# Metasploit Pro

User Guide
Release 4.4

RAPID7

# TABLE OF CONTENTS

## About this Guide



## Overview



## Features Overview

## Administration



## Projects

## Discovering Hosts

## Nexpose



## Gaining Access

## Taking Control of a Session



## Application Scanning and Exploitation



## Evidence Collection

## Social Engineering



## Reports

## Task Chains



## FAQs

# About this Guide

This chapter covers the following topics:



## Target Audience

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

## Organization

This guide includes the following chapters:

- About this Guide
- Overview
- Metasploit Pro Tour
- Administration
- Projects
- Discovering Hosts
- Gaining Access
- Taking Control of a Session
- Social Engineering
- Application Scanning and Exploitation
- Evidence Collection
- Reports
- Task Schedules
- Index

# 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.

# Revisions

The following table describes the revisions to this document since the previous release.

| Date Revised | Description |
|---|---|
| 07/17/2012 | Release 4.4: Added a new Nexpose chapter that covers asset groups, vulnerability exceptions, nexpose data scans, and nexpose data import. Updated Social Engineering chapter with new contextual content. Added a new FAQ chapter. |

# Overview

This chapter covers the following topics:



## Product Overview

Metasploit Pro is a penetration testing solution that provides you with access to the largest fully tested and integrated public database of exploits in the world. You can use Metasploit Pro to identify security issues, verify vulnerabilities, and perform real-world security assessments. Metasploit Pro leverages the power and functionality of the Metasploit Framework to provide organizations with an easy-to-use penetration testing tool that takes security testing to the next level.

## Component Overview

The following table describes the components that make up Metasploit Pro:

| Component | Description |
|---|---|
| Metasploit Framework | A penetration testing and development platform that you can use to create security tools and write exploits. It consists of tools, libraries, mix-ins, modules, and multiple interfaces.<br><br>The basic function of the Metasploit Framework is a module launcher that allows you to configure an exploit module and launch the exploit against a target system.<br><br>The Metasploit Framework provides you with access to the modules that you need to use Metasploit Pro. This includes exploit, auxiliary, payload, encoder, and NOP modules. |

| Component | Description |
|---|---|
| Modules | A standalone piece of code, or software, that can extend functionality of the Metasploit Framework. Modules automate the functionality that the Metasploit Framework provides and enables you to perform tasks in Metasploit Pro.<br><br>A module provides the components that a task needs to run. A task can be any action that you perform through the Metasploit Web UI, such as a scan or exploit run. Every task is performed through the use of modules. |
| Projects | The logical component that stores and organizes the tasks that you want to run against a set of targets. You can save projects and rerun them to perform vulnerability verification |
| User Interfaces | Metasploit Pro delivers a graphical user interface through the Web UI or command line automation capabilities through the Metasploit Console.<br><br>The Web UI runs on HTTPS on port 3790. To access the Web UI, go to https://localhost:3790. |

# Service Listeners

The following table lists and describes the service listeners that Metasploit Pro uses to display the Web UI:

| Service Listener | Service | Description |
|---|---|---|
| 0.0.0.0:3790 | NginX | Metasploit Pro utilizes NginX as a front end web server for the Rails UI application. This is the primary service you interact with when you use Metasploit Pro. |
| 127.0.0.1:3001 | Thin Rails Server | Metasploit Pro utilizes Ruby on Rails, and Thin is used as the glue layer between Apache and Rails. |
| 127.0.0.1:7337 | PostgreSQL Database | Metasploit Pro uses PostgreSQL as the host for the Pro datastore. |

| Service Listener | Service | Description |
|---|---|---|
| 127.0.0.1:50505 | Metasploit RPC Service | This service makes it possible to communicate directly with Metasploit Pro through RPC. The Rails UI utilizes RPC on this port to communicate with the Metasploit Pro engine. |

# Supported Bruteforce Targets

The following sections describe the bruteforce targets that Metasploit Pro supports as well as the bruteforce capabilities for each target.

## Windows

The following table describes the bruteforce targets supported by Metasploit Pro on Windows systems:

| Service | Bruteforce Capability |
|---|---|
| SSH | Session |
| Telnet | Session |
| SMB | Session |
| MS SQL | Session |
| MySQL | Crack |
| PostgreSQL | Crack |
| Tomcat | Session |
| DB2 | Crack |
| FTP | Crack |
| Finger | Crack |
| SNMP | Crack |
| VNC | Crack |
| rlogin | Crack |
| RSH | Crack |
| rexec | Crack |

## Linux

The following table describes the bruteforce targets supported by Metasploit Pro on Linux systems:

| Service | Bruteforce Capability |
|---|---|
| SSH | Session |
| Telnet | Session |
| SMB | Session |
| MS SQL | None |
| MySQL | Crack |
| PostgreSQL | Crack |
| Tomcat | Session |
| DB2 | Crack |
| FTP | Crack |
| Finger | Crack |
| SNMP | Crack |
| VNC | Crack |
| rlogin | Session |
| RSH | Session |
| rexec | Session |

## UNIX Systems

The following table describes the bruteforce targets supported by Metasploit Pro on UNIX systems, such as OS X, Solaris, and AIX:

| Service | Bruteforce Capability |
|---|---|
| SSH | Session |
| Telnet | Session |
| SMB | Session |
| MS SQL | None |
| MySQL | Crack |
| PostgreSQL | Crack |

| Service | Bruteforce Capability |
|---|---|
| Tomcat | Session |
| DB2 | Crack |
| FTP | Crack |
| Finger | Crack |
| SNMP | Crack |
| VNC | Crack |
| rlogin | Session |
| RSH | Session |
| rexec | Session |

# Supported Exploit Targets

Metasploit Pro categorizes exploits into four tiers.

The following table describes the tiers and the exploit targets that belong to each tier:

| Tier | Exploit Targets Supported |
|---|---|
| Tier 1 Platform (Windows) | Multitude of exploits are available. 0day regularly released. Meterpreter support. New exploitation research is regularly integrated. |
| Tier 2 Platform (Unix) | Many exploits are available. Some payloads and shellcode are available. |
| Tier 3 Platform (Solaris/OSX) | Some exploits available. Few payloads and shellcode are available. |
| Tier 4 Platform (BDS, AIX, HPUX, Netware) | Few exploits are available. Payloads or shellcode may not be available. |

# Supported Browsers

The Metasploit Web UI runs on the following browsers:

- Google Chrome 8+
- Mozilla Firefox 4+
- Internet Explorer 9+

**Note:** Since Windows XP does not support Internet Explorer 9, Windows XP users must use

Chrome or Firefox to access the Metasploit Web UI.

# Supported Operating Systems

Metasploit Pro runs on the following operating systems:

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

Ubuntu 10.04+

# Support for IPv6 Targets

IPv6 is the latest version of the Internet Protocol designed by the Internet Engineering Task Force to replace the current version of IPv4. The implementation of IPv6 predominantly impacts addressing, routing, security, and services.

An IPv6 address consists of 128 bits and contains eight groups of hexadecimal numbers separated by colons. For example, you can define a full IPv6 address as `fe80:0:0:0:200:f8ff:fe21:67cf`. To save space, you can use a double colon (::) to replace groups of leading zeros. In this example, you can enter `fe80:0:0:0:200:f8ff:fe21:67cf as fe80::200:f8ff:fe21:67cf`.

For more information on IPv6, visit

http://ipv6.com/articles/general/ipv6-the-next-generation-internet.htm.

In Metasploit Pro, you can define IPv6 addresses for target hosts. For example, when you perform a discovery scan, scan a web application, execute a bruteforce attack, or run a module, you can define an IPv6 address for the target hosts. For modules, Metasploit Pro provides several payloads that provide IPv6 support for Windows x86, Linux x86, BSD x86, PHP, and cmd.

**Note:** Metasploit Pro does not support IPv6 for link local broadcast discovery, social engineering, or pivoting. However, you can import IPv6 addresses from a text file or you can manually add them to your project. If you import IPv6 addresses from a text file, you must separate each address with a new line.

# Features Overview

This chapter covers the following topics:



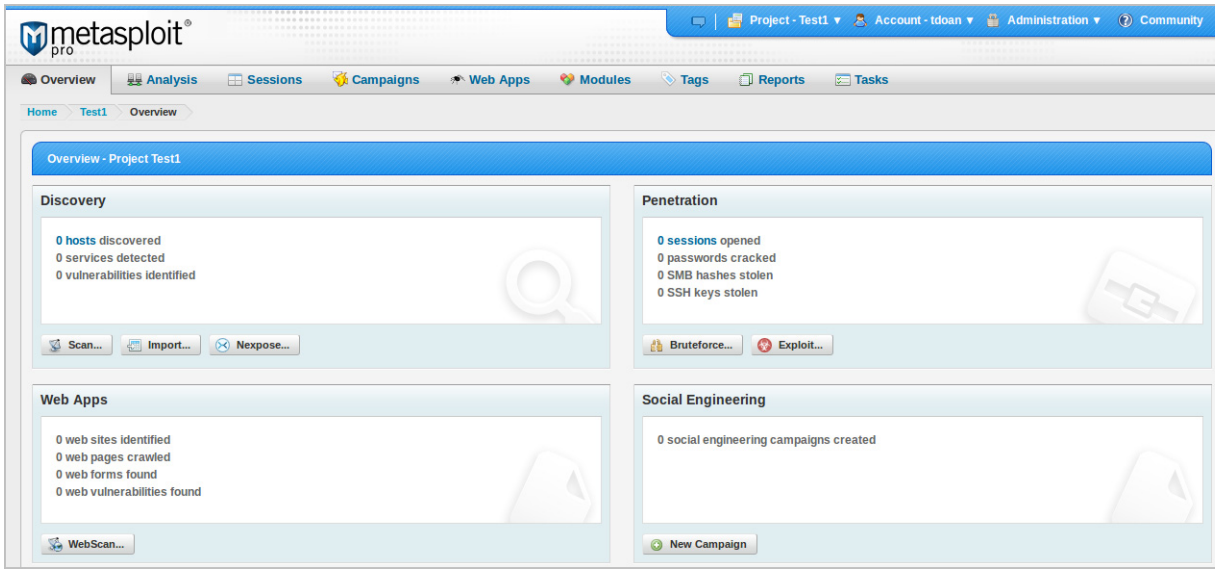
## Features Overview

Metasploit Pro provides a comprehensive and intuitive workspace that you can use to perform administrative tasks and to configure penetration tests.

## The Dashboard

The Dashboard provides a high level overview of the project and shows a numerical and graphical breakdown of discovered hosts, opened sessions, identified web applications, and social engineering campaigns.

The following figure shows the Dashboard:



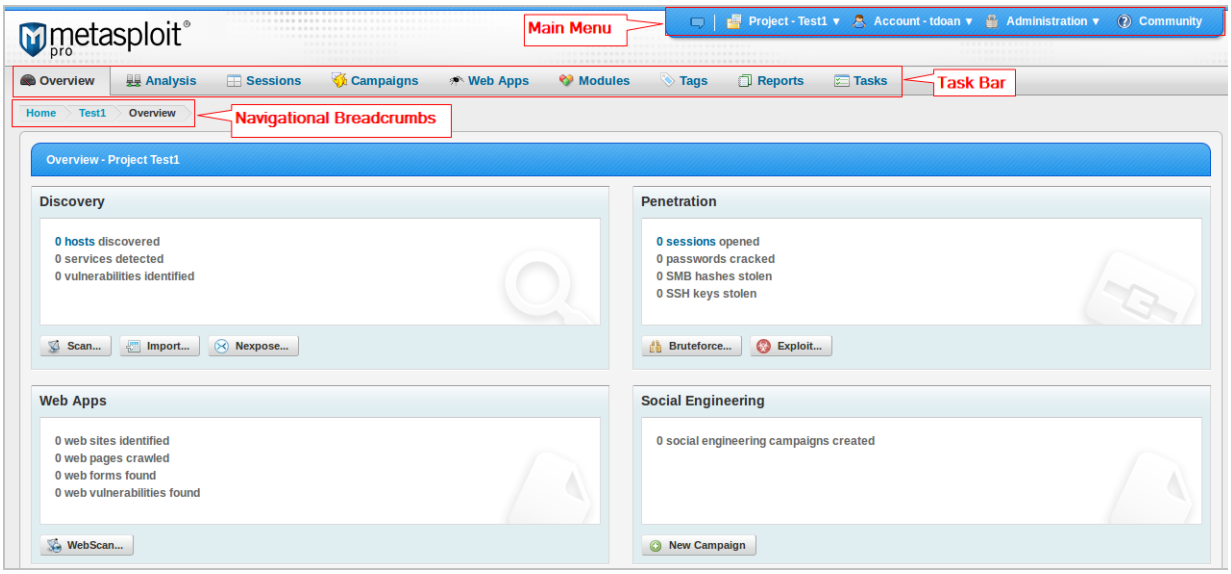
# Navigational Tour

You can use the navigational features to navigate between the different areas of Metasploit Pro.

The following list describes the navigational options:

1. Main menu - Use the main menu to manage project settings, configure user account information, and perform administration tasks.
2. Task bar - Use the task bar to navigate between task pages.
3. Navigational breadcrumbs - Use the navigational breadcrumbs to switch between task pages.
4. Quick tasks - Use the quick tasks to access the task configuration page.

The following figure shows the navigational features:




# Administration Tour

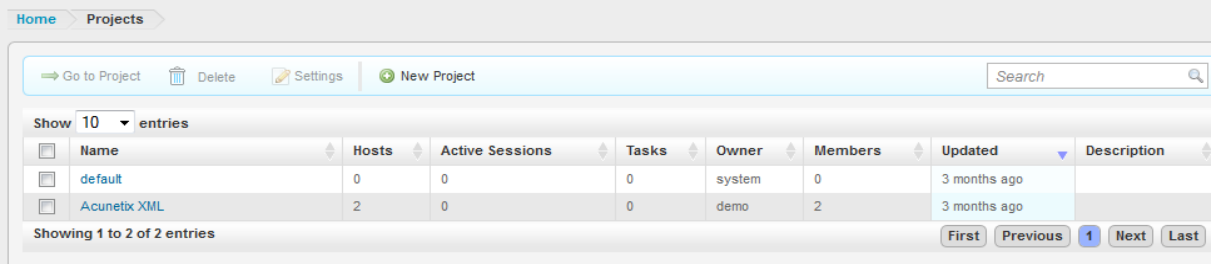
Administrators can perform administrative tasks, like manage projects, accounts, global settings, and software updates, from the main menu.

## Project Management

A Metasploit Pro project contains the penetration test that you want to run. A project defines the target systems, network boundaries, modules, and web campaigns that you want to include in the penetration test. Additionally, within a project, you can use discovery scan to identify target systems and bruteforce to gain access to systems.

Administrators and project owners can manage the users who can view, modify, and run the penetration test.

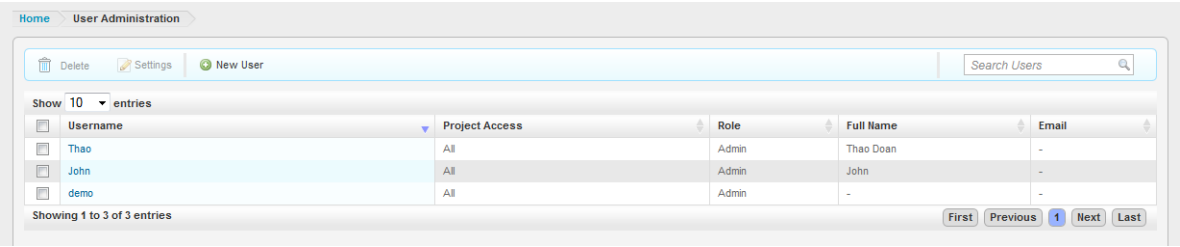
The following figure shows the project management area:




## User Management

Administrators can assign user roles to manage the level of access that the user has to projects and administrative tasks. You can manage user accounts from the Administration menu.

The following figure shows the user management area:



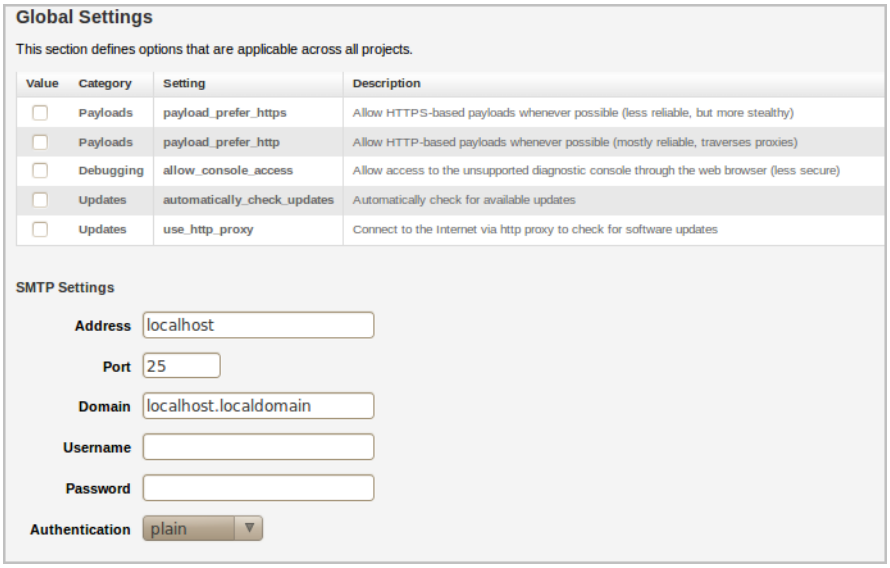

## Global Settings

Global settings define settings that all projects use. You can access global settings from the Administration menu.

From the global settings, you can set the payload type for the modules and enable access to the diagnostic console through a web browser.

Additionally, from global settings, you can create API keys, post-exploitation macros, persistent listeners, and Nexpose Consoles.

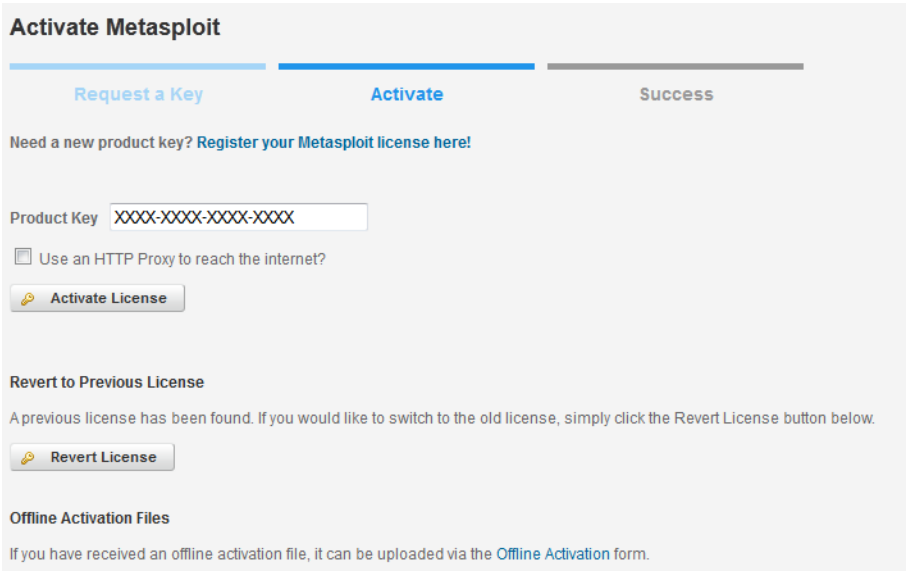
The following figure shows the global settings area:




## System Management

As an administrator, you can update the license key and perform software updates. You can access the system management tools from the Administration menu.

The following figure shows the license key management area:




# Features Tour

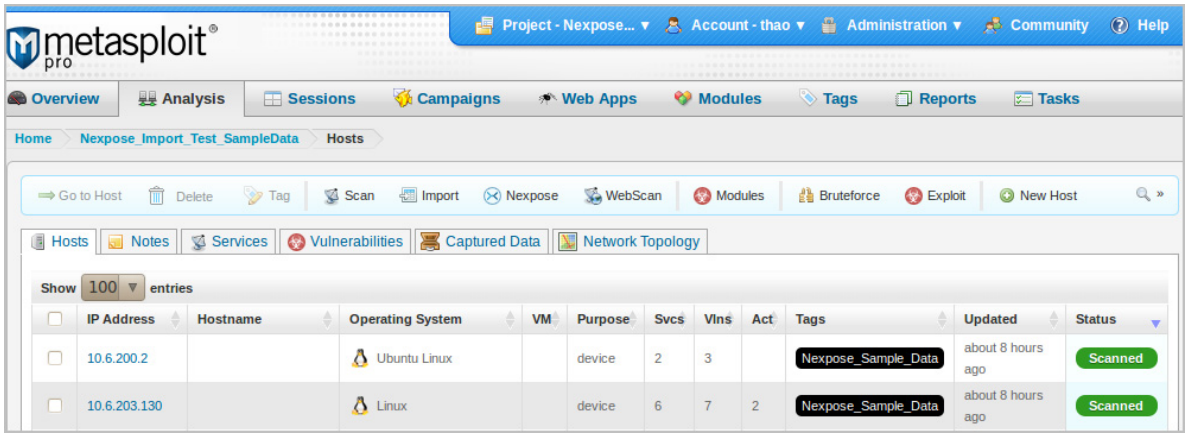
Metasploit Pro provides a comprehensive penetration testing system that you can use to scan for target hosts, open and control sessions, exploit vulnerabilities, and generate reports.

## Host Scan

A host scan identifies vulnerable systems within the target network range that you define. When you perform a scan, Metasploit Pro provides information about the services, vulnerabilities, and captured evidence for hosts that the scan discovers. Additionally, you can add vulnerabilities, notes, tags, and tokens to identified hosts.

You can scan target systems and view discovered host information from the Analysis tab.

The following figure shows the features that you can access from the Analysis tab:




## Bruteforce

Bruteforce uses a large number of user name and password combinations to attempt to gain access to a host. Metasploit Pro provides preset bruteforce profiles that you can use to customize attacks for a specific environment. If you have a list of credentials that you want to use, you can import the credentials into the system.

If a bruteforce is successful, Metasploit Pro opens a session on the target system. You can take control of the session through a command shell or Meterpreter session. If there is an open session, you can collect system data, access the remote file system, pivot attacks and traffic, and run post-exploitation modules.

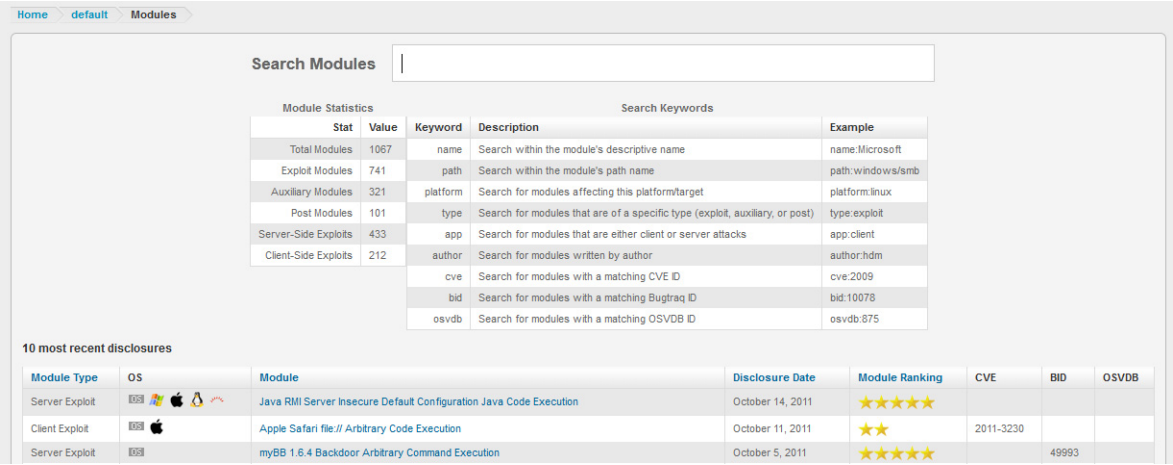
## Exploitation

Modules expose and exploit vulnerabilities and security flaws in target systems. Metasploit Pro offers access to a comprehensive library of exploit modules, auxiliary modules, and post-exploitation modules. You can run automated exploits or manual exploits.

Automated exploitation uses the minimum reliability option to determine the set of exploits to run against the target systems. You cannot select the modules or define evasion options that Metasploit Pro uses.

Manual exploitation provides granular control over the exploits that you run against the target systems. You run one exploit at a time, and you can choose the modules and evasion options that you want to use.

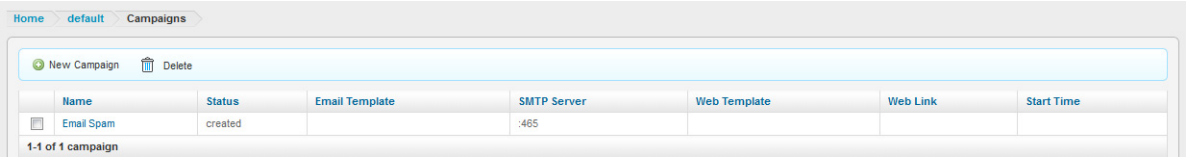
The following figure shows the modules area:




## Social Engineering

Social engineering exploits client-side vulnerabilities. You perform social engineering through a campaign. A campaign uses e-mail to perform phishing attacks against target systems. To create a campaign, you must set up a web server, e-mail account, list of target e-mails, and e-mail template.

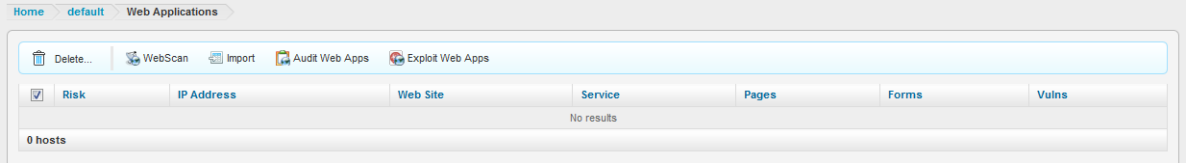
The following figure shows the campaigns area:




## Web Application Scanning

WebScan spiders web pages and applications for active content and forms. If the WebScan identifies active content, you can audit the content for vulnerabilities, and then exploit the vulnerabilities after Metasploit Pro discovers them.

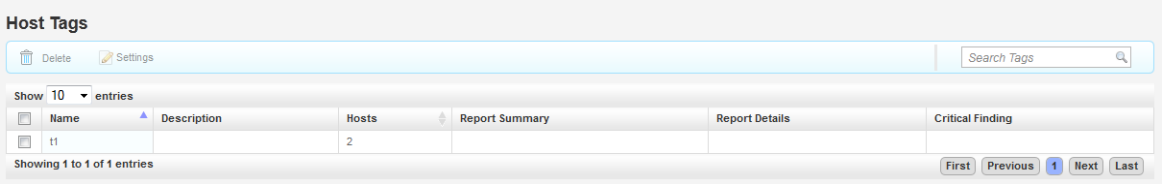
The following figure shows the web application area:



## Host Tagging

Host tags organize assets, create work queues, and track findings for report generation. You can use host tags to assign an identifier with a descriptive message to hosts.

