Task Page](image)

The **Tasks** page has several notable areas:

1. **Task** – Shows the task that Metasploit Pro is currently performing.
2. **Description** – Provides a description of the action Metasploit Pro is performing.
3. **Task bar** – Tracks the progress of the task.
4. **Log** – Shows the log for the running task.
5. **Collect** – Use the **Collect** button to gather information.
6. **Stop** – Use the **Stop** button to stop the task from running.

---

**Figure 12: Individual Task Page**

---

**Metasploit Pro Getting Started Guide 3.6**
Getting Started with Metasploit Pro

The following sections will get you started with Metasploit Pro – this includes walking you through launching Metasploit Pro for the first time and creating your first project. After you have created a project, you should visit the Metasploit Pro User Guide for more information on performing specific tasks.

Launching Metasploit Pro

You can run Metasploit Pro on Windows or in Linux. The following two sections detail how to launch Metasploit Pro in both operating systems.

Launching Metasploit Pro in Windows

To access Metasploit Pro in Windows, navigate to Start > All Programs > Metasploit. To run the Web client, select the application Access Metasploit Pro.

You can manually install, start, stop, and uninstall Metasploit Pro services by using the options under the Metasploit Pro Service subdirectory.

Launching Metasploit Pro in Linux

The Linux installer places a startup script in the root directory of the install - $INSTALLERBASE/ctlscript.sh. This script can be used to start, stop, and check the status of the Metasploit services. Additionally, if you chose to install Metasploit Pro as a service, a symbolic link to the ctlscript.sh script will be placed in the /etc/init.d directory.

To run the web client for Metasploit Pro in Linux, browse to https://localhost:3790 (assuming the default SSL port was chosen).

Creating a Project

A Metasploit Pro Project consists of a name and network boundaries (optional). Network boundaries help you set and maintain scope, which prevent you from targeting devices outside of the range of intended devices and provide a default range for tasks.

Projects can be created when testing different networks or different components of one network. For example, when doing an internal and external penetration test, you may want to create separate projects for each test. This allows you to have separate reports for each test scenario and enables you to perform comparisons between the test results.
Creating a Project

To create a new Project:

1. Click the **New Project** button located at the top of the **Projects** page. To access the **Projects** page, click on the **Home** link (located in the navigational breadcrumbs).

2. Fill in the following fields:
   - Project Name – This can be any name. You can change it later using the **Settings** button located on the **Projects** list page.
   - Network Range – These are the IP addresses that should be used as the defaults for all new tasks.
   - Description – Provide a description for the project.

3. Select the **Project Owner**.

4. Select the members who should have access to the project from the **Project Members** list.

5. Click the **Create Project** button.

Your new project will be added to the bottom of the **Projects** list. To open the project, click on the project name. You are now ready to begin testing.