The following figure shows the host tagging area:

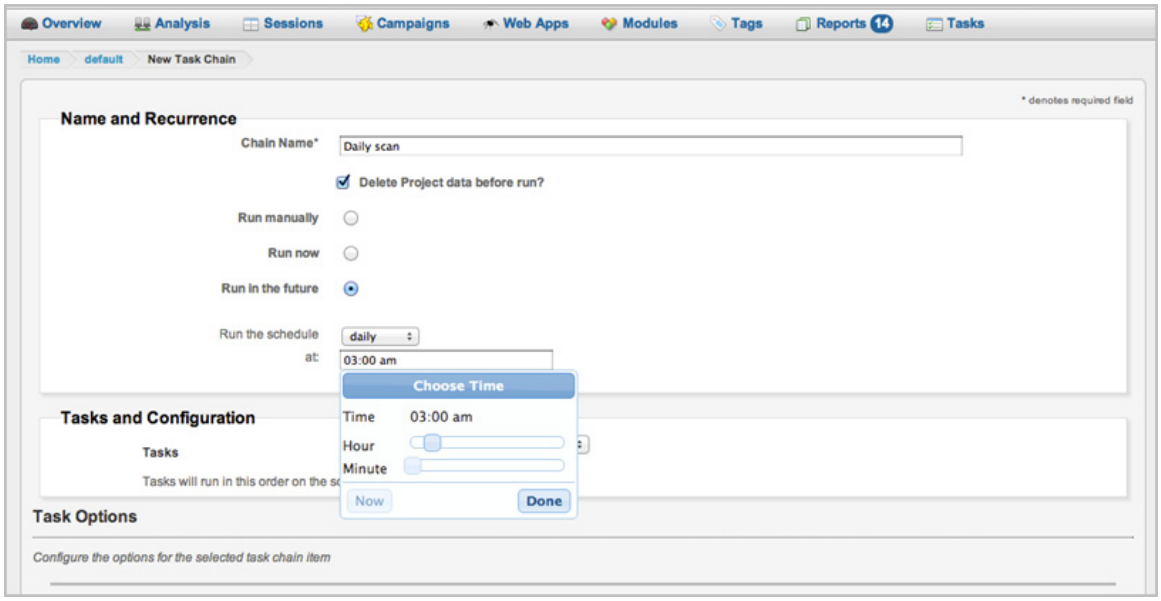



## Task Chains

A task chain is a series of tasks that you can automate to follow a specific schedule. The Metasploit Web UI provides an interface that you can use to set up a task chain and an interactive clock and calendar that you can use to define the schedule.

Use a task chain when you have multiple tasks that you want to run together or when you have a specific time frame that you have to access a target system.

The following figure shows the Task Chains area:




## Reports

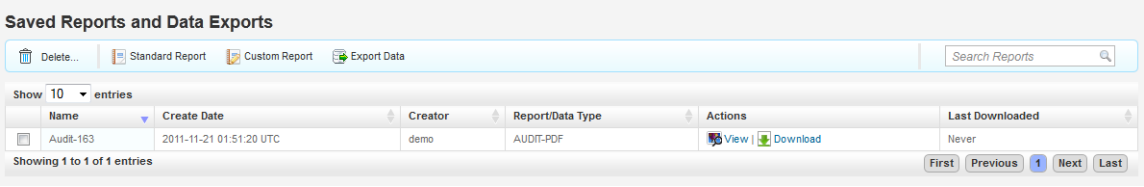
A report provides comprehensive results from a penetration test. Metasploit Pro provides several types of standard reports that range from high level, general overviews to detailed report findings. You can generate a report in PDF, Word, XML, and HTML.

You can use reports to compare findings between different tests or different systems. Reports provide details on compromised hosts, executed modules, cracked passwords, cracked SMB hashes, discovered SSH keys, discovered services, collected evidence, and web campaigns.

Additionally, you can use a custom template to generate a report. A custom template uses customizations that you add to the report.

For example, a custom template can include a company logo. Metasploit Pro provides custom templates, which include the default template, simple template, and Jasper iReport template.

The following figure shows the reports area:



# ADMINISTRATION

This chapter covers the following topics:



## User Account Management

Metasploit Pro allows you to add multiple user accounts to the system. A user account can be a basic user account or an administrator account. A basic user account cannot add, modify, or remove user accounts or configure global settings and network boundaries for the system. An administrator account has unrestricted access to Metasploit Pro features.

### Creating a User Account

1. Click **Administrator > User Administration** from the main menu.
2. Click **New User**.
3. Enter a user name.
4. Enter the first and last name in the **Full Name** field.
5. Enter a password. Use mixed case, punctuation, numbers, and at least six characters to create a strong password. You must create a strong password because Metasploit Pro runs as root.
6. Reenter the password in the **Password Confirmation** field.
7. Select a role for the user. If you do not choose “Administrator,” the default user role is basic.
8. Save the changes to the user account.

### Editing a User Account

1. Click **Account > User Settings** from the main menu.
2. Edit the **Full Name**, **Email**, **Organization**, or **Time Zone** fields for the user account.
3. Save the changes.

### Changing a User Account Password

1. Click **Administration > User Administration** from the main menu.
2. Click the user account that you want to modify.

3. Enter a new password for the user account. Use mixed case, punctuation, numbers, and at least six characters to create a strong password. You must create a strong password because Metasploit Pro runs as root.
4. Reenter the new password.
5. Apply the changes to the password.

## Resetting a User Account Password on Windows

If you forget your Metasploit Pro account password, you can reset the password. The system resets the password to a random value, which you can change after you log back in to Metasploit Pro.

To reset the password, you must be logged in to Windows as a administrator.

1. From the Start menu, choose **All Programs > Metasploit > Password Reset**. The Password Reset window appears. Wait for the environment to load.
2. Type `yes`. The system resets the password to a random value.
3. Copy the password and use the password the next time you log in to Metasploit Pro.
4. Exit the **Password Reset** window.

## Resetting a User Account Password on Linux

1. In the console, execute the following command: `sudo /path/to/metasploit/diagnostic_shell`.
2. Next, `execute /path/to/metasploit/apps/pro/ui/script/resetpw`.
3. Copy the password and use the password the next time you log into Metasploit Pro. You can change the password after you log in to Metasploit Pro.
4. Exit the console.

## Password Criteria

A password must meet the following criteria:

- Contains letters, numbers, and at least one special character.
- Cannot contain the user name.
- Cannot be a common password.
- Cannot use a predictable sequence of characters.

## Deleting a User Account

Users with administrator privileges can delete user accounts.

1. Click **Administration > User Administration** from the main menu.
2. Click the user account that you want to delete.

3. Click **Delete**.
4. Click **OK** to confirm that you want to delete the account.

## Setting the Time Zone

You can set the time zone that Metasploit Pro uses. The time zone is specific to each user account.

1. Click **Account > User Settings** from the main menu.
2. Under Preferences, click the **Time zone** dropdown and choose the time zone that you want to use.
3. Save your changes.

# System Management

Metasploit Pro has a few features that help you determine when updates are available. You can use the Product News panel to see when the Metasploit team has released an update. You can set up an alert that appears when a software update is available. Or you can manually run a check to see if there is an update.

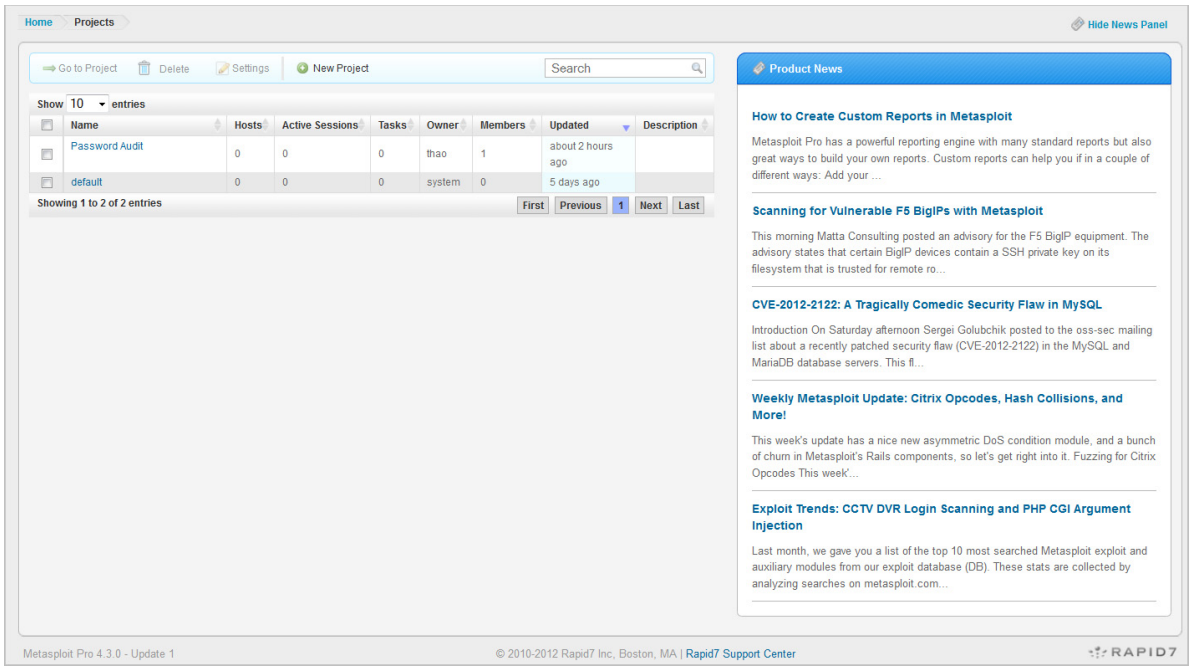
Additionally, as a administrator, you can manage payload settings, mail server settings, API keys, listeners, Nexpose consoles, and Metasploit services. The following sections cover the tasks that help you manage Metasploit Pro.

## Viewing the Latest Product News

The Product News panel shows you the latest blog posts from the Metasploit Community. The Metasploit blog provides you with the latest information from the security community and updates for the Metasploit Framework. To view a blog post, click on the blog title. The blog post will display in a separate browser window.

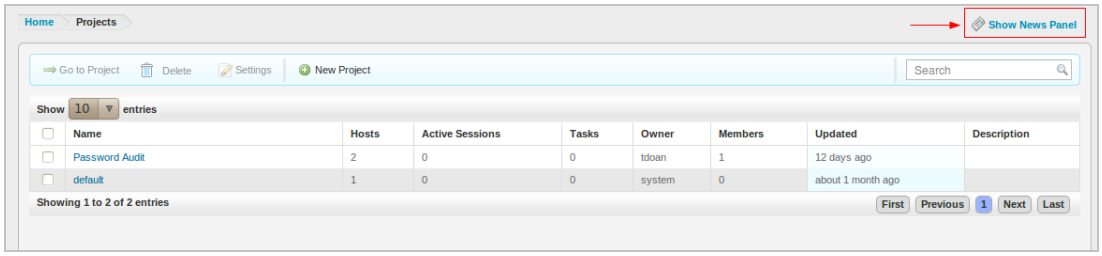
You can access the Product News panel from the project overview page. The Product News panel displays by default; however, you can use the **Hide News Panel** and **Show News Panel** links to control the whether the product news displays or is hidden from view.

The following figure shows the Product News panel:



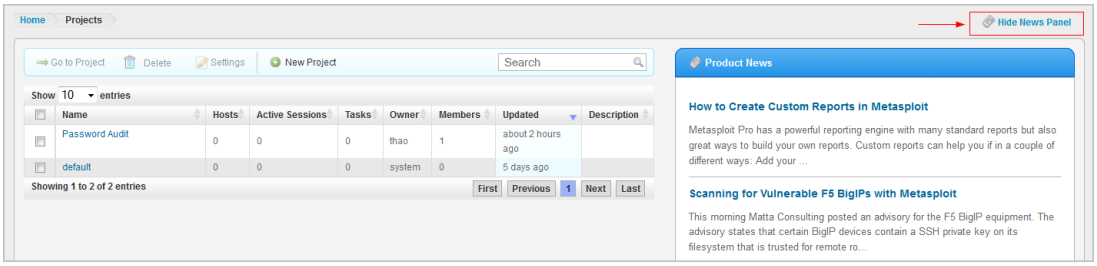

## *Showing the Product News Panel*

1. From the main menu, choose **Project > Show All Projects** to go to the project overview page.
2. Click the **Show News Panel** link.




## *Hiding the Product News Panel*

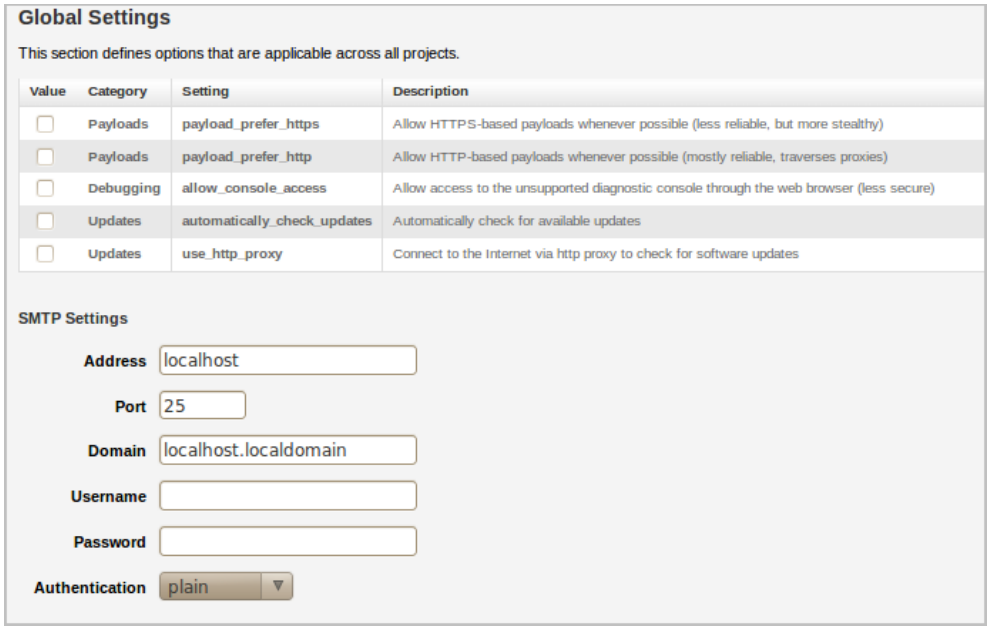
1. From the main menu, choose **Project > Show All Projects** to go to the project overview page.
2. Click the **Hide News Panel** link.



# Configuring Global Settings

Metasploit Pro applies global settings to all projects. Use global settings to set HTTP and HTTPS payloads and to access diagnostic data through a Web browser. Additionally, you can configure an HTTP proxy so that the system can alert you when updates are available for Metasploit Pro.

The following image shows the Global Settings:




## *Setting HTTP Payloads*

1. Select **Administration > Global Settings** from the main menu.
2. Select or deselect **payload_prefer_http** from the Global Settings.
3. Update the settings.

## *Setting HTTPS Payloads*

1. Choose **Administration > Global Settings** from the main menu.
2. Choose **payload_prefer_https** from the Global Settings.
3. Update the settings.

## *Accessing Diagnostic Data*

1. Choose **Administration > Global Settings** from the main menu.
2. Choose **payload_prefer_access** from the Global Settings.
3. Update the settings.

### *Setting Automatic Checks for Updates*

1. Choose **Administration > Global Settings** from the main menu.
2. Choose **automatically_check_updates** from the Global Settings.
3. Update the settings.

### *Setting HTTP Proxy Settings for Update Notifications*

1. Choose **Administration > Global Settings** from the main menu.
2. Choose **use_http_proxy** from the Global Settings.
3. Enter the settings for the HTTP proxy server. You must define the IP address, port, user name, and password for the proxy server.
4. Update the settings. The settings that you define automatically fill the HTTP proxy server settings when you perform an update.

### *Setting the SMTP Settings for a Mail Server*

To send e-mail from Metasploit Pro, you must configure the SMTP settings for the mail server that you want to use. For example, if you have task schedules, and you want to e-mail a report after the schedule runs, you need to set up the SMTP settings so that the system can e-mail the report.

1. Choose **Administration > Global Settings** from the main menu.
2. Under SMTP Settings, define the following fields:

    - Address - The address to the remote mail server.
    - Port - The port that the mail server uses. The default port is 25.
    - Domain - The fully qualified domain name for the sending client.
    - User Name - The user name that the system uses to authenticate the mail server.
    - Password - The password that the system uses to authenticate the mail server.
    - Authentication - The authentication type that the mail server uses. Choose from plain, login, and cram_md5.

3. Update the global settings.

## Managing API Keys

Use API keys to enable remote access to Metasploit Pro over a standard web service. To use API keys, you must generate a token that you use to access Metasploit Pro. The token provides you with administrator privileges. For more information, see the Remote API Guide.

### *Creating API Keys*

1. Select **Administration > Global Settings** from the main menu.
2. Click **Create an API Key**. Metasploit Pro generates the authentication token and automatically populates the **Authentication token** field.
3. Click **Create**.

## Managing License Keys

License keys define the product edition and the registered owner of Metasploit Pro. Metasploit Pro uses the license key to identify the number of days that remain on the license.

### *Updating License Keys*

1. Select **Administration > Software Licenses** from the main menu.
2. Enter the license key in the **Product Key** field.
3. Activate the license.

### *Performing an Offline Activation*

If you do not have network access, use the offline activation file to activate Metasploit Pro. To obtain an offline activation file, contact customer support.

1. Select **Administration > Software Licenses** from the main menu. The **Offline Activation** window appears.
2. Browse to the location of the activation file.
3. Select the activation file.
4. Click **Activate Product** to complete the activation.

### *Reverting to a Previous License Key*

You can revert to a previous license key if Metasploit Pro detects that a previous license key exists on the system. Use license key reversion to switch between different versions of Metasploit products. For example, if you install a trial version of a Metasploit product, use license key reversion to switch back to the full version.

1. Select **Administration > Software Licenses** from the main menu.
2. Click **Change Key**.
3. Click **Revert License**. The **License Details** window appears if Metasploit Pro reverts to the previous version.

## Updating the System

The Metasploit team releases weekly updates that include bug fixes, new modules, and feature enhancements. If you have administrator privileges, you should regularly check for

software updates and apply the updates to the system. This ensures that you have the latest code from the Metasploit Framework and access to the newest modules and features.

### *Updating the System after Installation*

If you recently installed Metasploit Pro, you should immediately check to see if an update is available. The Metasploit installer does not include the latest software updates for the Metasploit Framework. So, if you do not update Metasploit Pro after you install, you may not have the most current code from the Metasploit Framework.

### *Updating the System*

If you are an administrator, you should regularly check for available updates to Metasploit Pro. From the Web UI, Metasploit Pro alerts you when a newer version is available for you to install. If a newer version of Metasploit Pro is not available, the system notifies you that you have the latest version.

1. Click **Administration > Software Updates** from the main menu. The **Software Updates** window appears.
2. Select **Use an HTTP Proxy to reach the internet** if you want to use an HTTP proxy server to check for updates. If you select this option, the proxy settings appear. Configure the settings for the HTTP proxy that you want to use.
3. Check for updates.

After the update completes, Metasploit Pro prompts you to restart the back end services. If you restart the services, Metasploit Pro terminates active sessions and requires up to five minutes to restart.

### *Update Notifications*

If you have Metasploit Pro update alerts enabled, the system will alert you when there is a software update available. The notification appears in the main menu of the Web UI.

The following figure shows the update notification.


### *Maintaining the System*

Metasploit Pro uses log files to store system information.

The log file sizes can become large over time because there is no automatic rotation for log files. To reduce the amount of disk space the log files consume, regularly review and clear log files.

The following table describes the log files that are available:

| Log File | Log File Location |
|---|---|
| Database log | $INSTALL_ROOT/postgres/postgresql.log |
| Web server error log | $INSTALL_ROOT/apache2/logs/error_log |
| Web server access log | $INSTALL_ROOT/apache2/logs/access_log |
| Rails log | $INSTALL_ROOT/apps/pro/ui/log/production.log |
| Rails server log | $INSTALL_ROOT/apps/pro/ui/log/thin.log |
| Metasploit Framework log | $INSTALL_ROOT/apps/pro/engine/config/logs/framework.log |
| Metasploit RPC log | $INSTALL_ROOT/apps/pro/engine/prosvc.log |
| Task log | $INSTALL_ROOT/apps/pro/engine/tasks |
| License log | $INSTALL_ROOT/apps/pro/engine/license.log |

### *Uninstalling Metasploit Pro on Linux*

When you uninstall Metasploit Pro, you remove the Metasploit components and modules from the system and delete the data stored within the projects.

**Note:** Before you uninstall Metasploit Pro, you must stop the active Metasploit services

1. Open the command line terminal.
2. Use the `cd` command to change the directory path to the Metasploit directory. If you installed Metasploit in the default directory, type the following:

```
user@computer:~$ cd /opt/metasploit-4.4.0
```

   Note: Replace the version number with your version number.

3. Type the following to stop all Metasploit services and press **Enter**:

```
user@computer:~/opt/metasploit-4.4.0$ ./ctlscript.sh.stop
```

4. Type the following to uninstall Metasploit and all its components:

```
user@computer~/opt/metasploit-4.4.0$ ./uninstall.
```

5. Click **Yes** to confirm that you want to uninstall Metasploit Pro components and modules.
6. Click **Yes** to confirm that you want to delete the data saved in the projects. If you click **No**, the `$INSTALLER_ROOT/apps` directory remains intact, and you can access

Metasploit Pro data stored in this directory.

### *Uninstalling Metasploit Pro on Windows*

1. Navigate to **Start > All Programs > Metasploit**.
2. Click **Uninstall Metasploit**.
3. Click **Yes** to confirm that you want to delete all saved data from the penetration tests.
4. Click **OK** when the process completes.

### *Restarting the Metasploit Service on Linux*

1. Open the command line terminal.
2. Use the `cd` command to change the directory path to the Metasploit directory location. If you installed Metasploit in the default directory, type the following:

```
user@computer:~$ cd /opt/metasploit-4.4.0
```

   Note: Replace the version number with your Metasploit version.

3. Type the following and press **Enter**:

```
user@computer:/opt/metasploit-4.4.0$ sudo bash ctlscript.sh restart
```

4. Enter your sudo password when the system prompts you for it.

After you enter the sudo password, the system stops and restarts all services associated with Metasploit. This includes prosvc, nginx, and PostgreSQL.

After the system restarts the services, wait a few minutes before you access the Metasploit Web Interface.

### *Restarting the Metasploit Service on Windows*

To restart the Metasploit service on Windows systems, you must stop the Metasploit services before you can start them again. When you stop and start the Metasploit services, a few command line windows appear. These prompts run a control script that stop and start all Metasploit services, which include PostgreSQL, nginx, and prosvc.

This is a two step process.

1. Choose **Start > Programs > Metasploit > Services > Stop Services**.

   Note: If the system prompts you to allow the program to make changes to the computer, click **Yes**.

2. Choose **Start > Programs > Metasploit > Services > Start Services**.

# Project Management

Each project has a name, description, network range, and user access list. A project represents the workspace for your penetration test. Within a project, you can perform tasks like scans and exploits.

A project stores the hosts information and evidence that you have collected. A project provides a clear way for you to create penetration tests for each engagement. Use projects to define the targets that you want to test and to configure tasks for the test.

You want to create multiple projects to test different networks or different components of a single network. For example, if you want to perform an internal and external penetration test, create separate projects for each penetration test.

## Configuring Project Settings

Project settings define the project name, description, network range, and user account access.

### *Defining the Network Range*

When you create a project, you can define optional network boundaries that Metasploit Pro enforces on the penetration test. Use network boundaries to maintain the scope of a project. If you enforce network boundaries, you ensure that you do not target devices outside the range of targeted devices. Additionally, the network range defines the default range that all tasks use.

Administrators and project owners can define the network range for a project.

1. Open the project.
2. Click **Project > Project Settings** from the main menu.
3. Define the network address range.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses. You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0` for a link local address.

4. Update the project.

### *Restricting the Network Range*

Restrict the network range to enforce network boundaries on a project. When you restrict the network range for a project, a user cannot run the penetration test unless the network range for the project falls within network range that you define.

Before you restrict the network range, you must define the network range.

1. Open the project.
2. Click **Project > Project Settings**.
3. Select **Restrict to Network Range**.
4. Update the project.

### *Changing the Project Owner*

Administrators and project owners can change the owner of a project.

1. Open the project.
2. Click **Project > Project Settings** from the main menu.
3. Click the **Project Owner** dropdown to select a project owner.
4. Update the project.

### *Managing User Access for a Project*

Administrators and project owners can specify the users who can view and modify a project.

1. Open the project.
2. Click **Project > Project Settings** from main menu.
3. Select or deselect project members who can view and modify the project.
4. Update the project.

# PROJECTS

This chapter covers the following topics:



## Project Overview

A project is a container for a set of targets and the tasks that perform to test them. You create projects to organize a penetration test. A project represents a workspace that you can use to divide the penetration tests that you create in Metasploit Pro. You may want to create a project for each segment, or subnet, within an organization, to keep track of the areas that you are testing.

## Working with a Project

A project consists of a name, description, and network boundaries. Network boundaries define the scope of the project and ensure that you do not target devices outside of the range of intended devices. You use network boundaries to enforce a default network range for all tasks. You can restrict a project to a single network range or multiple network ranges.

Within a project, you can scan for hosts, open and take control of sessions, and generate reports.

You create a project when you want to test multiple networks or different components of a single network. For example, if you want to perform an internal and external penetration test, you create a separate project for each test. Each project generates a separate report for each test scenario that you can use to compare test results.

### Creating a Project

1. Select **Project > Create New Project** from the main menu.
2. Enter the project name.
3. Enter a description for the project.
4. Define an optional network range. To enter multiple network ranges, use a comma to separate each range.
5. Select **Restrict to network range** if you want to enforce network boundaries on the project.

6. Select the project owner.
7. Select the users who can access, edit, and run the test.
8. Create the project.

## Editing a Project

1. Select **Project > Project Settings** from the main menu.
2. Edit the project name, description, user access, project owner, network range, or network range restriction.
3. Update the project.

## Network Boundaries

Network boundaries define the default network range that the project uses. If you enforce network boundaries, the host scan, bruteforce, exploit, and report tasks must use the network range and cannot target outside the network range that you define.

You can define the network range as a single IP address (10.10.10.1), a CIDR notation (10.10.10.0/16), or a range (10.10.10.1-10.10.10.99).

**Note:** Network boundaries are optional.

### *Setting the Network Boundaries*

1. Open or create a project.
2. Define the network range.
3. Select **Restrict to network range** to enforce the network boundaries.
4. Save the project.

## Showing a List of All Projects

To view a list of all projects, select **Project > Show All Projects** from the main menu.

# Team Collaboration

The multi-user support provides you with the ability to collaborate on an engagement or penetration test with other team members. You and your teammates can log into the same instance of Metasploit to perform tasks, review data, and work on projects. You can access Metasploit Pro through the Metasploit Web UI, which can run on the local machine or across the network.

Some features that you can implement to enhance team collaboration are network boundaries, host tags, and host comments. These features help you create separate

workloads for each team member or organize an engagement into logical containers. For example, you may want to assign certain hosts to a specific team member to test.

## User Access

Each project has a list of users who can access the project. Any person who has access to the project can edit, view, and run tasks from the project. You can manage the user access to control who you want to have access to the information stored within the project.

To add or remove users from the user access list for a project:

1. Open the project.
2. Choose **Project > Project Settings**.
3. Find the **User Access** settings. The user access list displays all available Metasploit Pro users.
4. Select or deselect the users that you want to have access to the project.
5. Update the project.

## Host Tags

Host tags assign an identifier with a descriptive message a host. You can use tags to organize assets, create work queues, and track findings for automatic inclusion into the generated reports.

A tag consists of one word with no spaces, a description, and three flags. The flags indicate whether or not tagged hosts display in the generated report.

To reference a tagged hosts, you can add a pound or hash symbol to the prefix of the tag. Most Metasploit Pro features allow you to use `#tag` instead of an IP address or address range. By using `#tag`, you can easily test a subset of a discovered system.

### *Creating a Tag*

1. Click the **Analysis** tab.
2. Click the host IP address.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses. You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0` for a link local address.

3. Click the **Tags** tab.
4. Enter a name for the tag.
5. Enter a description for the tag.
6. Enable any of the following options: **Include in report summary**, **Include in report details**, and **Critical Finding**.

7. Save the tag.

### *Tagging a Host*

1. Click the **Analysis** tab.
2. Select the host you want to tag.
3. Click **Tag**.
4. Search for the tag you want to use.
5. Click **Tag**.

## Host Comments

You can add a host comment to share information about a host. For example, if you identify a vulnerability on a host, and you want to share that information with other project users, you can add a host comment to that host. When you view the host details, you can see comments that other users have added to the host.

Host comments are visible to all users.

### *Adding Host Comments*

1. Click the **Analysis** tab.
2. Click the host that you want to add a comment to. The host details page appears.
3. Click **Update Comment**.
4. Enter a comment for the host.
5. Save the comment.

# Discovering Hosts

This chapter covers the following topics:



## Discovery Overview

Host discovery is the process that Metasploit Pro uses to identify live valid hosts within a target network address range. You can use the Metasploit Pro discovery scan or Nexpose scan to identify hosts or you can manually add hosts to the system.

## Discovery Scan

A discovery scan queries network services to identify and fingerprint valid hosts. You can perform a discovery scan to identify the details of the hosts within a target address range and to enumerate the listener ports. To perform a discovery scan, you must supply Metasploit Pro with a valid target range.

### IPv6 Addresses for Target Hosts

Metasploit Pro does not automatically detect IPv6 addresses during a discovery scan. For hosts with IPv6 addresses, you must know the individual IP addresses that are in use by the target devices and specify those addresses to Metasploit Pro. To identify individual IPv6 addresses, you can use SNMP, Nmap, or thc-alive6, which is part of the thc-ipv6 tool kit.

After you identify the IPv6 addresses for the target devices, you can either import a text file that contains the host addresses into a project or manually add the hosts to a project. If you choose to import the addresses, the text file that you use must list one IPv6 address on each line.

To import a host address file, select **Analysis > Hosts > Import**. The **Import Data** window appears. Browse to the location of the host address file and import the host address file.

To manually add a host, select **Analysis > Hosts> New Host**.

## Discovery Scan Options

The following table describes the settings that you can configure for a discovery scan:

| Option | Description |
|---|---|
| Target addresses | Defines the target hosts or host range that you want to scan. |
| Perform initial portscan | Performs a portscan before the discovery scan performs service version verification. |
| Custom Nmap arguments | Sends flags and commands to the Nmap executable. Discovery scan supports most Nmap options except for:<br><br>-o<br>-i<br>-resume<br>-script<br>-datadir<br>-stylesheet |
| Additional TCP ports | Appends additional TCP ports to the existing Nmap scan ports. Discovery scan appends the ports to -p. |
| Excluded TCP ports | Excludes the TCP ports from service discovery, which includes all Nmap options. |
| Custom TCP port range | Specifies a range of TCP ports for the discovery scan to use instead of the default ports.<br><br>For example, if you specify ports 1-20, the following Nmap command is returned:<br><br>/nmap -sS - -PS1-20 -PA1-20 -PU51094 -PP -PE -PM -PI -p1-20 --host-timeout=5m -O<br>--max-rtt-timeout=300 --initial-rtt-timeout=100 --max-retries=2 --stats-every 10s --min-rate=200<br><br>Note: UDP Service Discovery or Identify Unknown Services run even if you configure a custom TCP port range. |
| Custom TCP source port | Specifies the TCP source port that the discovery scan uses instead of the default port. Use this option to test firewall rules. |
| Fast detect: Common TCP ports only | Performs a scan on the most common TCP ports, which reduces the number of ports that the discovery scan scans. |

| Option | Description |
|---|---|
| Portscan speed | Controls the Nmap timing option (-T). Choose from the following timing templates::<br><br>**Insane (5) -** Speeds up the scan. Assumes that you are on a fast network and sacrifices accuracy for speed. Scan delay is less than 5 ms.<br>**Aggressive (4)** - Speeds up the scan. Assumes that you are on a fast and reliable network. Scan delay is less than 10 ms.<br>**Normal (3)** - The default portscan speed. Does not affect the scan.<br>**Polite (2)** - Uses less bandwidth and target resources to slow the scan.<br>**Sneaky (1)** - Use this portscan speed for IDS evasion.<br>Paranoid (0) - Use this portscan speed for IDS evasion. |
| Portscan timeout | Determines the amount of time Nmap spends on each host. Default value is 5 minutes. |
| UDP service discovery | Sets the discovery scan to find all services that are on the network. |
| Scan SNMP community strings | Launches a background task that scans for devices that respond to a variety of community strings. |
| Enumerate users via finger | Queries user names when the discovery scan detects fingers. |
| Identify unknown services | Sets the discovery scan to find all unknown services and applications on the network. |
| Single scan: scan hosts individually | Runs a scan on individual hosts. The discovery scan scans the first host entirely and stores the information in the database before it moves onto the next host. |
| Dry run: only show scan information | Prepares the Nmap command line, but does not execute the command line. |
| SMB user name | Defines the user name that the Metasploit SMB enumeration modules use. |
| SMB password | Defines the password that the Metasploit enumeration modules use. |
| SMB domain | Defines the domain that the Metasploit enumeration modules use. |

## Discovering Hosts

1. Create or open a project to run a discovery scan.
2. Click **Scan**. The **New Discovery Scan** window displays.
3. Enter the target addresses that you want to include in the scan. Enter a single address, an address range, or a CIDR notation. If you are entering multiple addresses, use a newline to separate each address.
4. Click **Show Advanced Options** to verify and configure the advanced options for the scan. If you do not configure additional options, Metasploit Pro uses the default configuration for the scan.
5. Run the scan.

## Discovering Virtual Hosts

When you perform a discovery scan, Metasploit Pro automatically discovers guest operating systems on the target system. Metasploit Pro displays a list of virtual machines on the host page and denotes the virtual machine with a VM icon. For example, a machine that runs VMware ESX displays the VMware icon and the guest operating system and version.

Virtualization support enables you to easily differentiate between actual machines and virtual machines. This ability becomes useful when you plan the scope of a penetration test.

### *Supported Guest Operating Systems*

Metasploit Pro supports the following guest operating systems:

- VMware
- Xen
- BreakingPoint
- Virtual PC
- Virtual Iron
- QEMU
- VirtualBox

### *Supported Host VM Servers*

Metasploit Pro supports the following host VM servers:

- VMware ESXi 3.5, 4.0, 4.1, and 5.0
- VMware ESX 1.5, 2.5, 3.0, and 4.0
- vCenter

### *Compromised Virtual Systems*

If you gain access to a target system that a runs virtual environment, Metasploit Pro captures screenshots of the guest operating systems on the host system. To view the screenshots of the guest operating systems, go to **Analysis > Host s > Captured Evidence**. The **Captured Evidence** tab displays a list of looted evidence, such as screenshots from virtual machines.

## Scanning the Network for H.323 Video Conferencing Systems

1. Create or open a project.
2. Click **Scan**.
3. Click **Show Advanced Options**.
4. Enter `1720` for the Custom TCP source port.
5. Clear the **UDP service discovery** option.
6. Select the **Scan H.323 video endpoints** option.
7. Run the scan.

## Defining Nmap Arguments

Administrators can define a list of command line arguments to the Nmap executable for a discovery scan. The command line arguments take precedence over any internal system settings. You can use Nmap arguments to perform custom scan techniques, alternate configurations, and modify scan speeds.

The discovery scan supports most Nmap options except for -o, -i, -resume, -datadir, and -stylesheet.

1. Open a project and launch a discovery scan. The **New Discovery Scan** window appears.
2. Click **Show Advanced Options**.
3. Enter the Nmap arguments in the **Custom Nmap arguments** field.
4. Configure any additional options for the scan.
5. Run the scan.

# Scan and Vulnerability Data

You can import scan data into Metasploit Pro. When you import scan data, you import the hosts, ports, and services that the scan report contains.

## Supported Scan Data Formats

Metasploit Pro supports the following data file formats:

- Metasploit PWDump Export
- PWDump
- Metasploit XML (all versions)
- Metasploit ZIP (all versions)
- NeXpose Simple XML or XML
- NeXpose Raw XML or XML Export
- Foundstone Network Inventory XML
- Microsoft MBSA SecScan XML
- nCircle IP360 (XMLv3 and ASPL)
- NetSparker XML
- Nessus NBE
- Nessus XML (v1 and v2)
- Qualys Asset XML
- Qualys Scan XML
- Burp Session XML
- Acunetix XML
- AppScan XML
- Nmap XML
- Retina XML
- Amap Log
- IP Address List
- Libcap
- Spiceworks Inventory Summary CSV
- Core Impact XML

Raw XML is only available in commercial editions of Nexpose and includes additional vulnerability information.

**Note:** Metasploit Pro does not import service and port information from Qualys Asset files. If you import a Qualys Asset file, you need to run a discovery scan on the imported hosts to enumerate services and ports that are active on those hosts.

## Importing Data

1. Open or create a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click **Import**. The **Import Data** window appears.

4. Click **Browse** to choose a file to import. The **File Upload** window appears.
5. Navigate and choose a file to import. Click **Open** after you select the file.
6. Enter the target addresses that you want to exclude.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses. You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0` for a link local address.

7. Select **Do not change existing hosts** if you do not want the imported information to affect the existing hosts.
8. Select if you want Metasploit Pro to automatically tag hosts with their OS as the system imports them. Enable any additional tags that you want to use.
9. Import the data.

# Host Data

During a scan, Metasploit Pro collects additional host information that you can view from the Analysis page. Metasploit Pro collects information from notes, services, vulnerabilities, and captured evidence.

You can view host data though a grouped view or an individual view. The grouped view shows the information grouped together by service type, vulnerability type, and evidence type. The individual view lists all services, vulnerabilities, and evidence.

## Viewing Host Notes

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the **Notes** tab. A list of all notes appears.

## Viewing Host Services

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the **Services** tab. A list of all services appears.

## Viewing Host Evidence

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the **Captured Evidence** tab. A list of all captured evidence appears.

## Viewing Host Vulnerabilities

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the **Vulnerabilities** tab. A list of all vulnerabilities appears.

# Vulnerability Management

When Metasploit Pro scans target systems, it identifies and fingerprints hosts as well as determines the details of the hosts within a target address range. During the scanning process, Metasploit Pro identifies any known vulnerabilities for the target hosts.

If Metasploit Pro does not identify a known vulnerability during a scan, you can add the vulnerability to a target host.

**Note:** Before you modify or add a vulnerability, you must run a discovery scan for the project.

## Adding a Vulnerability

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click on a host IP address to open the host details window.
4. Click the **Vulnerabilities** tab.
5. Click **New Vuln**. The **New Vuln** window appears.
6. Enter the vulnerability name. For example, `exploit/windows/smb/psexec`.
7. Enter reference information for the vulnerability (CVE identifier, OSVDBID). Use the **Add Reference** button to add a new line of information.
8. Save the vulnerability.

## Exploiting a Known Vulnerability

After Metasploit Pro identifies the vulnerabilities that exist on a host, you can access and run the exploit for each vulnerability directly from the host page. If you want to view more information about the vulnerability, you can click the reference number that Metasploit Pro lists for each vulnerability.

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click on a host IP address to open the host details window.
4. Click the **Vulnerabilities** tab. The tab displays the vulnerabilities for the host.
5. Click the exploit name. The module page appears. Configure the options that you want the exploit to use.

6. Run the exploit.

## Editing a Vulnerability

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the **Vulnerabilities** tab.
4. Locate the vulnerability that you want to edit and click **Edit**.
5. Edit the settings and reference information.
6. Save the changes.

## Deleting a Vulnerability

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click on a host IP address to open the host details page.
4. Click the **Vulnerabilities** tab.
5. Locate the vulnerability that you want to delete and click **Delete**.

# Host Management

You can manually configure a host if there is a host that you want to add to the project. You can configure the details for the host, which includes the network, operating system, and service information. You can also delete any hosts that you no longer need to access for the project.

## Adding a Host

1. Open a project.
2. Click the **Analysis** tab. The **Hosts** window appears.
3. Click **New Host**.
4. Enter a name for the host.
5. Enter an IP address for the host.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses. You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0` for a link local address.

6. Enter an optional Ethernet address for the host.
7. Enter an optional OS system for the host. For example, enter `Windows XP`.

8. Enter an optional OS version for the host. For example, enter `SP2`.
9. Enter an optional OS flavor for the host.
10. Enter an optional purpose for the host. For example, enter `client` or `server`.
11. Select **Lock edited host attributes** if you do not want import, discovery scan, or Nexpose scan to change the host on subsequent scans.
12. Click **Add Service** if you want to add a service to the host. If you add a service, enter the name, port, protocol, and state for the service.
13. Save the host.

### Deleting a Host

1. Open a project.
2. Click the **Analysis** tab. The **Hosts** window appears.
3. Select the hosts that you want to delete.
4. Click **Delete**.
5. Confirm that you want to delete the host.

# Host Tags

Host tags are identifiers that you can use to classify hosts and services. Use host tags if you have hosts and services that exist on different IP ranges. For example, you can tag hosts as servers or Windows hosts.

You can use host tags to provide a descriptive message for a host. Use tags to organize assets, create work queues, and track findings for automatic inclusion in reports. Tags enable you to easily test a subset of a discovered system.

A tag consists of a single word with no spaces and a description. You can assign multiple host tags to a host. You can assign host tags as the scan discovers them or you can add them afterwards.

If you assign a tag to host, you can add a hash or pound symbol to the tag prefix to reference the host. For example, use `#tagName`.

### Adding a Tag

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click on a host IP address to open the host details window.
4. Click the **Tags** tab.
5. Enter a name for the tag.
6. Enter a description for the tag.

7. Choose whether you want to include hosts that use the tag in the report summary, in the report details, or as a critical finding.
8. Save the tag.

## Applying a Tag

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Select the hosts you want to tag.
4. Click **Tag**. The **Tag Hosts** window appears.
5. Enter the name of the tag that you want to use in the search field. Metasploit Pro auto-populates the field with matching results.
6. Select the tag that you want to use.
7. Click **Tag**.

## Updating a Tag

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the host IP address to open the host details window.
4. Click the **Tags** tab.
5. Locate the tag you want to edit.
6. Edit the description and any of the tag attributes.
7. Save the tag.

## Deleting a Tag

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click the host IP address to open the host details window.
4. Click the **Tags** tab.
5. Locate the tag you want to delete and click **Remove**. A confirmation window appears.
6. Click **OK**.
7. Save the tag.

## Automatically Tagging Imported Hosts

Automatic host tagging enables you to tag hosts with their OS type and with custom tags as Metasploit Pro discovers them.

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click **Import**. The **Import Data and Automatic Tagging** window appears.
4. Configure the import options that you want to use. For example, upload the file that you want to use to import hosts.
5. Select if you want to automatically tag hosts with their OS type as Metasploit Pro discovers them.
6. Select the tags that you want to enable for automatic tagging.
7. Import the hosts.

### Automatically Tagging Hosts from Nexpose

Automatic tagging enables you to tag hosts with their OS type and with custom tags as the Nexpose scan discovers them.

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click **Nexpose**. The **Nexpose Scan** window appears.
4. Click **Show Advanced Options**.
5. Select if you want to automatically tag hosts with their OS type as Nexpose discovers them.
6. Select the tags that you want to enable for automatic tagging.
7. Configure any additional options that you would like to define for the Nexpose scan.
8. Launch the scan.

### Automatically Tagging Hosts from Discovery Scan

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click Scan. The Discovery Scan window appears.
4. Click Advanced Options.
5. Select if you want to automatically tag hosts with their OS type as the discovery scan finds them.
6. Select the tags that you want to enable for automatic tagging.
7. Configure any additional options that you would like to define for the scan.
8. Launch the scan.

# Host Badges

A host badge identifies the status of each discovered host. Use the host badge to determine whether Metasploit Pro has scanned, cracked, shelled, or looted the host.

You can view the host badge for a host from the **Status** column on the **Analysis** window.

The following table describes the host badges:

| Host Badge | Description |
|---|---|
| Scanned | The discovery scan discovered the host. |
| Cracked | The bruteforce was successful, but the system could not open a session. |
| Shelled | The system opened a session on the target device. |
| Looted | The system collected evidence from the device. |

# Web Scan

During a web scan, Metasploit Pro spiders web pages and applications to search for active content and forms.

To perform a web scan, you may need to configure the spider settings multiple times before you get the results that you want. Typical applications can take 5,000 or more requests to spider.

## Running a Web Scan

1. Open a project.
2. Click the **Web Apps** tab.
3. Click **WebScan**.
4. Enter a list of URLs for the Web crawler to use.
5. Enter the maximum number of pages that the web scanner requests for each website.
6. Enter the maximum amount of time that the Web crawler spends on each website.
7. Enter the number of concurrent requests that you want to allow per website.
8. Click **Advanced Options**.
9. Define the authentication information that you want to send in each request. For example, define the HTTP user name, HTTP password, HTTP cookie data, and HTTP user agent.
10. Run the scan.

# NEXPOSE

This chapter covers the following topics:



## Nexpose Overview

Vulnerability analysis is the process that detects, identifies, and assesses the vulnerabilities that exist within an organizational infrastructure. A vulnerability is a characteristic of an asset that an attacker can exploit to gain unauthorized access to sensitive data, inject malicious code, or generate a denial of service attack. To prevent security breaches, it is important to identify and remediate security holes and vulnerabilities that can expose an asset to an attack.

Generally, to perform vulnerability analysis, you perform the following steps:

1. Define and classify network or system resources.
2. Identify potential threats for each resource.
3. Prioritize the risks.
4. Develop a plan to remediate the vulnerabilities.

Nexpose automates the steps that you typically use to find and analyze vulnerabilities. Nexpose scans the assets to identify the active services, open ports, and applications that run on each machine. After the scan, Nexpose attempts to identify vulnerabilities that may exist based on the attributes of the known services and applications. Nexpose discloses the results in a scan report, which help you to prioritize vulnerabilities based on risk factor and determine the most effective solution to implement.

### Nexpose Integration with Metasploit

Nexpose integrates with Metasploit Pro to provide a complete vulnerability assessment and verification tool. Metasploit Pro helps you eliminate false positives, verify vulnerabilities, and validate effective remediation measures. You can run a Nexpose scan directly from the Metasploit Web UI or you can import Nexpose scan data into Metasploit Pro.

When you import data from Nexpose into Metasploit Pro, Metasploit Pro automatically indexes the vulnerability data from Nexpose and uses the service and vulnerability reference ID to map each vulnerability to a matching exploit. The mapped exploits helps you to easily launch

attacks against the vulnerability and to quickly determine if the vulnerability is a real risk or a false positive.

In addition to vulnerability scanning, Metasploit Pro provides a vulnerability exception management interface and the ability to create a Nexpose asset group.

### *Working with Nexpose from Metasploit*

You can perform the following Nexpose related task from within Metasploit Pro:

- Run a Nexpose scan.
- Import Nexpose scan data.
- Manage vulnerability exceptions.
- Create asset groups that export to Nexpose.

# Nexpose Scanner

You can use the Community and Enterprise editions of Nexpose to discover and scan assets for known vulnerabilities. After you run a Nexpose scan, you can import the scan data into Metasploit Pro to validate the results of the vulnerability scan.

Metasploit Pro provides a connector that allows you to run and automatically import the results of a Nexpose scan into a project. In order to run a Nexpose scan from Metasploit Pro, you must configure a Nexpose Console for the system to use.

Metasploit Pro only supports the number of hosts that you have licenses for in Nexpose. If you provide more hosts than the number of licenses that you have available, the scan fails. For example, if you have a Community license, the most number of hosts Nexpose supports is 32. If you provide 35 hosts, the scan fails.

You can download the Community edition of Nexpose from http://www.rapid7.com/vulnerability-scanner.jsp. For more information on how to install and configure Nexpose, visit http://community.rapid7.com.

## Configuring a Nexpose Console

Before you can run a Nexpose scan, you must add a Nexpose Console to the system. You can manage Nexpose consoles globally. Connections to the Nexpose Console act as a persistent connections that you can use to import individual assets into a project.

After you set up the Nexpose Console, you can access the console to perform a Nexpose scan. Nexpose consoles are global components and are available to all projects.

1. Open a project.
2. Click **Administration > Global Settings** from the main menu.

3. Scroll down to the Nexpose Consoles area.
4. Click **Configure a Nexpose Console**.
5. Enter a console name.
6. Enter the console address. For example, if Nexpose runs on the local system, you can use 127.0.0.1.
7. Enter the console port. By default, Nexpose runs on port 3780.
8. Enter the user name that you use to log in to the Nexpose Console.
9. Enter the password that you use to log in to the Nexpose Console.
10. Save the Nexpose Console configuration.

## Running a Nexpose Scan

1. Open a project.
2. Click the **Analysis** tab.
3. Click **Nexpose** from the Quick Tasks menu.
4. Select a Nexpose Console. The list shows Nexpose consoles that you have added to the project.
5. Enter the addresses for the scan targets. You can specify an IP address or a host name. There can be one address on each line.

   Note: You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0` for a link local address.
6. Select a scan template.
7. Click **Show Advanced Options** to configure additional options for the scan.
8. Launch the Nexpose scan.

### *Nexpose Scan Options*

The following table describes the settings that you can configure for a discovery scan:

| Option | Description |
|---|---|
| Nexpose scan targets | Defines the IP addresses that you want to scan. |
| Scan Template: Penetration Test Audit | Uses safe checks to perform an in-depth penetration test of the target systems. Enables host discovery and network penetration options, which allows Nexpose to dynamically discover additional systems in the target network. |

| Option | Description |
|---|---|
| Scan Template: Full Audit | Uses safe checks to perform a full network audit of all target systems. The network audit includes network-based vulnerability checks, patch/hot fix checks, and application layer audits. The Full Audit scan only scans default ports. Policy checking is disabled, which makes the Full Audit scan perform faster than the Exhaustive scan. |
| Scan Template: Exhaustive Audit | Uses safe checks to perform an exhaustive network audit of all target systems and services. The network audit includes network-based vulnerability checks, patch/hot fix checks, and application layer audits. An Depending on the number of target hosts, an Exhaustive scan can take several hours or days to complete. |
| Scan Template: Discovery | Identifies live devices on the network, which includes the host name and operating system for each host. The Discover scan does not perform any additional enumeration or policy/vulnerability scanning. |
| Scan Template: Aggressive Discovery | Performs a fast and cursory scan to identify live devices on high speed networks. The discovery scan identifies the host name and operating system for each host. The discovery scan sends packets at a high rate, which may trigger IPS and IDS sensors, SYN flood protection, and exhaust states on stateful firewalls. The Aggressive Discovery scan does not perform any additional enumeration or policy/ vulnerability scanning. |
| Scan Template: DoS Audit | Uses safe and unsafe checks to perform a basic audit of all target systems. The DoS Audit scan does not perform any additional enumeration or policy/ vulnerability scanning. |
| Purge scan results upon completion | Removes the results from the scan from the Nexpose Console after the scan completes. |
| Specify additional scan credentials | Defines the credentials that the Nexpose scan uses. Multiple credentials are not supported. You must use Nexpose to configure multiple credential support. |
| Pass the LM/NTLM hash credentials | Enables a Nexpose scan to use the password hashes that Metasploit Pro collects to authenticate against the host. |

| Option | Description |
|---|---|
| Hash credentials | Defines the hash credentials that you want to use to authenticate against a target. The hash credentials are populated with the hash values that Metasploit Pro collects from the target. If you need to modify the hash list, use the following format to add or modify hash credentials: `<user name>:LM:NTLM`. |
| Type | Use Windows/CIFS, Secure Shell/SSH, Telnet, HTTP, FTP, SNMP, or POP3. This option appears if you select that you want to specify additional scan credentials. |
| User | Defines the user name for the scan credentials. This option appears if you select that you want to specify additional scan credentials. |
| Password | Defines the password for the scan credentials. This option appears if you select that you want to specify additional scan credentials. |

## Running a Nexpose Scan with a Custom Scan Template

To use a custom scan template for a Nexpose scan, you must supply the scan template ID, not the scan template name. To identify the scan template ID, log into the Nexpose Security Console, select **Administration > Scan Templates**, and choose the scan template that you want to use.

When the **Scan Template Configuration** page displays, locate the URL address box at the top of the Nexpose Console. The URL address box displays the address and the template ID for the scan template. For example, in the following address, https://my.console.address:3780/admin/wizard/scan-template.html?templateid=dos-audit, the template id is `dos-audit`.

For more information on scan template IDs, visit the Nexpose documentation.

1. Open a project.
2. Click the **Analysis** tab.
3. Click **Nexpose** from the Quick Tasks menu.
4. Select a Nexpose Console. The list shows Nexpose consoles that you have added to the project.
5. Enter the addresses for the scan targets. You can specify an IP address or a host name. There can be one address on each line.

   Note: You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0`

for a link local address.

6. Click the Scan Template list. Choose **Custom**, which enables you to select a custom scan template.
7. Click **Show Advanced Options**.
8. From the **Advanced Nexpose Scan Settings** area, enter the scan ID for the that you want to use in the **Custom scan template name** field.

   Note: Scan template IDs cannot contain a hyphen. If the scan template ID contains a hyphen, replace the hyphen with an underscore. If the scan template ID changes, the Nexpose scan does not update the scan template ID. You must update the Nexpose scan to use the new scan template ID.

9. Launch the Nexpose scan.

## Nexpose Asset Tags

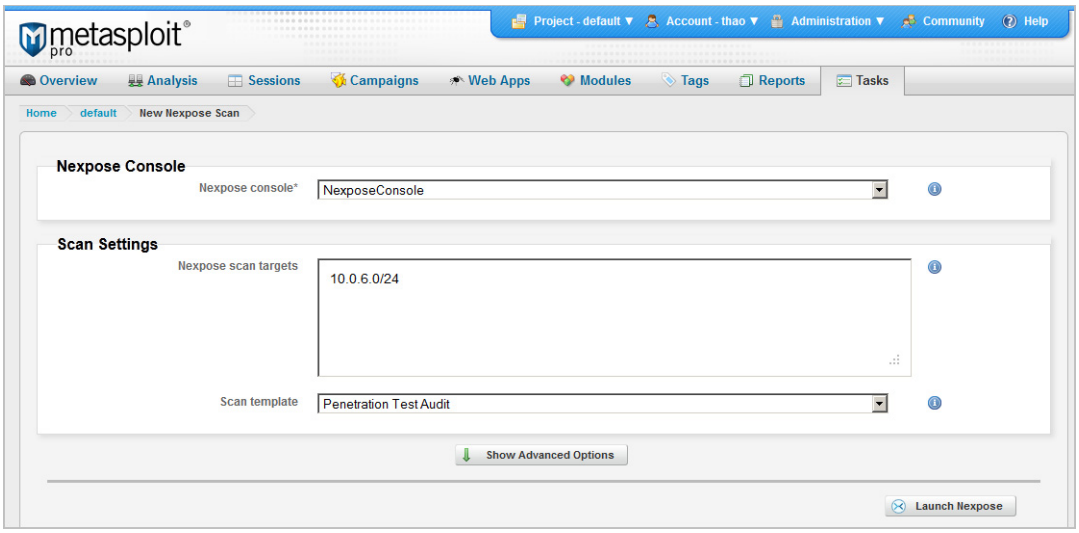
A tag is a descriptive label that you can use to categorize assets. You can use tags to create a subset, or group, of assets. For example, when you import scan data from Nexpose, you may want to tag the assets so that you can easily search for them at a later time. You can apply tags to hosts during a Nexpose scan or import.

### *Asset Tag Criteria*

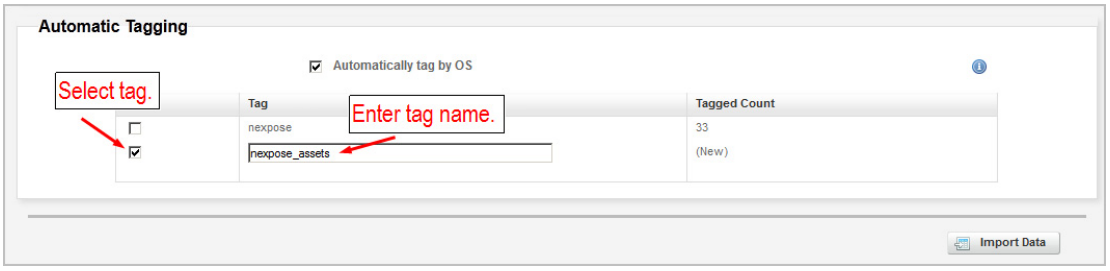
A tag cannot contain spaces and should use descriptive words. You can use an underscore (_) to link together multiple words. For example, if you want to tag assets that are on the IT subnet, you can use a tag like `IT_assets`.

### *Tagging Assets from a Nexpose Scan*

1. Open a project.
2. Click the **Analysis** tab.
3. Click **Nexpose** from the Quick Tasks menu. The Nexpose configuration page appears.



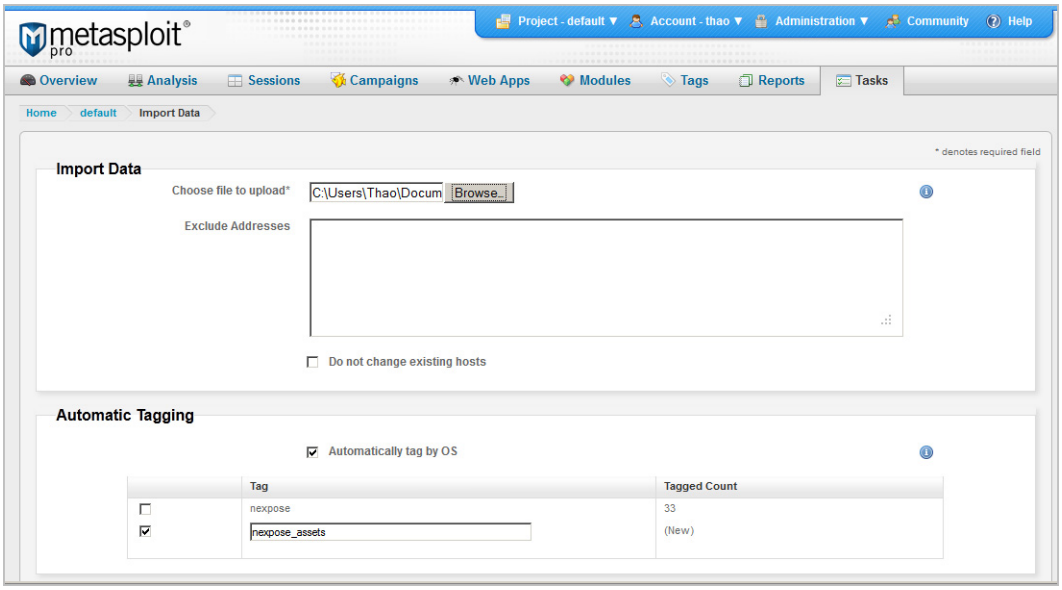

4. Select a Nexpose Console. The list shows Nexpose consoles that you have configured for Metasploit Pro to use.
5. Enter the addresses for target assets that you want to scan. You can specify an IP address or a host name. Enter one entry per line.
6. Select a scan template.
7. Click **Show Advanced Options** to configure additional options for the scan.
8. Select the Automatically tag by OS option if you want to tag assets with their OS type. For example, Metasploit Pro uses the `os_windows` tag for Windows systems and the `os_linux` tag for Linux systems.
9. From the Automatic Tagging area, you can choose or create the tags that you want to apply to the hosts. To create a tag, type the tag name in the empty tag field and select the tag.



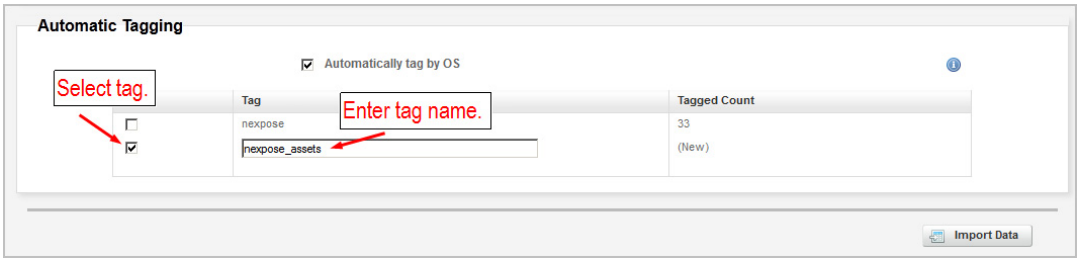

10. Launch the Nexpose scan.

### *Tagging Assets from a Nexpose Import*

1. Open or create a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click **Import**. The **Import Data** window appears.




4. Click **Browse** to choose file that you want to import. The **File Upload** window appears.
5. Navigate and choose the Nexpose XML file to import. Click **Open** after you select the file.
6. Enter the target addresses that you want to exclude.
7. Select **Do not change existing hosts** if you do not want the imported information to overwrite the data for an existing host.
8. Select the Automatically tag by OS option if you want to tag assets with their OS type. For example, Metasploit Pro uses the `os_windows` tag for Windows systems and the `os_linux` tag for Linux systems.
9. From the Automatic Tagging area, you can choose or create the tags that you want to apply to the hosts. To create a tag, type the tag name in the empty tag field and select the tag.



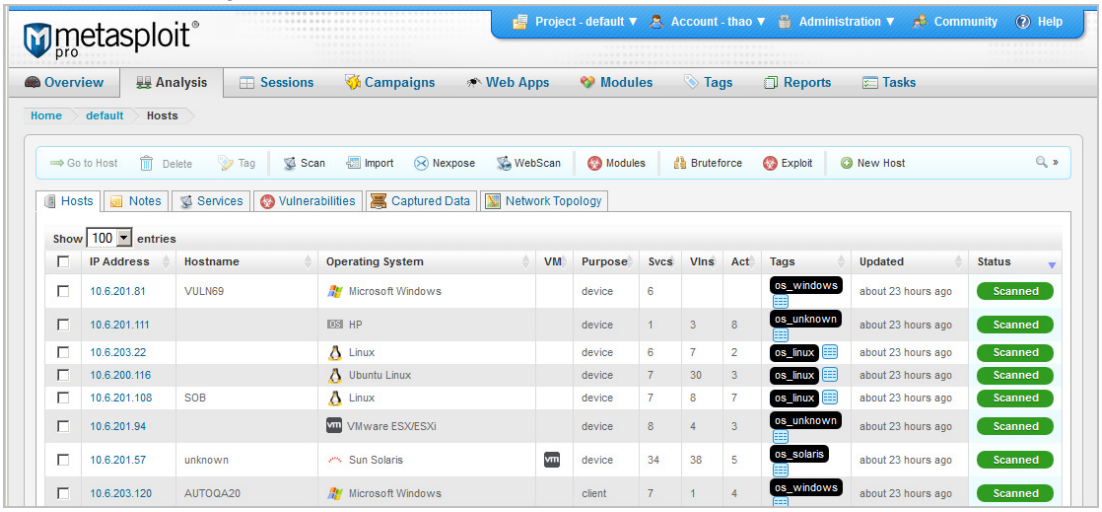

10. Import the data.

### *Manually Tagging Assets*

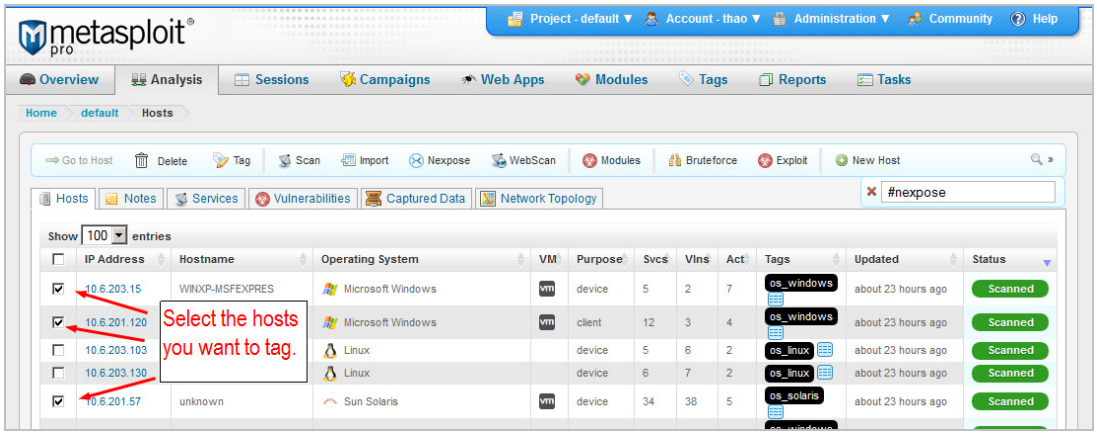
You can manually tag assets when you want to choose the individual assets that you to tag. For example, if you scan a range of systems, Metasploit Pro may discover many different devices, such as printers, mail servers, and workstations. Since Metasploit Pro discovers the

devices as part of the same scan, you cannot tag each host individually. This is a case where you may want to go through the host list after an import or scan to manually tag the hosts.

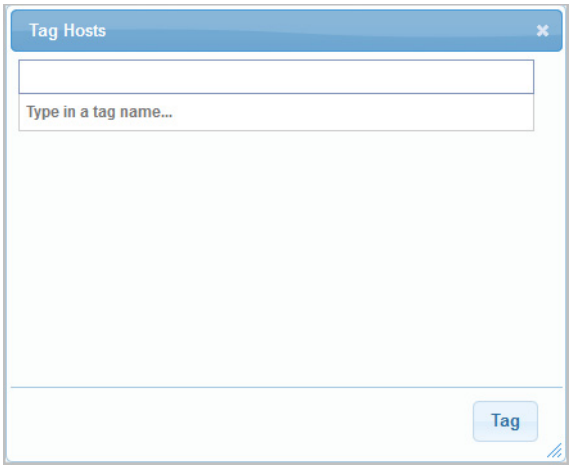
1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.




3. Select the hosts that you want to tag.




4. Click **Tag**. The Tag window appears.



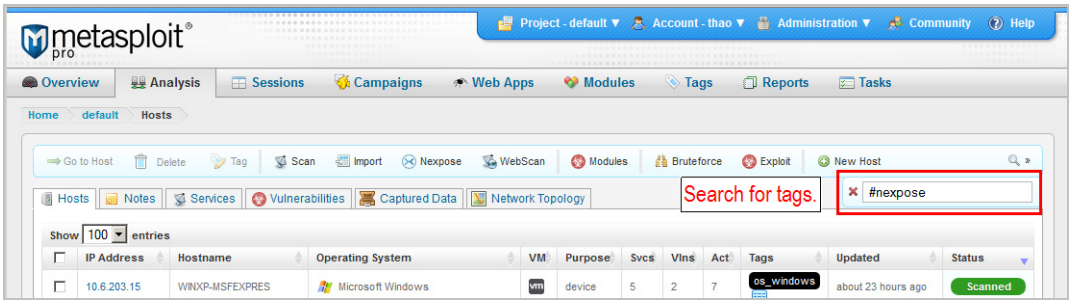

5. Type the name of the tag that you want to use. If the tag does not exist, Metasploit Pro adds the tag to the system for you.
6. Click **Tag**.

### *Searching for Tags*

You can use any search field in the Metasploit Web UI to search for tagged assets. To search for a tag, prefix the tag with the hash (#) symbol. Metasploit Pro returns a list of all assets that use the tag.

For example, if you search for `#nexpose`, Metasploit Pro returns any host that references that tag

The following image shows an example of a search for the #nexpose tag:




## Passing the Hash from Metasploit Pro

Passing the hash is a technique that enables attackers to use the NTLM and LM of a user's password to authenticate to a remote server or service. During exploitation, Metasploit Pro collects data, such as password hashes, from the exploited system. After Metasploit Pro collects password hashes from a target system, you can pass the hash and run a Nexpose scan to perform a credential scan.

**Note:** Before you can pass the hash in Metasploit Pro, you must configure a Nexpose Console from the Global Settings. After you configure a Nexpose Console, you can launch a Nexpose scan from the Metasploit Pro interface to pass the hash to the Nexpose scan.

1. Open a project.
2. Click the **Analysis** tab.
3. Click **Nexpose** from the Quick Tasks menu.
4. Select a Nexpose Console. The list shows Nexpose consoles that are available for the project.
5. Enter addresses for the scan targets. You can specify an IP address or a host name. There can be one address on each line.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses. You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the address. For example, enter `fe80::1%eth0` for a link local address.
6. Select a scan template.
7. Click **Show Advanced Options** to configure additional options for the scan.
8. Select **Pass the LM/NTLM hash credentials**. The **Hash Credentials** box displays. Metasploit Pro automatically populates the **Hash Credentials** box with a list of looted hashes. You can modify or add hashes to the hash list.
9. Launch the Nexpose scan.

## Purging Scan Data

A purge removes all scan data from the Nexpose Console and ensures optimal performance from the Nexpose scanner.

If you enable the purge scan option, Nexpose automatically deletes the scan data when the scan completes.

1. Open a project.
2. Click the **Analysis** tab.
3. Click **Nexpose** from the Quick Tasks menu.
4. Select a Nexpose Console. The list shows Nexpose consoles available for the project.
5. Enter addresses for the scan targets. You can specify an IP address or a host name. There can be one address on each line.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses. You can use standard IPv6 addressing to define individual IPv6 addresses. For example, use fe80::202:b3ff:fe1e:8329 for single addresses and 2001:db8::/32 for CIDR notations. For link local addresses, you must append the interface ID to the

address. For example, enter `fe80::1%eth0` for a link local address.

6. Select a scan template.
7. Click **Show Advanced Options** to configure additional options for the scan.
8. Select **Purge Scan results** upon completion.
9. Launch the Nexpose scan.

# Nexpose Data Import

Metasploit Pro supports the import of Nexpose simple XML and Nexpose raw XML files. When Metasploit Pro import data from a Nexpose report, it brings in the information that Nexpose found for each asset and displays it on the Hosts page.

Metasploit Pro imports the following asset information:

- IP address
- Host name
- Operating system
- Services
- Known vulnerabilities

## Importing Nexpose Reports

1. Open or create a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Click **Import**. The **Import Data** window appears.
4. Click **Browse** to choose a file to import. The **File Upload** window appears.
5. Navigate and choose a file to import. Click **Open** after you select the file.
6. Enter the target addresses that you want to exclude.
7. Select **Do not change existing hosts** if you want to retain the current host information.
8. Select if you want Metasploit Pro to automatically tag hosts with their OS as the system imports them.
9. Enable any additional tags that you want to assign to the assets.
10. Import the data.

# Nexpose Vulnerability Exceptions

An exception defines a scenario where it is acceptable for a vulnerability to exist. When you define an exception for a vulnerability, you exclude it from a report and consider the vulnerability as an accepted risk. For example, you may want to define a exception for a

vulnerability that poses minimal security risk, but requires more resources than you want to invest. In this particular case, it may be more cost effective to accept the vulnerability as a known risk than to remediate it.

When you import Nexpose data or perform a Nexpose scan, Metasploit Pro pulls the exception data for the vulnerability and stores it in the project. After you test and verify the vulnerabilities, you may want to use the results of the penetration test to update the vulnerability exception for each asset. Use the Nexpose Exception Push feature in Metasploit Pro to create and approve vulnerability exceptions for an asset. After you define the exceptions, you can export, or push, the vulnerability exceptions from Metasploit Pro to Nexpose. The Nexpose Console displays the updated vulnerability exception information on the asset summary page.

**Note:** You can only create an exception for a vulnerability that you import from Nexpose.

## Reasons for Vulnerability Exceptions

A vulnerability exception can exist due to any of the following reasons:

- **False positive** - You may want to exclude false positives reported by Nexpose. A false positive occurs when a vulnerability scanner detects a vulnerability when none exists.
- **Compensating control** - You may want to exclude vulnerabilities that have mitigated risks. For example, if a vulnerability exists on a device that has an firewall in place, an organization may determine that the firewall provides enough protection and relegate the vulnerability as a minimal threat.
- **Acceptable use** - You may want to create an exception for vulnerabilities that are part of organizational practices.
- **Acceptable risk** - You may want to exclude vulnerabilities that are low risk vulnerabilities. These vulnerabilities tend to pose minimal security risk and are likely to consume more resources than they are worth.

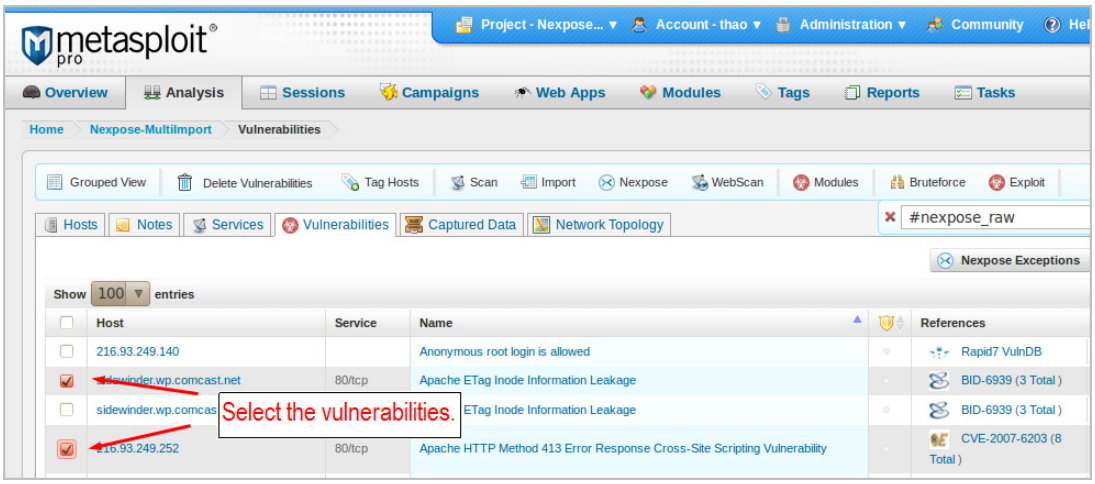
## Creating a Vulnerability Exception

To create a vulnerability exception, your project must contain assets from a Nexpose scan or import. You must also have an active Nexpose Console configure for the project. Metasploit Pro connects to the Nexpose Console that you configured for the project to create vulnerability exceptions for an asset.

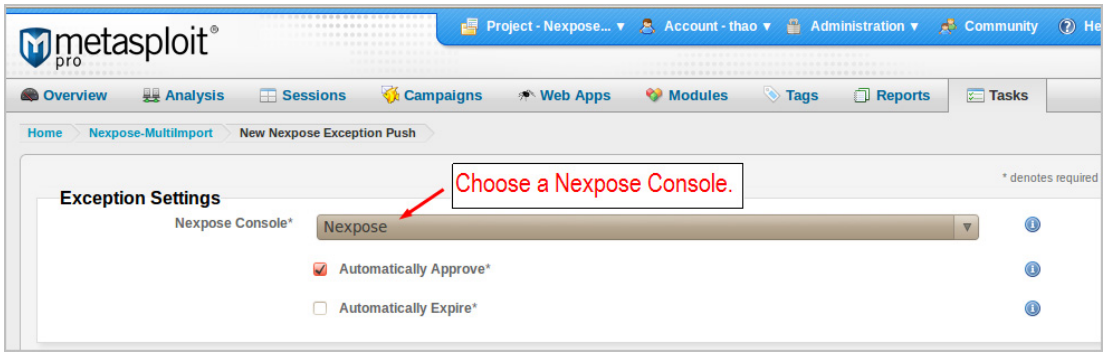
If the project does not contain an active Nexpose Console or assets, the Nexpose Exception Push feature is unavailable.

**Note:** When you import or scan assets from Nexpose, you should enable automatic tagging. A tag is a label that you apply to an asset in order to group them together based on a set of criteria. A tag helps you quickly identify and find assets to run tests against.

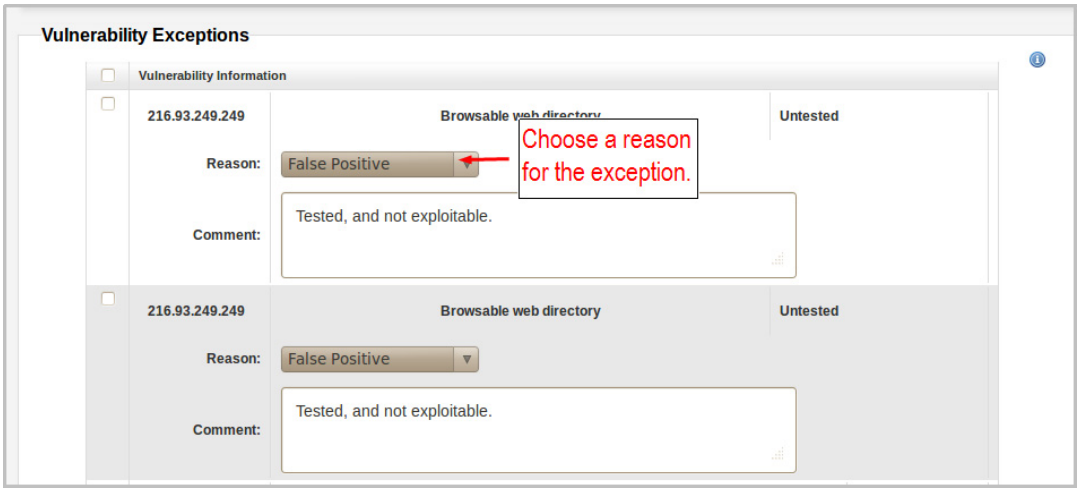
1. Select **Project > [Project Name] > Vulnerabilities** from the main menu. A list of assets and vulnerabilities appears.
2. Select the assets that you want to use to create vulnerability exceptions.




3. Click **Nexpose Exceptions**. The **New Nexpose Exceptions Push** window appears.
4. Choose the Nexpose Console that you want to use to push the vulnerability exceptions.




5. Choose if you want to automatically approve the vulnerability exception. If you do enable this option, you will need to approve the vulnerability request through the Nexpose Console.
6. Choose if you want to set an expiration date for the vulnerability exception. If you choose this option, Nexpose will remove the exception from the asset on the date that you specify.
7. The **Vulnerability Exceptions** area displays a table that lists the vulnerability information for each asset that you added to the exception push. Select the vulnerability that you want to create an exception for.
8. Choose a reason for the exception.




9. Add any additional comments about the exception, such as how the vulnerability meets the requirements for the exception.
10. Create the exceptions.

After you create the exceptions, open the Nexpose Console and verify that the asset shows the vulnerability exception that you created in Metasploit Pro.

# Nexpose Asset Groups

In Nexpose, an asset group represents the logical grouping of assets. Assets within an asset group may share some commonality, such as operating systems or services. You create asset groups so that you can easily assign a set of assets to a specific user. Any user who has access to the asset group can monitor and remediate the vulnerabilities that Nexpose identifies for the assets within the group.

In Metasploit Pro, host tags behave similarly to asset groups. Host tags help you logically group hosts, or assets, based on a set of criteria. For example, you can use tags to group together machines that are exploitable or to identify machines that have weak passwords.

Host tags are particularly useful if you want to use the results of a penetration test to create an asset group in Nexpose. In Metasploit Pro, you can search for assets based on their host tag and create an asset group for those assets.

## Creating a Nexpose Asset Group

To create a Nexpose asset group, your project must contain assets from a Nexpose scan or import. You must also have an active Nexpose Console configured for the project. Metasploit Pro connects to the Nexpose Console that you configure for the project to create asset groups.

If the project does not contain an active Nexpose Console or assets, the Nexpose Asset Group Push feature is unavailable.

Additionally, to utilize the Nexpose Asset Group Push feature, you must apply tags to the assets. A tag logically groups together a set of assets based on a set of criteria. For example, you can tag assets as vulnerable.

You can apply tags manually, or you can enable automatic tagging for Nexpose scans and imports.

1. Open a project.
2. Click the **Tags** tab.
3. Select the tags that you want to use to create asset groups.
4. Click **Nexpose Push**.
5. Choose the Nexpose Console that you want to use to create the asset groups.
6. Type a descriptive name for the asset group.
7. Type a description for the asset group.
8. Enter a list of IP addresses for the assets that you want to include in the asset group.
9. Create the asset group.

# Vulnerability Tracking

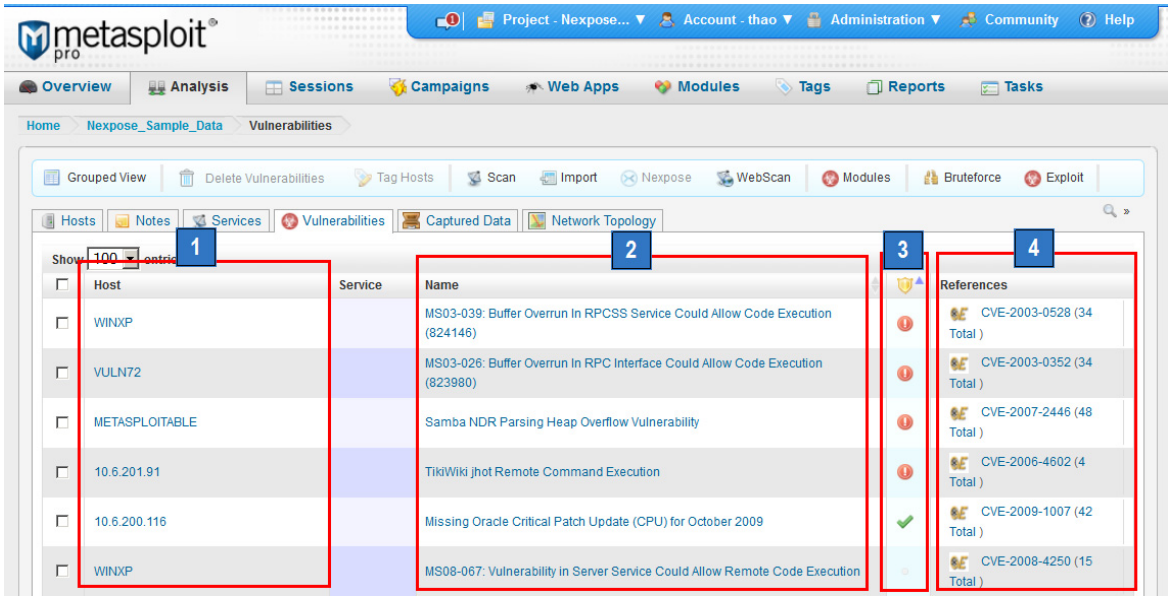
The Metasploit Web UI provides an interactive interface that you can use to visualize and validate the vulnerability data from a Nexpose report. Metasploit Pro identifies the assets, imports vulnerability data, indexes the data, and attempts to map the each vulnerability to an exploit. Metasploit Pro displays most of the content for each asset on the Hosts page.

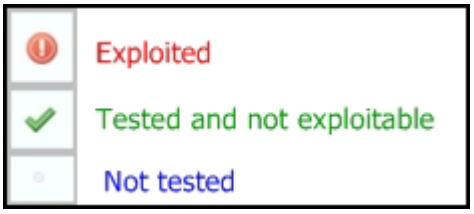
The Hosts page provides you with a high-level view of the assets that Metasploit Pro imported. You can see the number of services, vulnerabilities, and exploit attempts for each host. If you want to explore a bit more, you can visit the Vulnerabilities tab to learn more about each asset.

## Vulnerability Overview Page

The Vulnerability Overview page displays all the vulnerabilities that you import from Nexpose. The Vulnerability Overview page provides you with a broad scope of all the vulnerabilities that have been identified on your assets. View the Vulnerability Overview page to quickly identify the assets that Metasploit Pro has tested and exploited; assets that have not been tested; or assets that are not exploitable.

The following image shows the Vulnerabilities Overview page.




| Callout | Column Name | Description |
|---|---|---|
| 1 | Host | Shows the host name or IP address. |
| 2 | Name | Shows the vulnerability name. |
| 3 | Defended | Displays the current exploit status for the vulnerability.<br>  |
| 4 | Reference | Displays the vulnerability reference ID. Metasploit Pro will always show the CVE-ID if it is available. If a CVE-ID is not available, Metasploit Pro displays the BID. |

### *Viewing the Vulnerabilities Overview Page*

To view the Vulnerabilities Overview page, select **Project > [Project Name] > Vulnerabilities** from the main menu. A list of vulnerabilities that have been identified within the project displays in the browser.

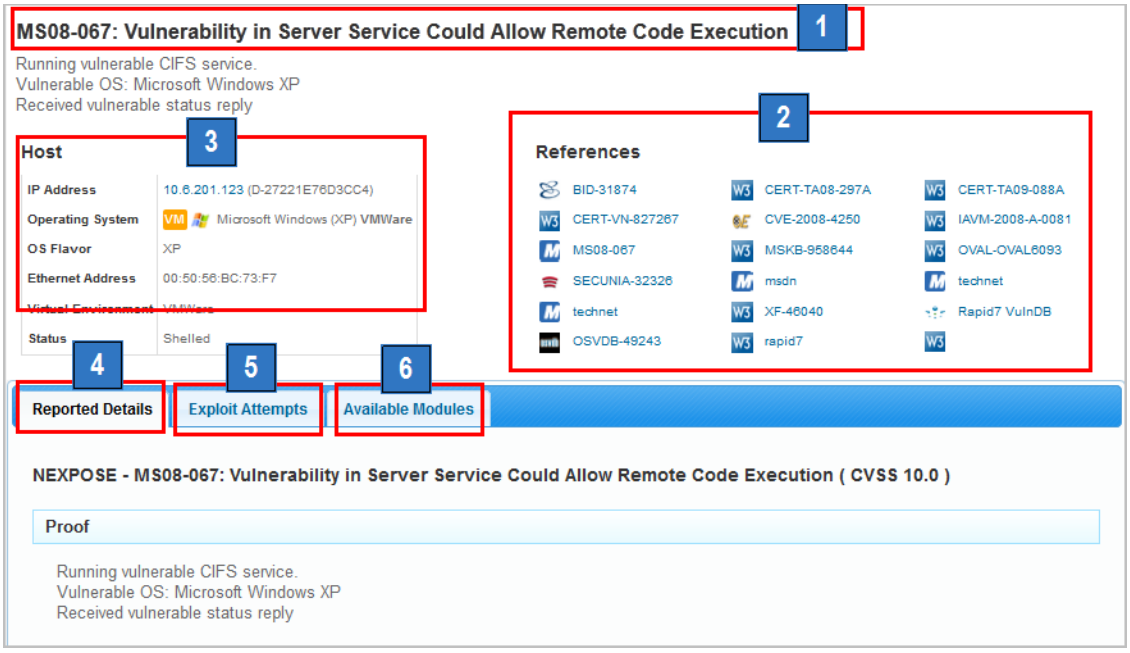
## Vulnerability Details Page

The Vulnerability Details page provides you with the granular details of a vulnerability. When you import vulnerability scan data from Nexpose, Metasploit Pro pulls the vulnerability details from the report, such as the Nexpose console ID, vulnerability name, description, test results, solution, and references. Metasploit Pro displays the vulnerability data for each asset on the Vulnerability Details page.

You can leverage the information on the Vulnerability Details page to launch an exploit against the vulnerability. Metasploit Pro automatically maps the vulnerability to a matching exploit based on service and vulnerability information. You can view the matching exploits from the Available Modules tab on the Vulnerability Details page.

**Note:** Metasploit Pro maps vulnerabilities to exploit modules. Other modules, like auxiliary, payload, and post-exploitation modules, are not mapped to vulnerabilities.

The following image shows the Vulnerability Details page.




| Callout | Name | Description |
|---|---|---|
| 1 | Vulnerability Name | Lists the full vulnerability name. |
| 2 | Reference IDs | Lists all known vulnerability reference IDs, such as the CVE, BID, and OSVDB. Click on any ID to view more information about the vulnerability. |
| 3 | Host Information | Lists the information for the host on which the vulnerability exists. |

| Callout | Name | Description |
|---|---|---|
| 4 | Reported Details Tab | Displays the vulnerability report data from Nexpose. Includes the Nexpose console information, proof data, vulnerability status, vulnerability severity level, description, and solution. |
| 5 | Exploit Attempts Tab | Displays the exploit module that Metasploit Pro ran against the vulnerability and shows the result of the exploit. |
| 6 | Available Modules Tab | Shows the exploit modules that correlate to the vulnerability. Provides a link that you can click to launch a matching exploit against the vulnerability. |

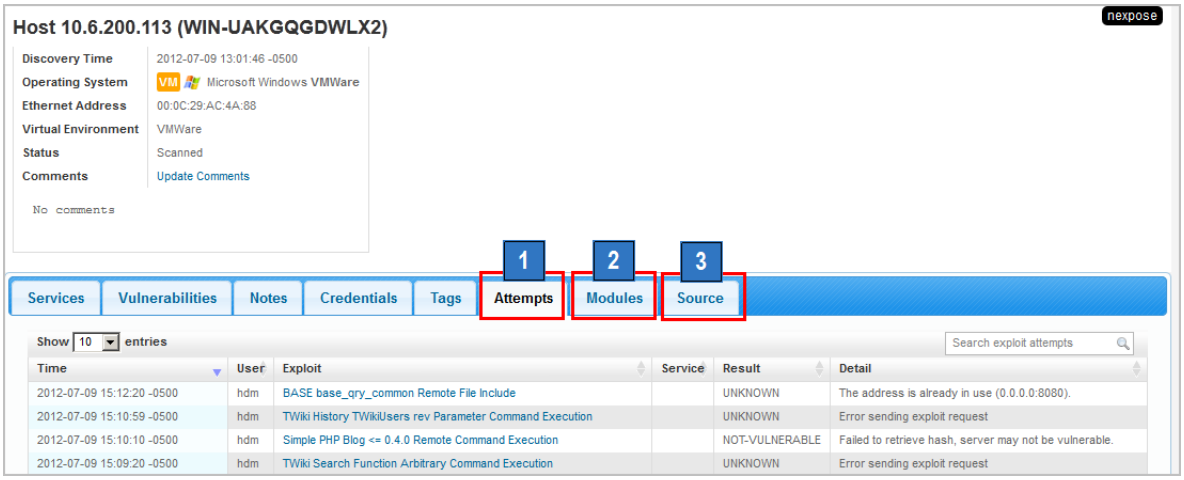
### *Viewing the Vulnerability Details Page*

To view the details page for a particular vulnerability, select **Project > [Project Name] > Vulnerabilities** from the main menu. A list of assets and vulnerabilities appears. Click on the vulnerability name. The details for the vulnerability display in the browser window.

## Host Details Page

The Host Details page provides you with a detailed look at a particular host or asset. You can view the on the Host Details page to view the data collected from a particular host, such as the active services, identified vulnerabilities, credentials, and notes. Use this data to perform further reconnaissance against a target so that you can pinpoint the best method to exploit a system.

The following image shoes the Host Details page.




| Callout | Tab Name | Description |
|---|---|---|
| 1 | Attempts | Displays the modules that Metasploit Pro has run against the host. |
| 2 | Modules | Displays the modules that you can run against the host based on the open services and vulnerabilities are available. |
| 3 | Source | Displays the Nexpose console name and ID. |

## *Viewing the Host Details Page*

To view the details page for a particular host, select **Project > [Project Name] > Hosts** from the main menu. A list of assets appears. Click on a host name or IP address to view more information about the host. The details for the host display in the browser window.

## *Attempts Tab*

If Metasploit Pro has run any module against the host, you can view the results from the Attempts tab. The Attempts tab shows when the modules were run, the person who launched the module, the result code for the module run, and the reason the module failed or succeeded.

For example, you may want to view the Attempts tab if you want to find a list of modules that Metasploit Pro has run against a particular port or service.

### Result Codes

A result code provides the reason why a module run was unsuccessful.

The following is a list of the possible result codes that can display for an exploit attempt:

- **None** - Metasploit Pro could not determine if the module was successful.
- **Unknown** - Metasploit Pro could not determine if the module was successfully.
- **Unreachable** - Metasploit Pro could not reach the network service.
- **Bad-config** - The exploit settings were not configured correctly.
- **Disconnected** - The network service disconnected during a module run.
- **Not-found** - Metasploit Pro could not find the application or service.
- **Unexpected-reply** - Metasploit Pro did not receive the expected response from the application.
- **Timeout-expired** - A timeout occurred.
- **User-interrupt** - The user stopped the module run.
- **No-access** - Metasploit Pro could not access the application.
- **No-target** - The target was not compatible with the module configuration.
- **Not-vulnerable** - The application response indicated that it was not vulnerable.
- **Payload-failed** - Metasploit Pro delivered the payload, but was unable to open a session.

### *Modules Tab*

Metasploit Pro automatically maps modules to a host based on the open services and vulnerability information that is available. Due to the number of vulnerability checks that are available, Metasploit typically matches exploits based on services rather than vulnerabilities. The Modules tab displays a full list of exploits and auxiliary modules that are available for a particular asset.

### *Source Tab*

The Source tab identifies the device used to import the host. For example, if you imported assets from a Nexpose report, the Source tab shows the Nexpose console ID and device ID.

# Gaining Access

This chapter covers the following topics:



## Gaining Access Overview

After you discover live hosts on the target network, you can execute bruteforce attacks or exploit modules to gain access to the target systems. To gain access to a target, you must identify the security vulnerability that exists on the target and successfully execute the exploit code to establish a connection to the target.

## Bruteforce Attacks

A bruteforce attack attempts a large number of common user name and password combinations to gain access to hosts. You can use preset bruteforce profiles to customize the bruteforce attack for the environment.

When Metasploit Pro successfully identifies a credential in a session capable module, such as SMB, SSH, Telnet, or MSSQL, the system automatically opens the session.

### Bruteforce Target Services

After Metasploit Pro opens the session, you can select the services that you want to target in the bruteforce attack.You can target the following services:

- SMB
- Postgres
- DB2
- MySQL
- MSSQL
- HTTP
- HTTPS

- SSH
- SSH_PUBKEY
- Telnet
- FTP
- POP3
- EXEC
- Login
- Shell
- VMAUTHD
- VNC
- SNMP

## Bruteforce Message Indicators

Metasploit Pro color codes bruteforce task logs to help you identify successful and unsuccessful attacks. Metasploit Pro records successful attacks in the database as authentication notes. You can view the authentication notes from the Analysis window.

The following list describes the color codes that Metasploit Pro uses for bruteforce tasks:

- Green Message - Good status indicator
- Yellow Message - Credential found indicator
- Red Message - Bad status indicator

## Bruteforce Attack Options

The following table describes the options for a bruteforce attack:

| Option | Description |
|---|---|
| Bruteforce Depth: Quick | Identifies the basic password combinations. Quick has the shortest duration because it attempts less than 25 known user name and password combinations. Quick uses a static list of credentials and tries them against discovered services. The list of credentials include:<br><br>Admin:admin<br>Admin:admin1<br>Admin:admin!<br>Test:test<br>Test:test1234<br>Test123:test123<br>cisco:cisco<br>user:user<br>administrator:administrator<br>root:root<br>root:toor<br><br>After the bruteforce attack tries the static credentials list, it tries the user names with a blank password. The bruteforce attack prepends known credentials to the static list.<br><br>The system generates approximately 20 credentials in order to bruteforce all services. |
| Bruteforce Depth: Defaults Only | Attempts a small number of known default and user names and passwords.<br><br>The default only mode generates the following credentials:<br><br>16 credentials for postgres<br>29 credentials for DB2<br>141 credentials for SSH<br>141 credentials for Telnet<br>22 credentials for MSSQL<br>150 credentials for HTTP<br>4 credentials for HTTPS<br>13 credentials for SMB<br>21 credentials for FTP |

| Option | Description |
|---|---|
| Bruteforce Depth: Normal | Attempts a fixed maximum number of credentials. The normal mode takes approximately 5 minutes per host on a fast LAN. The normal mode focuses on common, protocol-specific user names as well as discovered user names and passwords. The normal mode identifies discovered passwords from a list of common passwords. Most protocols have common defaults, which Metasploit Pro tries after known good credentials on other services.<br><br>The normal mode generates the following credentials:<br><br>4,000 credentials for postgres<br>3,000 credentials for DB2<br>10,000 credentials for MySQL<br>1,000 credentials for SSH<br>1,000 credentials for Telnet<br>10,000 credentials for MSSQL<br>6,000 credentials for HTTP<br>1,000 credentials for HTTPS<br>4,000 credentials for SMB<br>1,000 credentials for FTP<br><br>The system tries these generated credentials after the current known good credentials. The system adjusts the credentials figures after each successive run, if the credentials become known as the modules run. |
| Bruteforce Depth: Deep | Attempts three times more passwords than the normal mode. The deep mode takes 15-20 minutes for each host on a fast LAN, if all services are enabled. The additional passwords come from the common password list.<br><br>For the few protocols that support fast enough guesses, passwords are subject to a fixed set of transformations. For example, 1 for I and 0 for O.<br><br>The deep mode generates the following credentials:<br><br>12,000 credentials for postgres:5432<br>9,000 credentials for DB2:50000<br>30,000 credentials for MYSQL:3306<br>132 credentials for SSH:22<br>132 credentials for Telnet:23<br>30,000 credentials for MSSQL:13013<br>18,000 credentials for HTTP:8080 (tomcat)<br>3,000 credentials for SMB:445 (Microsoft)<br><br>SSH and Telnet are not subject to the deep multiplier because these credentials take longer to test than the other services. |

| Option | Description |
|---|---|
| Bruteforce Depth: 50K | Attempts 50,000 user name and password combinations for each service. |
| Bruteforce Depth: Imported Only | Uses the user name and password list, or credential file, that you import into the system. |
| Bruteforce Depth: Known Only | Attempts credentials that are already known for all services in the target workspace. This includes SSH keys and passwords. |
| Bruteforce Speed: Turbo | Use the Turbo speed on a fast LAN. |
| Bruteforce Speed: Fast | Use the Fast speed on most LANs. |
| Bruteforce Speed: Normal | Use the Normal speed for external use. |
| Bruteforce Speed: Slow | Use the Slow speed for slow WAN links or to hide the scan. |
| Bruteforce Speed: Stealthy | Use the Stealthy speed if you want the attack to be sneaky. |
| Bruteforce Speed: Glacial | Requires the most amount of time to complete. |
| Target Services | SMB, Postgres, DB2, MySQL, MSSQL, Oracle, HTTP, HTTPS, SSH, Telnet, FTP, EXEC, Login, Shell, VNC, SNMP |
| Target Addresses | Defines the hosts that the system includes in the bruteforce attack. |
| Excluded Addresses | Defines the hosts that the system excludes from the bruteforce attack. |
| Dry run | Runs a bruteforce attack, prints a transcript of the modules, and quits the attack. Metasploit Pro does not run a live bruteforce attack against the target system. |
| Produce verbose in the output task log | Records the successes and failures of the modules that the bruteforce attack runs. |

| Option | Description |
|---|---|
| Additional credentials | Defines the user name and password combinations that the bruteforce attack uses. Use commas to separate user name and password combinations.<br><br>For domain-specific user name and password combinations, use the following format: domain/username.password.<br><br>For user names with no password, define the user name only.<br><br>For user names with multiple passwords, use the following format: username password1, password2, password 3. |
| SMB Domains | Adds the domain as a space delimited list for services that accept Windows-based authentication. |
| Payload Type | Specifies the type of payload that the bruteforce attack uses. You can choose Meterpreter or command shell. |
| Listener Ports | Defines the port or port range that the bruteforce attack uses in reverse connect payloads. |
| Connection Type | Defines the connection type that the payload uses. Choose from auto, reverse, or bind. |
| Listener Host | Defines the IP address that the payload uses to connect back. Use this option to override the listener port. |
| Auto Launch Macro | Defines the macro that runs during the bruteforce attack. You can create macros from the Global Settings. |
| Automatically open sessions with guessed credentials | Opens the session when a credentials is successful. |
| Limit to one cracked credential per service | Stops the bruteforce attack after the system collects the first credential. |
| Max guesses per user | Limits the number of guesses for each user - not each user name. |
| Timeout per service | Limits the total time that the attack limits to each service instance. |
| Timeout overall | Limits the total amount of time that the system allocates to the bruteforce attack. |
| Max guesses overall | Limits the total number of guesses that the bruteforce attack attempts. |

| Option | Description |
|---|---|
| Skip blank password generation | Disables the use of blank passwords. |
| Exclude machine names as passwords | The bruteforce attack does not use known computer names and user names as passwords. |
| Skip common Windows machine accounts | Skips Windows accounts that do not have remote login rights or randomly generated passwords. The accounts include TsInternetUser krbtgt NetShowServices, IUSR_<anything>, IWAM_<anything>, WMUS_USER-<anything>. |
| Skip common UNIX machine accounts | Skips Unix accounts that don't have remote login rights or randomly generated passwords. This includes: daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data backup list, irc, gnats, nobody, libuuid, syslog, messagebus, haldaemon, hplip, avahi, couchdb, kernoops, saned, pulse, gdm, sshd, telnetd, dhcp, avahi-autoipd, speech-dispatcher. |
| SMB: Recombine known, imported, and additional credentials | Takes all the usernames:passwords from the known credentials list, imported list, and credentials textbox, and assigns all the passwords to all users. |
| SMB: Preserve original domain names | Tries the original domain name. |
| Mutate known credentials | Determines the portion of the credential list subjected to mutations – in this case, all known credentials. |
| Mutate imported credentials | Determines the portion of the credential list subjected to mutations – in this case, all imported credentials. |
| Mutate additional credentials | Determines the portion of the credential list subjected to mutations – in this case, all credentials manually added by the user. |
| Mutation: append numbers to candidate passwords | Strips off all trailing digits off a password and replaces it with a single digit and skips all passwords that do not contain a letter. |
| Mutation: prepend numbers to candidate passwords | Strips off all digits at the beginning of a password and replaces it with a single digit and skips all passwords that do not contain a letter. |

| Option | Description |
|---|---|
| Mutation: substitute numbers within candidate passwords | Strips off up to two digits within a password and replaces it with up to two digits. Passwords with more than three digits are ignored. |
| Mutation: transpose letters for “l33t-sp34k” alternatives in candidate passwords | Rotates through a number of alpha to numeric substitutions before substituting all of them. |
| Mutation: append special characters to candidate passwords | Appends a punctuation mark to the beginning of a password or replaces an existing punctuation mark. |
| Mutation: prepend special characters to candidate passwords | Prepends a punctuation mark to the end of a password or replaces an existing punctuation mark. |
| Recombine known, imported, and additional credentials | Takes the user names and passwords from the known credentials list, imported list, and credentials text box, and assigns all the passwords to all users. |
| Include known credentials | Uses all known credentials from the project. The bruteforce attack tries the known passwords first. All credentials that are “known only” and “quick” are not affected by the credential generation switch. |

## Running a Bruteforce Attack

Before you run a bruteforce attack, perform a discovery scan first.

1. Open a project.
2. Click the **Analysis** tab.
3. Select the hosts that you want to run the bruteforce attack against.
4. Click **Bruteforce**. The **Bruteforce** window appears. Metasploit Pro automatically populates the target addresses field with the selected hosts.
5. Select the depth of the bruteforce attack.
6. Select the services that you want the bruteforce attack to target.
7. Click **Show Advanced Options** to configure additional options for the bruteforce attack.
8. Launch the bruteforce attack.

## Running a Bruteforce Attack Against a Virtual Target

You can run a bruteforce attack against vmauthd, the authentication daemon for VMware's virtual infrastructure client, and for VMware Web Service. If the bruteforce attack successfully guesses the credentials, then you can use the credentials to administer VMware.

**Note:** You cannot access VMware directly from Metasploit Pro. However, after you gain access to a virtual machine, you can run post-exploitation modules to identify more information about the machine, such as configuration settings, logins, and other virtual machines.

1. Open a project.
2. Click the **Analysis** tab.
3. Select the virtual target that you want to bruteforce.
4. Click **Bruteforce**. The **Bruteforce** window appears. Metasploit Pro automatically populates the target address field with the vmauthd target address.
5. Click **Show Advanced Options** to configure additional options for the bruteforce attack.
6. Launch the bruteforce attack.

## Running a Bruteforce Attack Using an Imported Credential List

Before you can run a bruteforce attack using an imported credential list, you must import the user name and password list. To import credentials, click the **Manage Credentials** button and select the file that you want to upload.

1. Open a project.
2. Click the **Analysis** tab.
3. Select the hosts that you want to run the bruteforce attack against.
4. Click **Bruteforce**. The **Bruteforce** window appears. Metasploit Pro automatically populates the target addresses field with the selected hosts.
5. Select **Imported Only** for depth of the bruteforce attack.
6. Select the services that you want the bruteforce attack to target.
7. Click **Show Advanced Options** to configure additional options for the bruteforce attack.
8. Launch the bruteforce attack.

## Testing a Single Credential

1. Open a project.
2. Click the **Analysis** tab.
3. Select the hosts that you want to test the credential against.

4. Click **Bruteforce**. The **Bruteforce** window appears. Metasploit Pro automatically populates the target addresses field with the hosts that you chose.
5. Select **Quick** for depth of the bruteforce attack.
6. Select the services that you want the bruteforce attack to target.
7. Click **Show Advanced Options** to configure additional options for the bruteforce attack.
8. Enter the single credential that you want to use for the bruteforce attack in the Additional Credentials field. For example, enter `admin admin`.
9. Launch the bruteforce attack.

## Credential Management

You can import sets of untested credentials into Metasploit Pro. Use imported credentials when you run the scan in normal, deep, or imported only mode.

If you import multiple files, Metasploit Pro consolidates the credentials from each file and stores the data within a single, running file. The imported credentials do not display under the credentials area. To view the imported credentials, you can download the imported credentials as a single text file.

**Note:** You should use the **Additional Credentials** option for known credentials or for bruteforce attacks that use the **Include known credentials** option.

### *Supported Credential File Formats*

For imported credential files, you can add spaces and any other special characters to passwords by specifying them as `\x20` or any other hex value `-- \x09` for tab, `\x90` for a password with a NOP. If you have a password that contains the string `\x20`, you can use `\x5cx20` to protect the password.

The following table describes the credential file formats that Metasploit Pro supports:

| Format | Description |
|---|---|
| PWDump | A PWDump file can contain SMB hashes and space delimited user name and password pairs. Each item must be on a separate line. The bruteforce attack attempts the SMB hash credentials against services that accept SMB hashes as plain text.<br><br>When you use a PWDump file, you must define the SMB domains to target services that accept Windows authentication.<br><br>When you use a PWDump file, use the **imported only** bruteforce depth to test only this list of credentials.<br><br>Use this format if you have an exported a Metasploit PWDump. |
| | Example:<br>administrator:501:de8130a284642c74523fa0f66c35ef02:421a1c7abc7b160c20ed78a2e06e09c8::: |
| User names and passwords | A user name and password file is a text file that contains a user name and password on each line. You must use a space to separate the user name and password.<br><br>User names and passwords can contain non-ASCII in \xXX notation. For example, you can denote spaces within a user name or password as \x20.<br><br>When you use a user name and password file, use the **imported only** bruteforce depth to test only this list of credentials.<br><br>Use this format if you have a list of user names and passwords. |
| | Example:<br>username1 passwordA<br>username2 passwordA passwordB<br>username3 passwordA passwordB passwordC |

| Format | Description |
|---|---|
| Passwords only | A passwords only file is a text file that contains only passwords. There can be only one password for each line in the file.<br><br>Metasploit Pro assigns the passwords to known user names. Passwords can contain non-ASCII in \xXX notation. For example, you can enter `testuser d\xeadb\xeef`.<br><br>When you use a plain password file, do not use the **imported only** bruteforce depth. You must choose a different bruteforce depth so that Metasploit Pro can assign a user names to each password.<br><br>Use the plain password format if you have a list of passwords and you want Metasploit Pro to specify user names to test against. |
| | Example:<br>password1<br>password2<br>password3 |
| User names only | A user names only file is a text file that contains only user names. There can be one user name for each line in the file.<br><br>Metasploit Pro assigns the user names to common passwords. User names can contain non-ASCII in \xXX notation. For example, you can enter `testuser d\xeadb\xeef`.<br><br>When you use a user names only file, do not use the **imported only** bruteforce depth. You must choose a different bruteforce depth so that Metasploit Pro can assign a password to each user name. |
| | Example:<br>jack<br>joe<br>john |

### *Importing Credentials or a Custom Word List*

All credential files, or custom word lists, must use a newline delimited format.

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Select the hosts you that you want to include in the bruteforce attack.
4. Click **Bruteforce**.
5. Click **Manage Credentials**. The **Credential Import** page appears.
6. Click **Browse** to navigate to the location of the credentials file. The credentials file must be in plain ASCII.

7. Click **Open** after you select the credentials file.
8. Select the type of content that the list contains. The file type can be UserPass, Usernames, Passwords, PWDump, or SSH key. For example, choose **Usernames** if the list contains only user names or **Passwords** if the list contains only passwords.
9. Enter a name for the imported file.
10. Enter a description for the imported file.
11. Upload the file.

### *Using a Credential File or Custom Word List*

After you import a credential file or custom word list, you can select the file that you want the bruteforce attack to use.

1. Open a project.
2. Click the **Analysis** tab. The **Host** window appears.
3. Select the hosts you that you want to include in the bruteforce attack.
4. Click **Bruteforce**.
5. Choose the depth and services for the brute force attack.
6. Click **Show Advanced Options** and configure any additional options for the bruteforce attack.
7. Under Credential Selection, locate the **Imported Credential Files** list. Select the credential file, or keyword list, that you want to use.
8. Run the bruteforce attack.

### *Viewing Imported Credentials*

1. Open a project.
2. Click the **Overview** tab.
3. Click **Bruteforce**. The **Bruteforce** window appears.
4. Click **Manage Credentials**. The **Credential Import** window appears.
5. Locate the credentials that you want to view. Click Download.
6. Save the file to a location on your computer.

### *Deleting Imported Files*

1. Open a project.
2. Click the **Overview** tab.
3. Click **Bruteforce**. The **Bruteforce** window appears.
4. Click **Manage Credentials**. The **Credential Import** window appears.
5. Locate the credentials that you want to view. Click Delete for each file that you want to delete.

## Credential Generation Switches

You can use credential generation switches to specify how Metasploit Pro generates credentials.

The following table describes the credential generation switches that are available:

| Credential Generation Switch | Description |
|---|---|
| Include known credentials | Uses all credentials already in the project. These credentials are tried first. All credentials with the “known only” and “quick” are not affected by the Credential Generation Switch. |
| SMB: Preserve original domain names | Tries the original domain name. |
| Skip blank password generation | Disables using blank passwords. |
| Excludes machine names as passwords | Skips using known computer names and user names as passwords. |
| Skip common Windows machine accounts | Skips Windows accounts that don’t have remote login rights or randomly generated passwords. These include: TsInternetUser krbtgt NetShowServices, IUSR_<anything>, IWAM_<anything>, WMUS_USER-<anything>. |
| Skip common Unix machine accounts | Skips Unix accounts that don’t have remote login rights or randomly generated passwords. This includes: daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data backup list, irc, gnats, nobody, libuuid, syslog, messagebus, haldaemon, hplip, avahi, couchdb, kernoops, saned, pulse, gdm, sshd, telnetd, dhcp, avahi-autoipd, speech-dispatcher. |
| Recombine known, imported, and additional credentials | Takes all the usernames:passwords from the known credentials list, imported list, and credentials text box, and assigns all the passwords to all users. |

### *Enabling Credential Generation Switches*

1. Click the **Analysis** tab. The **Host** window appears.
2. Click **Bruteforce**. The **Bruteforce** window appears.
3. Click **Advanced Options**.
4. Under the Credential Generation Switches area, enable any of the generation switches that you want to use.
5. Configure and launch the Bruteforce attack.

## Credential Mutation Switches

You can use credential mutation switches to mutate known and imported credentials to detect common password variations during a bruteforce attack.

The following table describes the credential mutation switches:

| Credential Mutation Switch | Description |
|---|---|
| Mutate known credentials | Determines the portion of the credential list subjected to mutations – in this case, all known credentials. |
| Mutate additional credentials | Determines the portion of the credential list subjected to mutations – in this case, all credentials manually added by the user. |
| Mutate imported credentials | Determines the portion of the credential list subjected to mutations – in this case, all imported credentials. |
| Mutation: append numbers to candidate passwords | Strips off all trailing digits off a password and replaces it with a single digit and skips all passwords that do not contain a letter. |
| Mutation: prepend numbers to candidate passwords | Strips off all digits at the beginning of a password and replaces it with a single digit and skips all passwords that do not contain a letter. |
| Mutation: substitute numbers within candidate passwords | Strips off up to two digits within a password and replaces it with up to two digits. Passwords with more than three digits are ignored. |
| Mutation: transpose letters for “i33t-sp34k” alternatives in candidate passwords | Rotates through a number of alpha to numeric substitutions before substituting all of them. |
| Mutation: append special characters to candidate passwords | Appends a punctuation mark to the beginning of a password or replaces an existing punctuation mark. |
| Mutation: prepend special characters to candidate passwords | Prepends a punctuation mark to the end of a password or replaces an existing punctuation mark. |

## Enabling Credential Mutation Switches

1. Click the **Analysis** tab. The **Host** window appears.
2. Click **Bruteforce**. The **Bruteforce** window appears.
3. Click **Advanced Options**.
4. Under the Credential Mutation Switches area, enable any of the mutation switches that you want to use.

5. Configure and launch the Bruteforce attack.

# Modules

A module is the component that Metasploit Pro uses to perform an attack or a specific action. The attack or action that the module performs depends on the module type.

## Module Types

The Metasploit Framework categorizes modules based on the action that the module performs.

The following are modules types that are available:

- Exploit - A module that targets and exploits the vulnerabilities that the vulnerability scanners discover.
- Auxiliary - A module that performs tasks other than exploitation, such as fuzzing and scanning.
- Post-Exploitation - A module that runs after Metasploit Pro compromises a target system.

### *Excluded Modules*

Most modules that are available in the Metasploit Framework are available in Metasploit Pro. However, some modules may be excluded if their dependencies are unavailable.

Modules that are currently excluded are modules that depend on the following libraries:

- Oracle - Affects modules that target Oracle.
- Lorcon2 - Affects modules that target wireless systems.
- Libpcap - Affects modules that target sniffers.
- DECT - Affects modules that target telephony.

## Module Search

The module search engine searches the module database for the keyword expression and returns a list of results that match the query. Use the module search engine to find the module that you want to run against a target system.

### *Keyword Tags*

You can use keyword tags to define a keyword expression.

The following table describes keyword tags:

| Keyword Tag | Description |
|---|---|
| name | Searches for the keyword expression within the module descriptive name. |
| path | Searches for the keyword expression within module path name. |
| platform | Searches for the modules that affect the platform or target that you define in the keyword expression. |
| type | Searches for the modules that belong to the module type that you define in the keyword expression. For example, use exploit, auxiliary, or post. |
| app | Searches for modules that are either a client or server attack. |
| author | Searches for modules by author. |
| cve | Searches for modules by CVE ID. |
| bid | Search for modules by Bugtraq ID. |
| osvdb | Search for modules by OSVDB ID. |

### *Defining a Keyword Expression*

A keyword expression consists of a keyword tag and the keyword.

The following table contains examples of keyword expressions:

| Key Tag | KeyWord Expression Example |
|---|---|
| name | name:Java |
| path | path:windows/smb |
| platform | platform:linux |
| type | type:exploit |
| app | app:client |
| author | author:todb |
| cve | cve:2009 |
| bid | bid:10078 |
| osvdb | osvdb:875 |

### *Searching for Modules*

1. Open a project.
2. Click the **Modules** tab.
3. Enter a keyword expression to search for a specific module. Use the keyword tags to define the keyword expression.
4. Press **Enter** to perform a search.

## Module Statistics

Module statistics show the total number of modules that are available and show the number of modules that are available for each type of module. Module types include exploit modules, auxiliary modules, server-side exploits, and client-side exploits.

### *Viewing Module Statistics*

1. Open a project.
2. Click the **Modules** tab. You can view the module statistics from the **Module Statistics** area.

## IPv6 Payloads

The following table describes the IPv6 payloads that are available for Windows, Linux, BSD, Shell, and PHP targets. If the IPv6 payload successfully executes on the target machine, then a session opens on the target machine.

| IPv6 Target | Payloads |
|---|---|
| Windows x86 | stagers/windows/reverse_ipv6_http<br>stagers/windows/reverse_ipv6_https<br>stagers/windows/reverse_ipv6_tcp<br>stagers/windows/bind_ipv6_tcp |
| Linux x86 | singles/linux/x86/shell_bind_ipv6_tcp<br>stagers/linux/x86/reverse_ipv6_tcp<br>stagers/linux/x86/bind_ipv6_tcp |
| BSD x86 | singles/bsd/x86/shell_reverse_tcp_ipv6<br>singles/bsd/x86/shell_bind_tcp_ipv6<br>stagers/bsd/x86/reverse_ipv6_tcp<br>stagers/bsd/x86/bind_ipv6_tcp |
| Shell | singles/cmd/windows/bind_perl_ipv6<br>singles/cmd/unix/bind_netcat_ipv6<br>singles/cmd/unix/bind_perl_ipv6<br>singles/cmd/unix/bind_ruby_ipv6 |

| IPv6 Target | Payloads |
|---|---|
| PHP | singles/php/bind_perl_ipv6<br>singles/php/bind_php_ipv6<br>stagers/php/bind_tcp_ipv6 |

# Exploits

An exploit executes a sequence of commands to target a specific vulnerability found in a system or application. An exploit takes advantage of a vulnerability to provide the attacker with access to the target system. Exploits include buffer overflow, code injection, and web application exploits.

Metasploit Pro offers automated exploits and manual exploits. The type of exploit that you use depends on the level of granular control you want over the exploits.

## Automated Exploits

An automated exploit uses reverse connect or bind listener payloads and do not abuse normal authenticated control mechanisms. Automated exploits cross reference open ports, imported vulnerabilities, and fingerprint information with exploit modules.

When you run an automated exploit, Metasploit Pro builds an attack plan based on the service, operating system, and vulnerability information that it has for the target system. Metasploit Pro obtains this information from the discovery scan or from the information that you provide for the target host. The attack plan defines the exploit modules that Metasploit Pro will use to attack the target systems.

To run an automated exploit, you must specify the hosts that you want to exploit and the minimum reliability setting that Metasploit Pro should use. The minimum reliability setting indicates the potential impact that the exploits have on the target system. If you use a high ranking, such as excellent or great, Metasploit Pro uses exploits that will be unlikely to crash the service or system. Exploits that typically have a high reliability ranking include SQL injection exploits, web application exploits, and command execution exploits. Exploits that corrupt memory will most likely not have a high reliability ranking.

You can also specify the payload type that you want the exploit to use. By default, automated exploits use Meterpreter, but you can choose to use a command shell instead.

### *Automated Exploit Options*

The following table describes the options that are available for automated exploits:

| Option | Description |
|---|---|
| Minimum Reliability: Low | Exploits fail more than 50% of the time for common platforms. |
| Minimum Reliability: Average | Exploits are difficult to reliably leverage against some systems. |
| Minimum Reliability: Normal | Exploits are reliable, but depend on a specific version. Exploits cannot consistently auto-detect. |
| Minimum Reliability: Good | Exploits have a default target and are common to specific types of software. |
| Minimum Reliability: Great | Exploits have a default target. Exploits can auto-detect the appropriate target or use an application specific return address after it runs a version check. Exploits can crash the target, but are the most likely to succeed. |
| Minimum Reliability: Excellent | Exploits never crash the service. Exploits include SQL injection, CMD execution, and certain weak configurations. Most web application flaws belong to this category. |
| Ignore known fragile devices | Bypasses known fragile devices. |
| Payload Type | Defines whether the exploit executes a Meterpreter or command shell payload. |
| Connection Type | Defines the payload connection type. |
| Listener Ports | Defines the range of ports that reverse bind payloads use. |
| Listener Host | Defines the IP address that the payload uses to connect back. Use this option when the address needs to be overridden, such as NAT or Amazon Elastic IPs. |
| Auto Launch Macro | Defines the macro that the exploit runs. |
| Included Ports | Defines the ports to include in the exploit selection. |
| Excluded Ports | Defines the ports to exclude in the exploit selection. |
| Skip exploits that do not match the host OS | Bypasses exploits that do not apply to the target OS. |
| Match exploits based on open ports | Uses port information to match exploits. |
| Match exploits based on vulnerability references | Uses the vulnerability reference information to match exploits. |

| Option | Description |
|---|---|
| Concurrent Exploits | Defines the number of simultaneous exploit attempts that the system runs. The best number varies based upon available CPU horsepower. If you utilize one concurrent attempt, you can debug issues with the task log if you encounter any issues. |
| Time out in Minutes | Defines the number of minutes that the system waits for a given exploit. The default setting ensures that all exploits have sufficient time to complete, but you may need to increase this setting if target hosts are slow. |
| Transport Evasion | This option enables you to send small TCP packets and insert delays between them.<br><br>Low – Inserts a delay of between 1-10 seconds between TCP packets. The delay rate will be constant for a specific module, but will vary across multiple modules.<br>Medium – Transmits small TCP packets; payloads are fragmented into 15 byte payloads.<br>High – Combines the Low and Medium settings by transmitting small TCP packets and inserting delays between them. |
| Application Evasion | Defines application-specific evasion options for DCERPC, SMB, and HTTP-based exploits. These are the only protocols that support evasions. Please note that not all protocols support all levels of evasion.<br><br>DCERPC<br><br>Low – Adds fake UUIDs before and after the actual UUID that the exploit targets.<br>High – Sets the maximum fragmentation size of DCERPC calls to a value between 4 and 64.<br><br>SMB<br><br>Low – Obscures the PIPE string, places extra padding between SMB headers and data, and obscures path names.<br>Medium – Segments SMB read/write operations.<br>High – Sets the max size for SMB reads and writes to 4-64 bytes. |

| Option | Description |
|---|---|
| Application Evasion | HTTP (Client-Server Attacks Only)<br><br>Low – Adds "header folding," which splits HTTP headers into separate lines joined by white space by the server, and adds random cases to HTTP methods. This option adds between 1-64 fake HTTP headers.<br>Medium – Adds 1-64 fake query strings to get requests. Adds 1-64 white space characters between tokens. Adds 1-64 POST parameters.<br>High – Encodes some characters as percent-u unicoded characters (half, randomly), adds a fake "end" to HTTP requests before the attack, and uses backslashes instead of forward slashes. |
| Obtain one session per target | Opens one session per target and bypasses any targets that have a session open. |
| Dry run | Performs a dry run on the exploit, which provides you with details of the exploit, but does not run the exploit. |

### *Running Automated Exploits*

1. Open a project.
2. Click the **Analysis** tab. The **Hosts** window appears.
3. Select the hosts that you want to exploit.
4. Click **Exploit**. The **New Automated Exploitation Attempt** window appears.
5. Verify that target address field contains the addresses that you want to exploit.
6. Select the minimum reliability for the exploit.
7. Click **Show Advanced Options**.
8. Define the target hosts that you want to include or exclude from the exploit.
9. Define the payload options. This determines the type of payload the exploit uses, the type of connection the payload creates, and the listener ports that the exploit uses.
10. Define the exploit selection options. This determines the ports that the exploit includes and excludes from the attack.
11. Define the advanced options. The advanced options lets you define the number of exploits you can run concurrently, the time out for each exploit, and evasion options.
12. Run the exploit.

## Manual Exploits

A manual exploit is a module that you can select and run individually. You perform a manual exploit when you want to exploit a known vulnerability.

You choose the exploit module based on the information you have about the host. For example, if you know that the host runs Windows Service Pack 1, you can run an exploit that targets Windows Service Pack 1 vulnerabilities. Or if you know that the target system has a specific vulnerability that you want to test, you can run the exploit that targets that particular weakness.

Manual exploitation provides granular control over the module and evasion options that an exploit uses. Whereas automated exploits enable you to run simultaneously multiple exploits, manual exploits enable you to run one exploit at a time.

The options and instructions that you perform for manual exploits vary based on the exploit that you choose to run. Therefore, use the following instructions as a guideline to manually run exploits.

### *Manual Exploits Overview*

- Create a list of system targets.
- Create a map of all available exploits using references, ports, and service names.
- Create a match table of exploits for systems, but do not include devices that are fragile or devices that cannot be exploited.
- Create a prioritized queue of exploit modules based on reliability and interleave exploits between hosts.
- Execute exploit modules until Metasploit Pro obtains a session.

### *Running a Manual Exploit*

1. Open a project.
2. Click the **Modules** tab.
3. Use the search engine to find a specific module. Use the keyword tags to define the search term.
4. Click on a module name to select the module. The **Module** window appears.
5. Define the target hosts that you want to include or exclude from the exploit.
6. Define the payload options, if the options are available.
7. Define the module options. Module options vary between modules. Use the in-product help to view descriptions for each option.
8. Define the advanced options. Advanced options vary between modules. Use the in-product help to view descriptions for each option.
9. Define the evasion options. Evasion options vary between modules. Use the in-product help to view descriptions for each option.

10. Run the module.

# Post-Exploitation

After you gain access to a target system, you can run scripts through the command shell or run post-exploitation modules to take control of the system.

## Post-Exploitation Modules

A post-exploitation module provides a standardized interface that you can use to perform post-exploit attacks. The post-exploitation phase enables you to collect further information about a target system and to gain further access to the network. During the post-exploitation phase, you can identify things like additional subnets, routers, server names, network services, and installed applications.

After you obtain a session on the target system, you can view the post-exploitation modules that are applicable for that session.

### *Running Post-Exploitation Modules*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on a session name from the **Active Sessions** column.
4. Click the **Post-Exploitation Modules** tab. The **Module** window appears.
5. Click on a module name from the **Module Name** column. The module information appears.
6. Select the module options you wan to use.
7. Define the advanced options for the module.
8. Run the module.

### *Post-Exploitation Modules for Virtual Targets*

After you gain access to a virtual target, you can utilize post-exploitation modules to interact with the virtual machines. The post-exploitation modules that are available for virtual machines enable you to log into VMware and terminate user sessions and enumerate VirtualBox machines on the target machine.

The following are post-exploitation modules that you can use for virtual machines:

- post/multi/gather/find_vmx
- post/multi/gather/enum_vbox

## Post-Exploitation Macros

A post-exploitation macro is a set of predefined actions that deploy when Metasploit Pro obtains an active session. The session can be an existing session or a session that a task creates, like a campaign task. You can use a post-exploitation macro to automate the events that occur after Metasploit Pro opens a session on a target system.

A post-exploitation macro automatically runs after a target system runs an exploits and connects the post-exploitation macro to a listener. Therefore, before you can execute a post-exploitation macro, you must create a listener and assign the listener to the post-exploitation macro.

To create a listener, you can define a global listener, or you can assign a macro to a campaign. If you create a macro through a campaign, the campaign automatically creates a listener and connects the macro to the listener.

You can manage post-exploitation macros and persistent listeners from the global settings area of the project.

### *Creating a Post-Exploitation Macro*

1. Open a project.
2. Click **Administration > Global Settings** from the main menu. The **Global Settings** window appears.
3. Click **New Macro**, which is located under Post-Exploitation Macros. The **Macros Settings** window appears.
4. Enter a name for the post-exploitation macro.
5. Enter a description for the post-exploitation macro.
6. Enter a time limit, in seconds, for the post-exploitation macro.
7. Save the post-exploitation macro. After you save the post-exploitation macro, a list of available actions displays.
8. Search through the list of modules and find the module that you want to add to the post-exploitation macro.
9. Add the module. The **Module Configuration** window appears.
10. Configure the options for the module. Options vary between modules. Refer to the in-product help for descriptions of the options.
11. Repeat the previous step for each module that you want to add to the post-exploitation macro. Add the modules in the order in which you want the modules to execute.

## Listeners

After an exploit successfully compromises a target system, Metasploit Pro uses a listener to wait for an incoming connection from the exploited system. The listener is the component that handles persistent agents from exploited systems.

When you create a listener, you associate the listener to a specific project. Therefore, when an exploited target makes a connection with the listener, you see an active session open in the project.

**Note:** You can create global listeners that you can use across multiple projects. However, only one project can use the listener at a time.

You assign a post-exploitation macro to each listener. When the exploited system makes a connection with the attacking system, Metasploit Pro launches the post-exploitation macro. Listeners stop after you delete a project or you manually stop a listener.

### *Creating a Listener*

When you create a listener, Metasploit Pro uses the listener address and port to assign a listener name. For example, if the listener address is 10.10.10.1, and the port is 47385, then the port name is 10:10:10:1:47835.

1. Open a project.
2. Click **Administration > Global Settings** from the main menu.
3. Click New Listener, which is located under Persistent Listeners. The **Create a Listener** window appears.
4. Choose an associated project for the listener.
5. Define the listener payload type.
6. Enter an IP address for the listener.

   Note: Metasploit Pro supports IPv4 and IPv6 addresses.
7. Enter a port for the listener.
8. Choose a post-exploitation macro to deploy after the listener connects to the target system.
9. Enable the listener.
10. Save the listener.

### *Enabling and Disabling a Listener*

1. Open a project.
2. Select **Administration > Global Settings** from the main menu. The **Global Settings** window appears.
3. Click on a listener from the **Scope** column.
4. Select or deselect the Enabled option.
5. Update the listener.

### *Stopping a Listener*

To stop a listener, you can either delete the listener from the system or you can stop the listener from the Task screen.

1. Open a project.
2. Click the **Tasks** tab.
3. Find the listening tasks.
4. Click the **Stop** button in the **Timestamp/Duration** column.

# Taking Control of a Session

This chapter covers the following sections:



## Session Overview

An active session provides a connection between the target system and the attacker. Metasploit Pro opens an active session if it can gain access to the host and run a successful attack. After you gain obtain an active session, you can use the active session to take control of the target system.

## Active Sessions

Metasploit Pro opens an active session on a target system if an exploit or bruteforce attack is successful. An active session enables you to interact with and run tasks against the compromised host.

A session can be a Meterpreter or command shell session. The type of session that Metasploit Pro opens depends on the type of attack that the system used to obtain the session.

The session type depends on the mechanism that the attacker uses to create the session and the type of environment on which the session runs. To determine a the session type, open the **Sessions** window and view the **Type** column. The **Type** column lists each session for the session appears.

An active session enables you to take control of the session to perform tasks within the target system.

### Command Shell Session

A command shell session runs a collection of scripts and provides a shell that you can use to run arbitrary commands against the host.

Metasploit Pro opens a command shell session when the following events occur:

- Successful exploit on *nix
- SSH bruteforce on *nix
- Telnet bruteforce on *nix
- Tomcat bruteforce on *nix

### *Interacting with a Command Shell Session*

The command shell functions as a terminal emulator. You can use the command shell to run any non-interactive process on the target host.

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click the active session that you want to open. The session must be a shell session.
4. Click **Command Shell** from the **Available Actions** area. A simulated command shell opens in a new tab in the browser window.

## Meterpreter Session

A Meterpreter session enables you to use VNC to gain access to the device and enables you to use a built-in file browser to upload or download sensitive information.

Meterpreter shells are currently only available for Windows.

Metasploit Pro opens a Meterpreter session when the following events occur:

- Successful exploit on Windows
- SSH bruteforce on Windows
- Telnet bruteforce on Windows
- SMB bruteforce on Windows
- Tomcat bruteforce on Windows

### *Interacting with a Meterpreter Session*

Before you can interact with a Meterpreter session, you must have an active session on a compromised Windows target.

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click the active session that you want to open. The session must be a Meterpreter session.
4. Click **Virtual Desktop** from the **Available Actions a**rea.
5. Choose the Java client or choose to manually connect to an external client.

### Authentication Notes

All successful authentication results in an authentication note attached to the host and an entry in the corresponding reports. Some protocols and servers do not allow you to execute commands directly. For example, you can utilize FTP to bruteforce credentials, but after the attack finds a valid credential, you cannot run commands directly on the server. Therefore, the attacker cannot obtain a session.

When a case like this occurs during a bruteforce attack or an exploit, an alert appears on the **Analysis** tab that indicates that the system identified a valid account, but could not create a session. If the system identifies new credential information for a particular host, you can use the credentials to authenticate the host outside Metasploit Pro.

# Session Tasks

A session task is an action that you can perform within the active session. For example, an action enables you to collect evidence, access the file system, run a command shell, and create a pivot through the compromised host.

Tasks that you can perform include the following:

- Interact with command and Meterpreter sessions.
- Create a proxy pivot.
- Create a VPN pivot.
- Open a VNC session.
- Access a file system.
- Upload files to a remote file system.
- Search through a file system.

To view the tasks that are available for a session, you must view the session details.

### Session Details

The session details describe information about a particular session, such as the session type and attack module that Metasploit Pro used to obtain the session. Additionally, when you view the session details for an active session, you can access the actions that available for that session.

The session details for a closed session describe the event history for the session.

#### *Viewing Details for a Session*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.

3. Click on an active session name. The session details appear and show the actions that are available for the session.

## Proxy Pivot

A proxy pivot send attacks through the remote host and uses the remote host as a gateway over TCP/UDP. When a proxy pivot is active, discovery scans, bruteforce, and exploitation tasks source from the pivoted host.

**Note:** Metasploit Pro does not support IPv6 addresses for pivoting.

### *Creating a Proxy Pivot*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session name. The session details appear.
4. Click **Create Proxy Pivot**. Metasploit Pro automatically creates a route for the session.

## VPN Pivot

A VPN pivot creates a type of VPN tunnel to an exploited Windows host and turns the host into a pivot point for traffic. To create a VPN pivot, Metasploit Pro creates a a hook at the kernel level of the target system. The hook does not create an interface on the remote system and acts as a sniffer to return all traffic that Metasploit Pro initiates.

When Metasploit Pro creates a VPN Pivot, the VPN Pivot appears as a local interface, which enables you to use IP forwarding and use the interface as a gateway to the target network.

However, Metasploit Pro cannot create a bridge to a network that it is already attached to because it creates a conflicting route for the target network system. Therefore, you must verify that Metasploit Pro does not have an existing direct connection to any networks that have the same IP range and netmask as the target network.

**Note:** Metasploit Pro does not support IPv6 addresses for pivoting.

### *Virtual Interfaces*

In order to provide VPN pivot functionality on the Windows platform, Metasploit Pro must install a new network driver. The driver, `msftap.sys`, creates four virtual interfaces on the installed system, which provides the ability to run up to four concurrent VPN Pivot sessions.

If Metasploit Pro does not locate the virtual interfaces when MetasploitProSvc starts, Metasploit Pro automatically installs the network drivers. To reinstall or uninstall these drivers, you can use one of the batch scripts that are available. You can locate the batch scripts at: `$INSTALLROOT\apps\pro\data\drivers\<arch>\`. You can use the scripts to disable the VPN Pivot virtual interfaces or restore a previously removed driver.

### *Creating a VPN Pivot*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session name. The session details appear.
4. Click **Create VPN Pivot**. Metasploit Pro automatically creates a route for the session.

## VNC Sessions

You can use an active Meterpreter session to obtain a VNC session with the compromised system. You can either connect to the remote desktop manually or use the VNC client that is available through Metasploit Pro.

The VNC client is a Java applet that you can use to remote desktop to the target system. Before you use the Java applet, install the latest Java for your platform. You can download the latest version of Java at http://www.java.com/en/download/manual.jsp. If you do not want to use the Java applet, you can use an external client, such as VNC Viewer.

### *Opening a VNC Session*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session. The session details appear.
4. Click **Virtual Desktop** to connect to the remote desktop.
5. Click **OK** when the confirmation window appears.
6. Choose to connect manually or to use a Java applet.

## File Systems

For Meterpreter sessions, you can use the Metasploit Pro interface to browse the file system on the compromised system. Additionally, you can upload, download, or delete files.

### *Accessing the File System*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session. The session details appear.
4. Click **Access File System**. A new window appears and displays the remote file system.

### *Uploading File to a File System*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session. The session details appear.

4. Click **Access File System**. A new window appears and displays the remote file system.
5. Select the directory that you want to use to upload the file. You can enter the directory path or navigate through the directory and select the directory path that you want to use.
6. Click **Upload**.
7. Browse to the location of the file that you want to upload. After you locate the file, select and open the file.
8. Enter a name for the file. If you do not specify a name, the file uses `empty` as the name.
9. If you want to run the file after you upload the file to the file system, select the **Run the file** option.
10. Upload the file.

### *Searching the File System*

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session. The session details appear.
4. Click **Search File System**. A new window appears and displays the remote file system.
5. Enter the file name that you want to use to perform the search.
6. Press **Enter**.

# Application Scanning and Exploitation

This chapter covers the following topics:



## Application Scanning and Exploitation Overview

Application scanning and exploitation is the process that searches for vulnerabilities in active web content and forms and exploits them. To perform application scanning and exploitation, you can use the web app scan, web audit, and web exploitation features. Metasploit Pro bundles these features into the Web Apps feature.

Metasploit Pro can identify Cross Site Scripting (XSS), SQL Injection (SQLi), Remote and Local File Include, and Command Injection issues. Metasploit Pro can also replay XSS and SQLi and exploit Remote File and Command Injection.

Application scanning and exploitation consists of the following general steps:

1. Run a web app scan, which determines if there are any active forms or content running on the host.
2. Audit the applications to identify any vulnerabilities that exist in web forms and active content.
3. Run web exploits on vulnerabilities that the web audit discovers.

## Web App Scan

A web app scan is the process that Metasploit Pro uses to spider web pages and applications to search for active content and forms.

In order to achieve the correct web app scan configuration, you may need to configure the spider settings multiple times before you achieve the results that you want.

**Note:** Typical applications may take over 5,000 requests to spider.

## IPv6 Addresses

Metasploit Pro supports IPv6 addresses for URLs; however you must enclose the IPv6 address in parenthesis for the web scan to process the address.

## Web App Scan Options

The following table describes the options that are available for a web app scan:

| Option | Description |
|---|---|
| URLs | Defines a list of URLs that the web crawler uses as a starting point. To specify a custom virtual host, prefix the name to the address and add a comma to separate name from the address. For example, use `intranet,http://192.168.0.1`. |
| Maximum requests | Defines the maximum number of pages that the web crawler requests for each web page. |
| Time limit | Defines the maximum amount of time, in minutes, that the web crawler spends on each web site. |
| Concurrent Requests | Defines the maximum number of concurrent requests |
| HTTP user name | Defines the user name that the web crawler uses for authentication for each request. |
| HTTP password | Defines the password that the web crawler uses for authentication for each request. |
| HTTP cookie data | Sets the seed for the initial cookie for each request. |
| HTTP user agent | Defines the user agent that the web crawler sends in each request. |

## Running a Web Apps Scan

1. Open a project.
2. Click the **Web Apps** tab. The W**eb Applications** window appears.
3. Click **WebScan**. The **Web Application Scan** window appears.
4. Enter a list of URLs that the web crawler uses.

   Note: If you need to enter an IPv6 address, you must enclose the address in parenthesis. For example, use `http://[fde2:b7c5:94b2:ffaa:20c:29ff:fe6c:ebdb]`.

5. Configure the web app scan options.
6. Launch the web app scan.

# Web Audit

A web audit is the process that searches for vulnerabilities in Web forms and active content that the web crawler discovers. A web audit can discover the following classes of issues: XSS, SQL Injection, and LFI/RFI.

Before you can perform a web audit, you must run a web scan.

## Web Audit Options

The following table describes the options that are available for a web audit:

| Option | Description |
|---|---|
| Maximum request/form | Defines the maximum number of requests that the web audit requests for each form. |
| Time limit/form | Defines the maximum number of time, in minutes, that the web audit spends on each form. |
| Instance limit/form | Defines the maximum number of unique for instances that the web audit tests. |
| HTTP user name | Defines the user name that the web audit uses for authentication for each request. |
| HTTP password | Defines the password that the web audit uses for authentication for each request. |
| HTTP cookie data | Sets the seed for the initial cookie for each request. |
| HTTP user agent | Defines the user agent that the web audit sends in each request. |

## Running a Web Audit

1. Open a project.
2. Click the **Web Apps** tab. The **Web Applications** window appears.
3. Click **Audit Web Apps**. The **Web Application Audit** window opens.
4. Configure the Web Application Audit options.
5. Select the target web applications that you want to web audit. Metasploit Pro populates the target web applications list with the information the web crawler collects during the web app scan.
6. Launch the web audit.

# Web App Exploit

A web app exploit targets vulnerabilities that the web audit identifies.

Before you can run a web app exploit, you must perform a web app scan and web audit.

## Web App Exploit Options

The following table describes the options that are available for a web app exploit:

| Option | Description |
|---|---|
| Timeout in Minutes | Defines the maximum amount of time, in minutes, that the system allocates to each exploit. |
| Connection Type | Defines the payload type for each exploit. Payloads include:<br>• Reverse - Initiates a connection from the target system to the attacker.<br>• Bind - Forces the target to open a listening port on the target system.<br>• Auto - Selects the best method for the attacker to create a connection to the target system. |

## Running a Web App Exploit

1. Open a project.
2. Click the **Web Apps** tab. The **Web Application** window appears.
3. Click **Exploit Web Apps**. The **Exploit Web Applications** window appears.
4. Enter the maximum of time that the system allots to each exploit.
5. Specify the connection type for each exploit.
6. Launch the exploits.

# Evidence Collection

This chapter covers the following topics:



## Evidence Collection Overview

The system data that Metasploit Pro collects from a compromised host is called evidence. Evidence helps you determine the success of an exploit. You can use evidence to perform further analysis and penetration of a target system. Evidence includes system information, screen shots, password hashes, SSH keys, and other sensitive information.

## Collecting Evidence

You can collect system data for an active session.

### Collecting Evidence for a Project

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click **Collect**.
4. Select the sessions you want to use to collect evidence.
5. Select if you want to collect system information.
6. Select if you want to collect system passwords.
7. Select if you want to include screen shots.
8. Select if you want to collect SSH keys.
9. Select if you want to collect any other files besides the ones that you have already selected.
10. Enter a regular expression to filter the results by file name pattern.
11. Enter the maximum number of files that you want to collect for each session.
12. Enter the maximum file size that you want to enforce on each file in each session.
13. Collect the system data.

### Collecting Evidence for an Active Session

1. Open a project.
2. Click the **Sessions** tab. The **Sessions** window appears.
3. Click on an active session name. The session details appear.
4. Click **Collect System Data.**
5. Select the sessions you want to use to collect evidence.
6. Select if you want to collect system information.
7. Select if you want to collect system passwords.
8. Select if you want to include screen shots.
9. Select if you want to collect SSH keys.
10. Select if you want to collect any other files besides the ones that you have already selected.
11. Enter a regular expression to filter the results by file name pattern.
12. Enter the maximum number of files that you want to collect for each session.
13. Enter the maximum file size that you want to enforce on each file in each session.
14. Collect the system data.

### Password Cracking

Metasploit Pro automatically performs offline password cracking when it runs the collection task. If Metasploit Pro finds a hash supported by John the Ripper (JtR) during the collection process, the password cracker uses the LANMAN and NTLM formats to attempt to crack the password. Metasploit Pro tries to crack the word list using a combination of rules and incremental modes in both LANMAN and NTLM formats. Metasploit Pro parses any cracked passwords and adds the password to the word list.

# Collected Evidence

Evidence is information that Metasploit Pro collects about a target system.

### Viewing Evidence for a Session

1. Open a project.
2. Click the **Sessions** tab. The Sessions window appears.
3. Click on an active session name. The session details appear.
4. Click the **Stored Data & Files** tab.
5. Scroll through the list to view the stored data or download the evidence.

### Exporting Collected Evidence

1. Open a project.
2. Click the **Reports** tab. The **Reports** window appears.
3. Click **Export Data**.
4. Select an export format. Choose from XML, ZIP, Replay, PWDump, XML, PDF, and RTF.
5. Enter the addresses that you want to include and exclude in the exported data.
6. Choose if you want to mask user names and passwords.
7. Export the data.

# Session Clean Up

When you need to close an active session, you perform a session clean up. A session clean up retrieves evidence from the session and closes the session.

After you close a session, the session appears under the Closed Sessions list. You can view the session event history, but you can no longer interact with the session.

### Cleaning Up a Session

1. Click the **Sessions** tab.
2. Click **Cleanup**. A list of active sessions appears.
3. Select the sessions that you want to clean up.
4. Click **Cleanup Sessions**.

# Social Engineering

This chapter covers the following topics:



## Social Engineering Overview

Social engineering is a method of attack that typically uses a delivery tool, such as e-mail or a USB key, to target a local user. Social engineering focuses on the human factor and attempts to induce a user to share sensitive and confidential information. To target a victim, an attacker may send an e-mail that contains a linked web page requesting information or an attachment that installs malware.

Most recent vulnerabilities are client-side vulnerabilities, which are exploitable through vectors that only a local user can reach. Social engineering utilizes client-side exploits in order to target the applications or information stored on a target's local machine. For example, an attacker might attach a file that contains an exploit to an e-mail. When someone opens the attachment, the exploit may install a key logger or some other form of malware on the system.

In Metasploit Pro, you create and run campaigns to perform social engineering attacks. Social engineering campaigns can run phishing attacks, file format exploits, the browser autopwn module, and java signed applets. Metasploit Pro tracks the targets that succumb to the attack and presents the tracked data in the social engineering report.

An organization may want to perform social engineering tests to gauge how well their employees protect sensitive information or to identify vulnerabilities in their security infrastructure. The results gathered from social engineering can help an organization educate their employees about the security landscape and improve their security posture.

### Social Engineering General Workflow

Use the following general steps to set up a social engineering campaign:

1. Create a campaign.
2. Create a template, if the campaign is an e-mail or web campaign.

3. Run the campaign.

## Social Engineering Components

Social engineering consists of the following components:

- **Campaigns** - A container for a social engineering attack. Use a campaign to specify the content, attack configuration, delivery method, and target list for a social engineering attack.
- **Templates** - A file that automatically defines the web or e-mail content within a campaign.
- **Target Lists** - A list that defines the recipients and their e-mail addresses that the social engineering campaign targets.

# Campaigns

A campaign is a social engineering feature that you use to configure and implement client-side attacks and phishing scams. It represents your workspace for a social engineering attack. Within a campaign, you can define the campaign component, content, attack configuration, delivery method, and the target list for the social engineering attack. Create campaigns to set up the social attack that you want to execute to either gather information from a group of targets or to exploit them.

A campaign can be an e-mail, web, or USB drive campaign. Use campaigns to build a social engineering attack. For example, you can create a campaign that contains an e-mail and a web campaign. When you run the campaign, it sends an e-mail that contains a link to a web page.

Every campaign must have at least one campaign type configured. Most campaigns will have an e-mail campaign because it is the most commonly used delivery method for social engineering attacks. In addition to the e-mail component, you can add an attack method, such as a web page or malicious file to the campaign.

## E-mail Campaign

E-mail is the delivery tool that you use to send social engineering attacks to your target list. To send e-mail, you must configure the SMTP settings for your mail server, supply the e-mail content, and define the sender and recipient information. In most cases, your campaign will contain an e-mail component if you plan to send an exploit to a target.

After you configure and save the e-mail campaign, Metasploit Pro displays the e-mail template configuration page. The e-mail template defines the subject, body, and attack method that the e-mail campaign uses.

### *E-mail Campaign Options*

The following table describes the options that are available for an e-mail campaign:

| Option | Description |
|---|---|
| Send e-mail | Enables the e-mail campaign. |
| Subject | The subject that displays in the message header and the subject line. |
| From Address | The sender's e-mail address. |
| From Name | The sender's name. |
| Use SSL? | Uses SSL to send e-mail. SSL ensures that the e-mail content, user name, and password are encrypted. |
| SMTP Server | The SMTP server name. |
| SMTP Port | The SMTP port number. |
| SMTP User Name | The user name required for authentication. This field is not required if the SMTP server does not need to be authenticated. |
| SMTP - Password | The password required for authentication. This field is not required if the SMTP server does not need to be authenticated. |
| Display Address | The from header that displays in the e-mail body. For example, use a display address like the following: `Joe Smith <joe_smith@yourcompany.com>`. |
| E-mail Addresses | The list of targets, or recipients, that you want to receive the e-mail. Use CSV formatting to create a target list. The CSV file must include the following header row: `email_address, first_name, last_name`. |

## Web Campaign

A web page is an HTML page that a target can access online. The web page can be an online form that solicits information or it can be a simple message to the target that they should have not opened the web page.

### *Web Campaign Options*

The following table describes the options that are available for a web campaign:

| Option | Description |
|---|---|
| Start a web server | Enables the web campaign. |
| Web Server Listen Address | The host name that you want to use to serve the web page. For example, `www.metasploit.com`. |
| Web URI for Exploits | The resource name that you want to use to identify file or location on the web server. For example, `/file.html`. |
| Web Port | The port the web server uses. The default port is 80. |
| Use SSL | Uses SSL to encrypt data. |

## USB Drive Campaign

A USB drive campaign contains an executable file that automatically runs when someone opens the file.

### *USB Key Options*

The following table describes the options that are available for the USB key component:

| Option | Description |
|---|---|
| Generate an executable for manual delivery | Generates an executable file that you use to attach to an e-mail or web campaign. |
| Listener Callback Port | The port that Metasploit Pro uses to connect to a client, if a target runs the executable file and successfully exploits the target. |
| Filename | The name for the executable file that Metasploit Pro creates. For example, `clickme.exe`. |

## Creating a Campaign

1. Open a project.
2. Click the **Campaigns** tab.
3. Create a new campaign.
4. Enter a name for the campaign.
5. Enter an IP address for the listener.

Note: Metasploit Pro does not support IPv6 addresses for campaigns.

6. Select a post-exploitation macro for the campaign to run after Metasploit Pro compromises the target system.
7. If you want to use a web server, select the **Start a web server** option and define the web server information.
8. If you want to generate an executable, select the **Generate an executable** for manual delivery option and define the information for the executable file. When you enable this option, you can attach the executable when you create the e-mail template.
9. Define the payload settings for the campaign.
10. If you want to send an e-mail as part of the campaign, enable the **Send e-mail** option.
11. Save the campaign.

## Running a Campaign

You can run a campaign after you configure the campaign components that you want to use.

1. Open the campaign that you want to run. The Campaign window appears.
2. Verify that the components that you want to use have the correct configurations.
3. Start the campaign.

# Web Templates

Web templates define the content that Metasploit Pro uses for phishing attacks.

Before you can create a web template, you must create a campaign and enable the web server option for the campaign. If you enable the web server option, the Web Template window appears after you create the campaign.

## Web Template Options

The following table describes the options that are available for a web template:

| Option | Description |
|---|---|
| Exploit Type | The social engineering attack that the web page contains. |
| HTML Template | The HTML content for web page. |
| Clone URL | Clones the HTML from a website. |

| Option | Description |
|---|---|
| Exploit Type - Start Browser Autopwn | An option that runs a module that fingerprints HTTP clients and automatically attempts to exploit them based on their browser information. |
| Exploit Type - Start a specific browser exploit | An option that allows you to choose a specific exploit that you want to attach to the web page. |
| Exploit Type - Don't start any browser exploits | An option that allows you to run a web campaign without an exploit. |

## Creating a Web Template

1. Use the HTML editor to create a custom web template or use the clone URL feature to copy the data for an existing URL.
2. Select an exploit setting.
3. Save the web template.

## Cloning a Web Template

If you do not want to create a custom web template, you can clone an existing web template. When you clone a web template, you copy the template name, body content, and exploit settings into a new web template. Additionally, you can attach a file-format exploit to the e-mail.

To clone a web template, select the web template that you want to clone from the **Clone** drop-down menu.

# E-mail Templates

An e-mail template defines the subject and message that the phishing attack uses.

Before you can create an e-mail template, you must create a campaign and select the **Send e-mail** option for the campaign. When you enable the **Send e-mail** option, the **E-mail Template** window appears after you create the web template.

### *E-mail Template Options*

The following table describes the options that are available for an e-mail template:

| Option | Description |
|---|---|
| Template Name | The name that you want to assign to the template. |
| Subject | The subject for the e-mail. |

| Option | Description |
|---|---|
| Body | The content that displays as the e-mail message. |
| Attach Executable Payload | The executable file generated by Metasploit Pro that you can use as a USB drive. |
| Attach File-Format Exploit | The module, or exploit, that you want to attach to the e-mail. |
| Add Attachment | Any attachment that you want to add to the e-mail. For example, you can upload a custom executable file. |

### Creating an E-mail Template

1. Enter a name for the template.
2. Enter the subject for the e-mail.
3. Enter the body for the e-mail.
4. Select if you want to attach an executable payload to the e-mail.
5. Select if you want to attach a file format exploit to the e-mail. If you select this option, you must define a name for the file. The name is visible to the e-mail recipient. Then, choose an exploit module to attach to the e-mail.
6. Select if you want to add an attachment to the e-mail. If you add an attachment to the e-mail, you must define the file name and content type for the attachment. Additionally, you must upload the file that you want to attach to the e-mail.
7. Save the e-mail template.

# Target Lists

When you create and configure an e-mail campaign, you must add a target list that includes all the recipients that you want the campaign to target. You can add one target at a time or you can import a txt file that contains a comma separated list of targets.

The **E-mail Addresses** window appears after you create an e-mail template. From the **E-mail Addresses** window, you can add and import the e-mail addresses that the campaign uses.

### Adding an E-mail Address to a Campaign

1. Open the E-mail Addresses window.
2. Click the **Add Email Address** link.
3. Enter an e-mail address.
4. Optionally enter a first name and last name for the e-mail account.
5. Click the **Add Email Address** link to continue to add e-mail addresses.

6. Save the e-mail addresses when you are done.

## Importing an E-mail List for a Campaign

A target list defines the recipients and their e-mail addresses that you want to receive the social engineering attack. You must use CSV formatting to create a target list and import the list into Metasploit Pro.

The CSV file must include the following header row: `email_address, first_name, last_name`. The following is an example of a target list:

```
e-mail, first_name, last_name
joe@yahoo.com, joe, smith
mary@yahoo.com, mary, taylor
```

To import a target list:

1. Open the E-mail Addresses window.
2. Click **Import Addresses**.
3. Browse to locate the txt file that contains the e-mail list.
4. Open the txt file.
5. Import the txt file.

# REPORTS

This chapter covers the following topics:



## Reports Overview

A report provides detailed information and results for the penetration test. Use reports to perform an analysis of the target network and to provide valuable information to help solve and mitigate security vulnerabilities.

A report contains the information that you obtain during a penetration test. Reports help you identify vulnerabilities in a target network and help you to pinpoint how an organization can strengthen their security infrastructure.

You can generate and export a report in PDF, Word, RTF, and HTML.

## Standard Reports

A standard report provides default report formats that you can use to generate a report.

Metasploit Pro provides the following report formats:

- **Audit reports** – Covers all high-level data for the project, combining many available details into one unified view.
- **Compromised reports** – Details all hosts on which Metasploit was able to open a session, hosts on which a Metasploit module was successfully run, and hosts where a vulnerability was recorded.
- **Authentication token reports** – Details all cracked hosts, passwords, SMB hashes, and SSH keys that were collected and discovered.
- **Services reports** – Details all available network services discovered
- **Collected evidence reports** – Covers all looted hosts. Describes the files and screenshots that were collected from compromised hosts.
- **Campaigns reports** – Details all social engineering campaigns that were launched as part of the project.

- **Web app reports** – Enumerates all web sites and their vulnerabilities, forms, and pages.
- **PCI compliance reports** – Uses PCI compliance criteria to analyze the hosts.
- **FISMA compliance reports** – Uses FISMA compliance criteria to analyze the hosts.

## Generating a Standard Report

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears.
3. Click **Standard Report**. The **New Report** window appears.
4. Choose a report type.
5. Choose an audit report format, or the format that you want to use to generate the report.
6. Enter a name for the report. You can enter up to 63 characters and use alphanumeric characters, dashes, hyphens, periods, and spaces.
7. Specify the hosts that you want the report to include and exclude.
8. Select the report sections that you want to include in the report.
9. Choose if you want to mask any passwords, SMB hashes, or SSH keys.
10. Choose if you want to include detailed information for each session action.
11. Choose if you want to include charts and graphs in the report.
12. Generate the report. All generated reports appear under the **Saved Reports and Data Exports** area.

## Viewing a Report

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears
3. Click **View** to view any report.

## Downloading a Report

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears
3. Find the report that you want you to download from the **Saved and Data Exports** list.
4. Download the report. A window appears and prompts you to open or save the report.
5. Click **OK** when you are done.

## Deleting a Report

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears
3. Find the report that you want you to delete from the **Saved and Data Exports** list.
4. Click **Delete**. A window appears and prompts you to confirm the selection.
5. Click **OK**.

# PCI Compliance Reports

Metasploit Pro provides the ability to generate PCI reports for your penetration test. The findings should be used as an appendix for PCI standards testing and not as an actual audit.

Visit PCI for the latest requirements document.

Metasploit Pro tests for and reports on the following PCI standards:

- 2.2.1 – Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.
- 2.3 – Encrypt all non-console administrative access such as browser/Web-based management tools.
- 6.1 – Ensure that all system components and software have the latest vendor-supplied security patches installed. Deploy critical patches within a month of release.
- 8.2 – Employ at least one of these to authenticate all users: password or passphrase; or two-factor authentication.
- 8.4 – Render all passwords unreadable for all system components both in storage and during transmission using strong cryptography based on approved standards.
- 8.5 – Ensure proper user authentication and password management for non-consumer users and administrators on all system components.
- 8.5.8 – Do not use group, shared, or generic accounts and passwords, or other authentication methods.
- 8.5.10 – Require a minimum password length of at least seven characters.
- 8.5.11 – Use passwords containing both numeric and alphabetic characters.

## Generating a PCI Report

1. Open a project.
2. Click on the **Reports** tab. The **Reports** window appears.
3. Click **Standard Report**.
4. Select **PCI Compliance Report** for the **Report Type**.
5. Select PDF, RTF, HTML, or XML for the report format.

6. Enter a name for the report.
7. Specify the addresses that you want the PCI Report to include or exclude.
8. Choose if you want to mask discovered passwords.
9. Generate the report. You can view the report from the **Saved Reports and Exported Data** area of the Reports page.

### Viewing a PCI Findings Report

1. Open a project.
2. Click on the **Reports** tab. The **Reports** window appears.
3. Locate the **Saved Reports and Exported Data** area.
4. Download the report you would like to view. Select whether to save the report to a location on your computer or view the report immediately.

# FISMA Compliance Report

Metasploit Pro provides the ability to generate FISMA reports for the penetration test. The generated FISMA report is an appendix for an SP800-53r3 FISMA Compliance Audit.

Metasploit Pro tests for and reports on the following FISMA requirements:

- AC-1: Access Control Policy and Procedures
- AC-4: Information Flow Enforcement
- AC-7: Unsuccessful Login Attempts
- AT-1: Security Awareness and Training Policy and Procedures
- AT-2: Security Awareness
- CM-1: Configuration Management Policy and Procedures
- •CM-7: Least Functionality
- RA-1: Risk Assessment Policy and Procedures
- RA-5: Vulnerability Scanning
- IA-1: Identification and Authentication Policy and Procedures
- IA-2: User Identification and Authentication
- IA-7: Cryptographic Module Authentication
- IA-8: Identification and Authentication (Non-organizational users)
- SI-1: System and Information Integrity Policy and Procedures
- SI-2: Flaw Remediation
- SI-10: Information Output Handling and Retention

## Generating a FISMA Compliance Report

1. Open a project.
2. Click on the **Reports** tab. The **Reports** window appears.
3. Click **Standard Report**.
4. Select **FISMA Compliance Report** for the **Report Type**.
5. Select PDF, RTF, XML, or HTML as the report format.
6. Enter a name for the report.
7. Specify the addresses that you want the PCI Report to include or exclude.
8. Choose if you want to mask discovered passwords.
9. Generate the report. You can view the report from the **Saved Reports and Exported Data** area of the Reports page.

## Viewing a FISMA Compliance Report

1. Open a project.
2. Click on the **Reports** tab. The **Reports** window appears.
3. Locate the **Saved Reports and Exported Data** area.
4. Download the report you would like to view. Select whether to save the report to a location on your computer or view the report immediately.

# Custom Reports

A custom report is a report that you use template to generate. You can generate a custom report with a template that you created or with a Metasploit Pro template.

Metasploit Pro provides a JRXML template that you can use to customize a template. To build a custom template, you should download the template and use the template as a starting point for the custom template.

To customize a report template, you must be familiar with Jasper iReports, JasperReports, XML, Java, and SQL.

## JasperReports

JasperReports is an open source Java based reporting engine, or library, that Metasploit Pro uses to generate standard and custom reports. Metasploit Pro builds reports with the JasperReports reporting format, JRXML.

### *How JasperReports Works*

JasperReports operates similarly to a compiler. You create a JRXML file, which defines the instructions that determine where the report places text, puts images, and retrieves data. The Jasper compiler compiles the JRXML file to generate a report.

After you have a compiled report, the Jasper engine accesses the data source to pull data for the report. The combination of the data source and a Jasper report enable you to produce a report in PDF, HTML, RTF, and Word.

For more information on JasperReports, visit http://jasperforge.org/projects/jasperreports.

### *JasperReport and iReport Resources*

Use the following resources to learn more about iReport and JasperReport:

- iReport Ultimate Guide Documentation
- Chart Customizations article
- Report Design
- JasperReports Wiki
- Groovy documentation

### *Jasper iReport*

If you want to create a custom report template, you can use a GUI based program like Jasper iReport to design the layout and appearance of the template. Jasper iReport is the open source report designer that is available from JasperReports. With Jasper iReport, you can visually design reports without knowledge of the JasperReports library, XML, and Java.

The easiest way to create a custom template is to use the simple template that is available in Metasploit Pro as a starting point. The simple template uses Jasper iReport's default template and uses a single SQL query to create a table of host machines and a count of the services and vulnerabilities that are available for each host.

For more information on JasperReports, visit http://jasperforge.org/projects/jasperreports.

### *Data Source Parameters*

You can use data source parameters to define SQL queries to a database. The SQL queries that you define determine the data that displays in the report.

To build a report template, you must include the `workspace_id` parameter. The `workspace_id` parameter populates the report with data that is relevant for the current project.

In iReport, when you define the query that the report engine uses to retrieve the database fields, you must pass the `workspace_id` parameter as part of a `WHERE` clause in the SQL

statement that populates the data source. For example, you can enter `SELECT * FROM hosts WHERE workspace_id = $P{workspace_id}` to select the discovered hosts for a specific project.

## Downloading the Simple or Default Template

1. Open a project.
2. Click the **Reports** tab. The **Reports** window appears.
3. Click on the **Download Default Template** or **Download Simple Template** download links below the **Saved Reports and Data Exports** area.
4. Save the template to a location on your computer.

## Uploading a Custom Template

The custom template must have a JRXML, or Jasper file, extension.

1. Open a project.
2. Click the **Reports** tab. The **Reports** window appears.
3. Click **Upload Custom Report Collateral**.
4. Browse to the location of the custom report template and select the template. Click **Open**.
5. Enter a descriptive name for the template.
6. Upload the template. The template appears under the Custom Templates and Logos area. You can choose the template when you create a custom report.

## Uploading a Logo for Custom Reports

You can upload a logo to a project. The logos that you upload are globally available for you to add to any report that you generate within the project.

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears.
3. Click **Custom Report**. The **New Custom Report** window appears.
4. Click **Upload Custom Report Collateral**.
5. Click **Browse** and locate the logo file that you want to upload. Metasploit Pro supports GIF, JPEG, JPG, and PNG files.
6. Enter a name for the file.
7. Upload the file. The file appears under the **Custom Templates and Logos** area. You can choose the logo file when you create a custom report.

## Adding a Logo to a Custom Report

You can add a custom logo to a report. The custom logo that you use replaces the default Rapid7 logo on the cover page and footer of the report.

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears.
3. Click **Custom Report**. The **New Custom Report** window appears.
4. Choose a custom report format. You can choose PDF, Word, RTF, or HTML to generate the report.
5. Enter a name for the report. You can enter up to 63 characters and use alphanumeric characters, dashes, hyphens, periods, and spaces.
6. Specify the hosts that you want the report to include and exclude.
7. Click the **Custom report logo** dropdown and select the logo that you want to use.
8. Select the report sections that you want to include in the report.
9. Choose if you want to include detailed information for each session action.
10. Choose if you want to include charts and graphs in the report.
11. Generate the report. All generated reports appear under the **Saved Reports and Data Exports** area.

## Creating a Custom Report

Before you can create a custom report, you must upload a custom template to Metasploit Pro. Additionally, if you want to include a logo in the report, you must upload the GIF, JPEG, JPG, or PNG file for the image.

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears.
3. Click **Custom Report**. The **New Custom Report** window appears.
4. Choose a custom report format. You can choose PDF, Word, RTF, or HTML to generate the report.
5. Enter a name for the report. You can enter up to 63 characters and use alphanumeric characters, dashes, hyphens, periods, and spaces.
6. Specify the hosts that you want the report to include and exclude.
7. Choose the custom report template that you want to use to generate the report.
8. Select the report sections that you want to include in the report.
9. Choose if you want to include detailed information for each session action.
10. Choose if you want to include charts and graphs in the report.
11. Generate the report. All generated reports appear under the **Saved Reports and Data Exports** area.

# E-mailing Reports

You can choose to automatically send the report to a list of recipients after the system generates the report. To e-mail reports, you must define your mail server settings, enable the e-mail report option, and define the recipients.

E-mailing reports is particularly useful if you have task schedules in place. When you create a task schedule, you can add a report task to the end of a task chain to signify that you want to generate a report after the system finishes the task chain. If you configure the report task to e-mail the report, then the system automatically sends a report using the mailer information that you define for the report task.

Metasploit Pro uses the SMTP settings that configured in the Global Settings to e-mail the report to your recipient list. You must configure the SMTP settings before you can e-mail a report. To set up your mail server, select **Administration > Global Settings** and define the SMTP settings.

The default sender for reports is reports@pro.metasploit.com. You may want to add this e-mail address to the safe sender list to ensure that these e-mails are not moved to the Junk Mail folder. You cannot change the default sender through the Metasploit Web UI, but you can use the Metasploit Console to edit the sender.

## E-mailing a Report

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears.
3. Choose whether you want to generate a standard report or custom report.
4. Select the report type.
5. Select the report format.
6. Specify a name for the report.
7. Define the hosts that you want to include and exclude from the report.
8. Choose whether you want to mask discovered passwords and include session details.
9. Under Email Report To, select the **Email** option to enable the e-mail report feature.
10. In the **Recipients** box, enter the e-mail addresses that you want Metasploit Pro to send the report to. Use a comma or semi-colon to separate multiple e-mail addresses.
11. Generate the report.

# Replay Scripts

A replay script enables you to replay an attack without Metasploit Pro. Anyone who has access to the Metasploit Framework can use a replay script to replay an attack.

## Exporting Replay Scripts

1. Open a project.
2. Select the **Reports** tab. The **Reports** window appears.
3. Click **Export Data**. The **Export Project Data** window appears.
4. Choose **Replay (Scripts)** from the report format list.
5. Enter the addresses that you want the report to include or exclude.
6. Choose if you want to mask user names and passwords.
7. Choose if you want to include the activity log in the exported file.
8. Generate the replay script. The exported file appears under the **Saved Reports and Data Exports** area.

# Task Chains

This chapter covers the following topics:



## Task Chains Overview

A task chain is a series of tasks that you can automate to run at a specific time and date. To set up a task chain, you need to define a schedule for task chain to follow and configure the tasks that you want to be part of the task chain.

A task chain enables you to easily automate the execution of tasks within a project. For example, an organization may only allow you to access a system during a certain time frame, like between 12 and 4 a.m. Since that may not be an optimal time for you to manually run the tasks, you can create a task chain to automate tasks to run during that time frame.

Additionally, you may want to create a task chain when you want to perform a series of tasks and you don't want to wait for each task to finish before you run the next task. For example, if you want to perform a scan, run a bruteforce attack, and generate a report, you can create a task chain that runs those tasks in sequence.

### Task Chain Components

A task chain consists of tasks, a chain, and a schedule. The following sections describe the components of a task schedule.

#### *Task*

A task represents an action that the system can perform, such as a scan, bruteforce attack, exploitation, report generation, and data collection.

#### *Chain*

A chain is a series of tasks that you link together. The system runs tasks in the order in which they appear in the chain. When you add a task, the system adds it to the bottom of the chain.

### *Schedule*

A schedule determines the recurrence of a task chain. You can set the task chain to run once, regularly at set times, or immediately after you create it. Additionally, you can define the time and date that the schedule follows.

# Working with Task Chains

You can create task chains to automate the system to run a series of tasks at a specific time and date. A task schedule is specific to a project, and you can create multiple task schedules within a project.

The Metasploit Web UI provides an streamlined interface that you can use to set up a task chain and an interactive clock and calendar that you can use to define the schedule.

When you add a task to a task chain, the configuration page for the task appears. You configure the task as you normally would. The options and settings behave the same as they would if you configured them outside of a task schedule.

After you create a task chain, the system runs the task chain according to the schedule that you define for it.

## Supported Tasks

The following list describes the tasks that you can add to a task chain:

- Scan
- Import
- Nexpose Scan
- Bruteforce
- Exploit
- Module Run
- Collect Evidence
- Clean up
- Report

## Recurrence Settings

The recurrence settings define the frequency that a task chain runs and the schedule task chain follows. You can run the schedule once, daily, weekly, or manually.

The following table describes the recurrence types:

| Recurrence Setting | Description |
|---|---|
| Run manually | Use this option if you do not want the task chain to follow a schedule. This option saves the task chain so that you can choose when you want to run it.<br><br>When you run the task chain, the system schedules it to run within the next minute. |
| Run now | Use this option if you want to run the task chain after you create it. There may be a small delay from the time you run the task chain to the time the task chain starts. |
| Run in the future | Use this option to create a schedule for the task chain. This option enables you to run the task chain on a daily, and weekly schedule.<br><br>If you choose to run the task chain in the future, the scheduling information displays. |

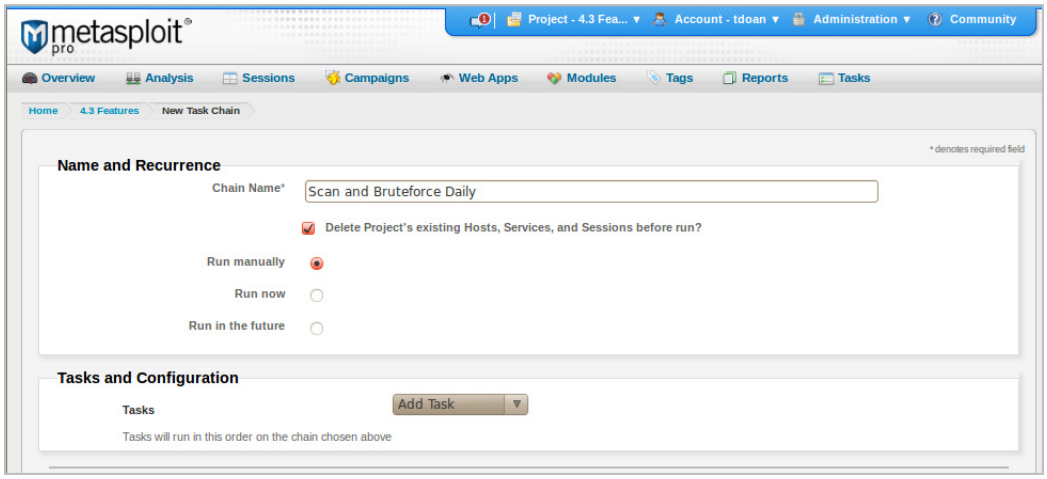
## Creating a Task Chain

When you create a task chain, you must configure it exactly as you want it the first time around. After you create the task chain, you cannot go back and modify it. Therefore, verify the recurrence and task configurations before you click the **Create** button.

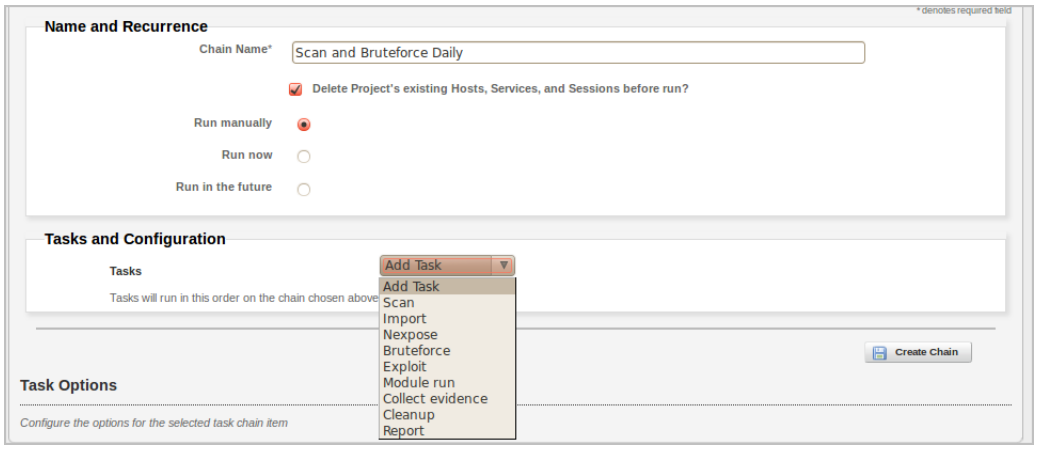
If you want to make any changes to a task chain, you must create a new one.

1. Create or open a project.
2. Select **Tasks > Chains**. The **Task Chain Schedules** page appears.
3. Click the **Create Chain** button. The **New Task Chain** page appears.

4. First, you need to define the task chain name and recurrence. Under Name and Recurrence, enter a name for the schedule.

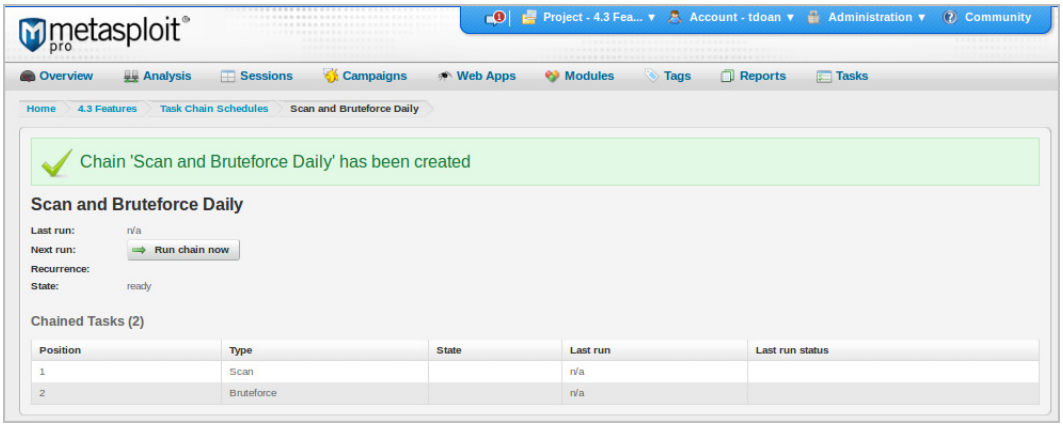



5. Next, enable the **Delete project data** option if you want the system to clear the information currently stored in the project and close open sessions before the system runs the task schedule.
6. Finally, choose whether you want to run the schedule manually, now, or in the future. If you want to run the schedule in the future, choose whether you want to run the schedule once, daily, weekly, or monthly. After you choose the recurrence type, choose the time and date for the task schedule to follow.
7. Now, you can create the task chain. Under Tasks and Configuration, click the **Add Task** dropdown and choose the task you want to add to the task chain. After you add a task, the task configuration page appears.




8. Configure the options for the task. The options that you can configure depend on the task that you have selected in the task chain. Please visit the documentation for the task that you want to configure to learn more about the task options.
9. After you set up the task chain, create the task schedule. The task chain details

page appears and displays the task chain information.

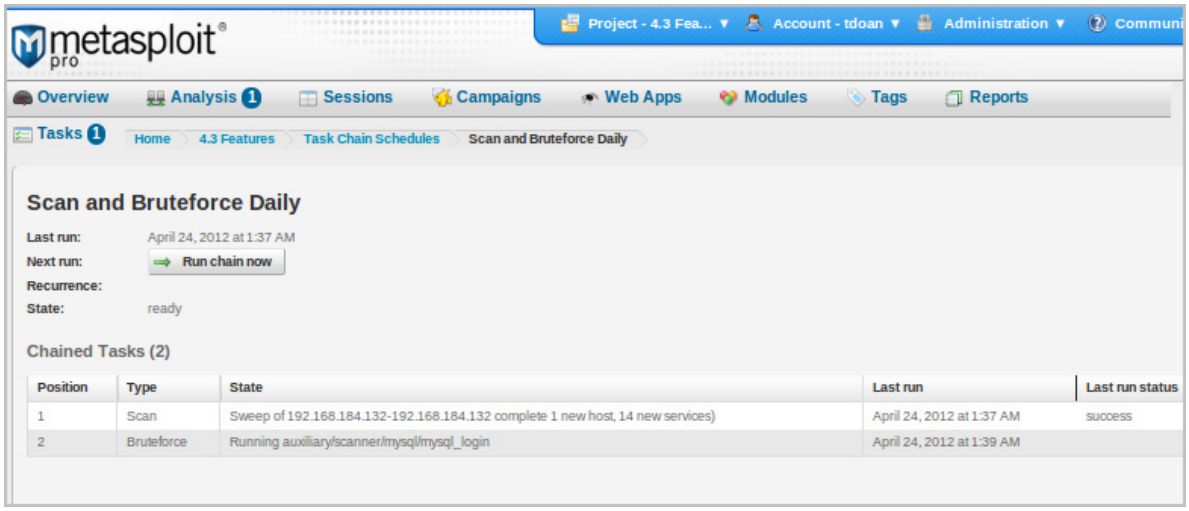



## Task Chain Details Page

The task chain details page provides an overview of the task chain configuration. It displays the last and next run time, recurrence type, state, and the tasks for the task chain. You can view this page to easily identify the latest state and status for the tasks within the task chain. Additionally, you can run and cancel task chains that have a manual or now recurrence setting directly from the task chain details page.

To access the task chain details page, select **Task > Chains**, and click on a task chain name.

The following image shows the task chain details page:

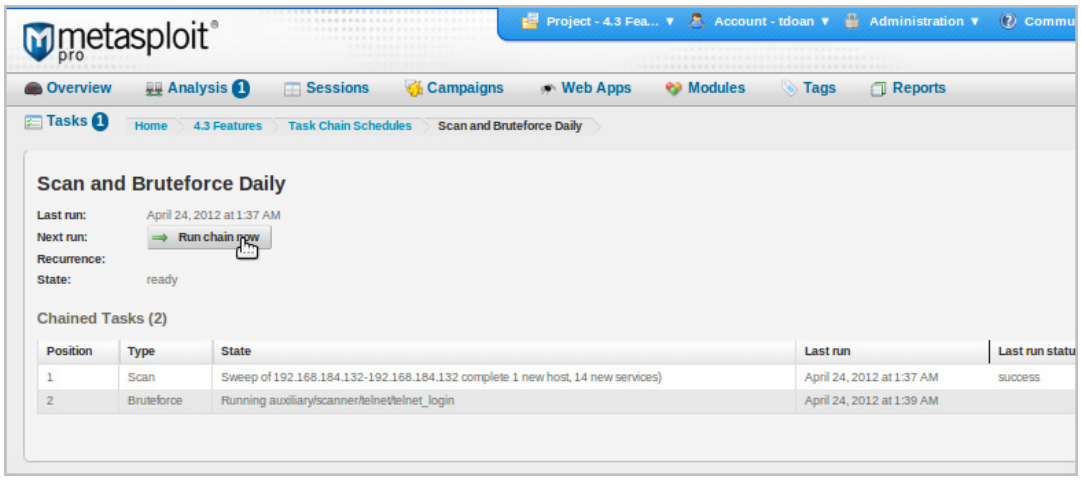



## Running a Task Chain

You can manually run any task chain that has a manual or now recurrence type. Manually running the task chain gives you control over when the task chain starts. When you run a task chain manually, the system schedules the task chain to run within the next minute.

The following steps provide a general overview of the steps you must take to manually run a task chain.

1. Open an existing project or create a new one.
2. Select **Tasks > Chains**. The **Task Chain Schedules** page appears.
3. Under Name and Recurrence, enter a name for the task chain and choose **Run manually** or **Run now** for the recurrence type.
4. Add and configure the tasks that you want to add to the task chain.
5. Before you create the task chain, verify that it is configured correctly. You cannot go back and edit the task chain after you create it.
6. Create the task chain. The task chain details page appears.
7. Click **Run Chain Now** when you are ready to run the task chain.




8. A confirmation window appears. Click **OK** to start the task chain.

After you start the task chain, you can go to the **Tasks** page to view the progress of the tasks.

## Deleting a Task Chain

1. Open the project that contains the task chain that you want to delete.
2. Select **Tasks > Chains**. The **Task Chain Schedules** page appears.
3. Select the task chain that you want to delete.
4. Click the **Delete Chains** button.
5. A window appears and prompts you to confirm that you want to delete the task chain. Click **OK** to confirm that you want to delete the task schedule.

## Rearranging Tasks in the Task Chain

You can only rearrange tasks in a task chain that you are currently creating. After you create and save the task chain, you cannot go back and edit it.

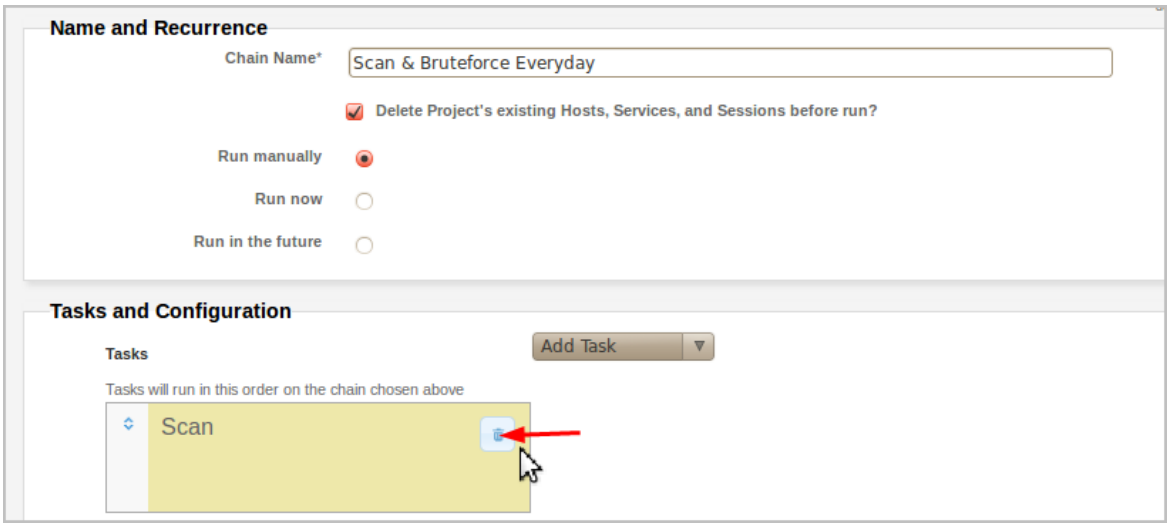
To move a task in a task chain, click the button and drag the task to the new position in the task chain.

## Deleting a Task from the Task Chain

You can only delete a task from a task chain while you are creating it. After you create and save the task chain, you cannot go back and delete a task.

To delete a task from the task chain, click the **Delete** button next to the task.

The following image shows how to delete a task from the task chain:




## Modifying a Task Chain

You cannot modify a task chain after you create it. Therefore, you must configure the task schedule exactly as you want it when you create it. Otherwise, to change the task schedule, you must delete the current task schedule and create a new one.

## Adding Post-Exploitation Modules to a Task Chain

Post-exploitation is the phase that occurs after the system successfully exploits the target. It is the process that you use to identify information that helps you gain further access to the target or to additional systems within the target's internal networks.

When you manually run an attack against a target and get an active session, Metasploit Pro provides actions that you can take against the session. The actions are available on the session page and vary based on the session type, such as shell or Meterpreter, and system information. For example, if the system opens a shell on a target, the actions that you can take include opening a command shell that connects to the target and collecting system data. If the system opens a Meterpreter session, you can do things like set up a proxy pivot or access the file system.

Using the target system information, Metasploit Pro automatically displays the post-exploitation modules that are applicable to the target. This makes it easy for you to identify and choose the post-exploitation modules that you want to run against the target.

When you work with task chains, the post-exploitation process is completely manual. You must search for the post-exploitation modules that you want to use based on the information that you have about the target. For example, if you know the target is a Windows system, and you want to capture screenshots, you may want to add a module task to your task chain that runs `post/Windows/gather/screenshot`. Or if you know your target is a Linux system, and you want to collect hashes, you may want to run `post/linux/gather/hashdump`.

### *Applying Post-Exploitation Modules to Future Sessions*

When you add a post-exploitation module to a task chain, the module configuration page provides an option to apply the module to future sessions. Enable this option to run the post-exploitation module against all future sessions, if the module is applicable to the session.

For example, if the target is a Linux system, a Windows-based post-exploitation module is not applicable to the target and will not run.

## Cleaning Up Active Sessions

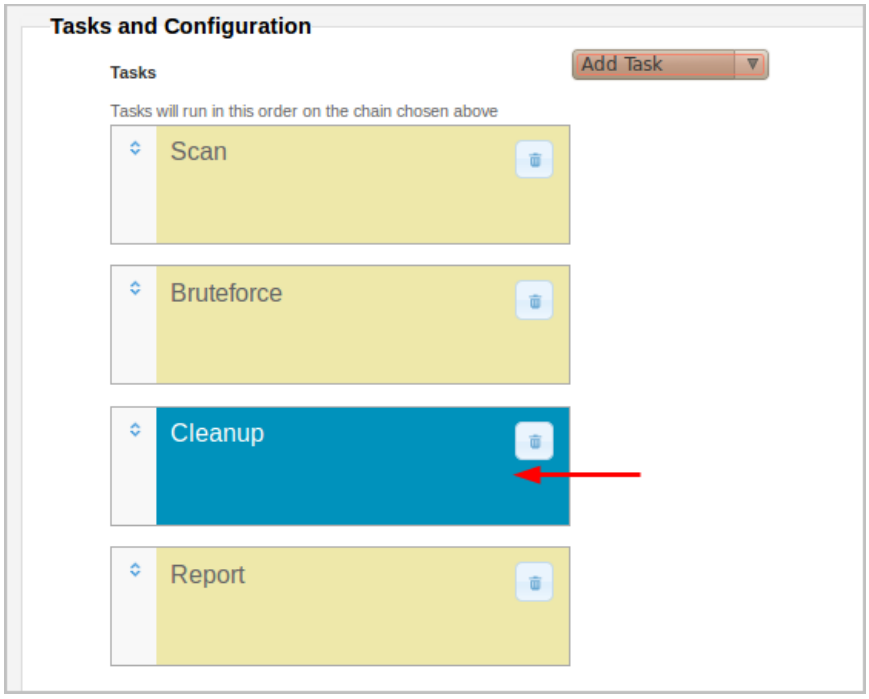
A task chain that includes a task like bruteforce, exploit, or module run may open a session on the target system. An open session enables you to interact with the exploited system. For example, you can do things like collect screenshots of the system or pivot to other hosts on the network.

When you are done with a session, you should close the connection with the session. This is known as a session clean up.

To clean up active sessions, you should add a clean up task to the task chain. As a rule of thumb, the clean up task should be one of the last tasks in the task chain. This ensures that Metasploit Pro has the opportunity to collect system information and take advantage of open sessions before it closes them.

Generally, a report task should be the only task that you add after a clean up task.

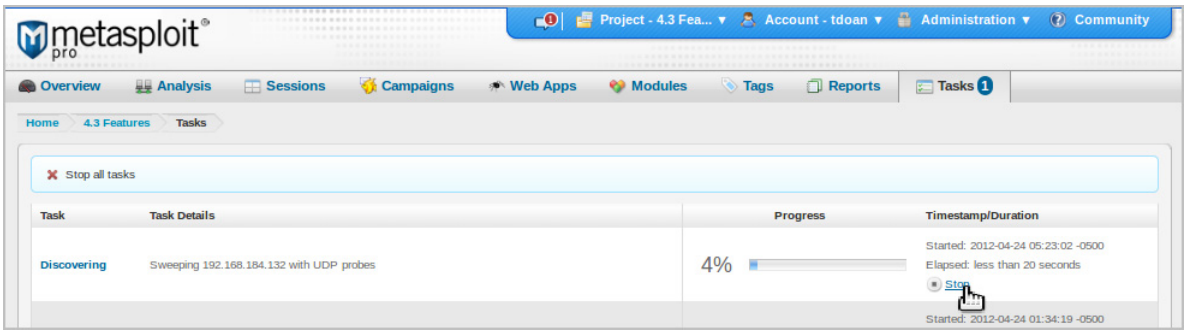
The following image shows a typical task chain that uses the clean up task:




## Stopping a Task

To stop a task, go to the Tasks page. A list of active and completed tasks displays. Click the **Stop** button for the task that you want to cancel. Metasploit Pro skips the task and moves to the next task in the task chain.

The following image shows how to stop a task:

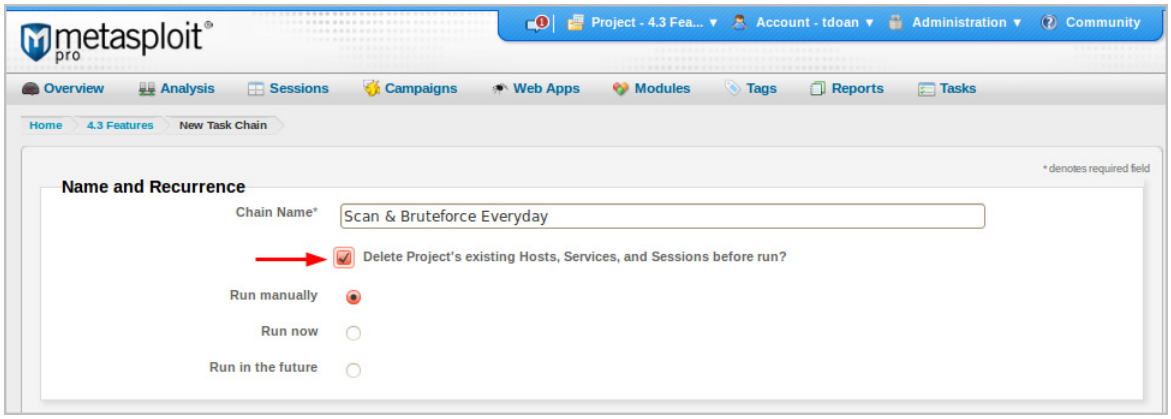



## Deleting Project Data Before a Task Chain Run

When the system runs a task, it stores any information that it collects in the project, such as hosts, services, passwords, hashes, and screenshots. If the system does not clear the stored data before it runs the task chain, the system may try to exploit offline hosts. To ensure that the system only exploits active hosts, delete the project data before the system runs the task chain.

To delete the project data before the system runs the task schedule, you must enable the **Delete project data** option for the task schedule. To locate the **Delete project data** option, select **Tasks > Schedules** and open a task schedule. The option is located under Name and Recurrence. Make sure to save the task schedule after you modify it.

The following image shows where you can access the **Delete project data** option:



# FAQs

### Question: How do I uninstall Metasploit Pro on Linux?

Uninstalling Metasploit Pro is a two step process. First you must stop the Metasploit service, then you must run a script that removes Metasploit and all its components. To uninstall Metasploit Pro, open the command line terminal. Change the current directory to the Metasploit directory. For example, if you used the default installation directory, you can type `cd Metasploit-4.4.0`. After you change the directory, type `./ctlscript.sh.stop` to stop the Metasploit service, and then type `./uninstall` to run the uninstall script.

### Question: How do I uninstall Metasploit Pro on Windows?

To uninstall Metasploit Pro, choose **Start > Metasploit > Uninstall Metasploit**.

### Question: How do I launch the Metasploit Web UI?

To launch the Metasploit Web UI, open a browser and go to `https://localhost:3790`. If you assigned the Metasploit service a different port, use that port instead of 3790.

### Question: How do I add a module to Metasploit?

If you are on a Windows machine, browse to `C:\metasploit\apps\pro\msf3\modules`. If you are on a Linux machine, browse to `$HOME\opt\metasploit-<version>\apps\pro\msf3\modules`.

You must match the path of the exploit with the physical structure defined within the Metasploit module directory. For example, if you want to use `exploit/multi/browser/firefox_xpi_bootstrapped_addon`, you must browser to `C:\metasploit\apps\pro\msf3\modules\exploits\multi\browser` and add the module to that location.

After you add a module, open the Metasploit console and type `reload_all` to refresh your module list.

### Question: How often does Metasploit release new exploits?

The Metasploit team releases a weekly update to the Metasploit Framework and Metasploit Pro. The update typically includes bug fixes, small feature enhancements, and new modules. The Metasploit Web UI will alert you when there is an update available.

If you are an msfconsole user, you can immediately get the latest modules that have been added to the Metasploit Framework. To update your local copy of the Metasploit Framework, open msfconsole and run `msfupdate`.

### Question: What do I do if I exceed the maximum number of license activations?

Single user license keys allow three unique installations. If you have exceeded this number, please contact support@rapid7.com for assistance.

# INDEX

## O



## P



## R



## S



## T



## U



## V



## W