

# Metasploit Express

User Guide

Release 4.4

# TABLE OF CONTENTS

## About this Guide

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

## Overview

Product Overview .....	3
Component Overview .....	3
Service Listeners .....	4
Supported Bruteforce Targets .....	4
Supported Exploit Targets .....	5
Supported Browsers .....	5
Support for IPv6 Targets .....	5

## Features Overview

Features Overview .....	7
The Dashboard .....	7
Navigational Tour .....	8
Administration Tour .....	8
Project Management .....	8
Global Settings .....	9
System Management .....	9
Features Tour .....	10
Host Scan .....	10
Bruteforce .....	11
Exploitation .....	11
Reports .....	12

## Administration

Administration Overview .....	13
User Account Management .....	13
Creating a User Account .....	13
Editing a User Account .....	13
Changing a User Account Password .....	14
Resetting a User Account Password on Windows .....	14
Resetting a User Account Password on Linux .....	14
Deleting a User Account .....	14
System Management .....	15
Product News .....	15
Configuring Global Settings .....	15
Managing License Keys .....	17
Managing the System .....	17
Project Management .....	19
Configuring Project Settings .....	19

## Projects

Project Overview .....	21
Working with a Project .....	21
Creating a Project .....	21
Editing a Project .....	22
Showing a List of All Projects .....	22

## Discovering Hosts

Discovery Overview .....	23
Discovery Scan .....	23
IPv6 Addresses for Target Hosts .....	23
Discovery Scan Options .....	24
Discovering Hosts .....	26
Discovering Virtual Hosts .....	26
Scanning the Network for H.323 Video Conferencing Systems .....	27
Defining Nmap Arguments .....	27
Nexpose Scan .....	27
Nexpose Scan Options .....	28
Configuring a Nexpose Console .....	30
Running a Nexpose Scan .....	31
Running a Nexpose Scan with a Custom Scan Template .....	31
Passing the Hash from Metasploit Express .....	32

Purging Scan Data.....	32
Imported Scan and Vulnerability Data .....	33
Supported Scan Data Formats .....	33
Importing Data .....	34
Host Data.....	34
Viewing Host Notes .....	35
Viewing Host Services.....	35
Viewing Host Evidence.....	35
Viewing Host Vulnerabilities .....	35
Vulnerability Management.....	35
Adding a Vulnerability.....	35
Exploiting a Known Vulnerability.....	36
Editing a Vulnerability .....	36
Deleting a Vulnerability.....	36
Host Management .....	36
Adding a Host.....	37
Deleting a Host.....	37
Host Badges .....	37

## Gaining Access

Gaining Access Overview.....	39
Bruteforce Attacks .....	39
Bruteforce Target Services.....	39
Bruteforce Message Indicators.....	40
Bruteforce Attack Options.....	40
Running a Bruteforce Attack.....	45
Running a Bruteforce Attack Against a Virtual Target.....	46
Running a Bruteforce Attack Using an Imported Credential List .....	46
Testing a Single Credential.....	47
Credential Management .....	47
Credential Generation Switches .....	50
Credential Mutation Switches .....	51
Modules .....	53
Module Types .....	53
Module Search.....	53
Module Statistics.....	55
IPv6 Payloads.....	55
Exploits .....	55
Automated Exploits.....	56
Manual Exploits .....	59
Post-Exploitation.....	60

Post-Exploitation Modules .....	60
Post-Exploitation Macros .....	61
Listeners .....	61

## Taking Control of a Session

Session Overview .....	64
Active Sessions .....	64
Command Shell Session .....	64
Meterpreter Session .....	65
Authentication Notes.....	65
Session Tasks .....	66
Session Details .....	66
Proxy Pivot.....	66
VPN Pivot .....	67
VNC Sessions.....	68
File Systems .....	68

## Evidence Collection

Evidence Collection Overview .....	70
Collecting Evidence .....	70
Collecting Evidence for a Project.....	70
Collecting Evidence for an Active Session .....	71
Password Cracking.....	71
Collected Evidence .....	71
Viewing Evidence for a Session .....	71
Exporting Collected Evidence.....	71
Session Clean Up.....	72
Cleaning Up a Session .....	72

## Reports

Reports Overview .....	73
Standard Reports .....	73
Generating a Standard Report.....	74
Replay Scripts .....	75
Exporting Replay Scripts .....	75

# ABOUT THIS GUIDE

This guide provides information and instructions for Metasploit Express. The following sections describe the audience, organization, and conventions used within this guide.

## Target Audience

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

## Organization

This guide includes the following chapters:

- About this Guide
- Overview
- Metasploit Express 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, " <b>Click Projects &gt; New Project.</b> "

Convention	Description
Code	Indicates command line, code, or file directories. For example, "Enter the following: <code>chmod +x Desktop/metasploit-3.7.1-linux-x64-installer.</code> "
Title	Indicates the title of a document or chapter name. For example, "For more information, see the <i>Metasploit Pro Installation Guide.</i> "
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	<a href="http://www.rapid7.com/customers/customer-login.jsp">http://www.rapid7.com/customers/customer-login.jsp</a>
E-mail	<a href="mailto:support@rapid7.com">support@rapid7.com</a>

### 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.

# OVERVIEW

This chapter covers the following topics:

- [Product Overview](#) 3
- [Component Overview](#) 3
- [Service Listeners](#) 4
- [Supported Bruteforce Targets](#) 4
- [Supported Exploit Targets](#) 5
- [Supported Browsers](#) 5
- [Support for IPv6 Targets](#) 5

## Product Overview

Metasploit Express 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 Express to identify security issues, verify vulnerabilities, and perform real-world security assessments. Metasploit Express 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

Metasploit Express consists of the following main components:

- **The Metasploit Framework** – The Metasploit Framework is a penetration testing system and development platform that you can use to create security tools and exploits. The Metasploit Framework is written in Ruby and includes components in C and assembler. The Metasploit Framework consists of tools, libraries, modules, and user interfaces. The basic function of the Metasploit Framework is a module launcher that allows the user to configure an exploit module and launch the exploit against a target system.
- **Modules** – Metasploit Express contains tasks, such as bruteforce and discovery, in the form of modules. The modules automate the functionality that the Metasploit Framework provides and enables you to perform multiple tasks simultaneously.
- **Projects** – A project is the logical component that provides the intelligent defaults, penetration testing workflow, and module-specific guidance during the penetration test.
- **User Interface** – In addition to the capabilities offered by the open source framework, Metasploit Express delivers a full graphical user interface, automated exploitation capabilities, complete user action audit logs, custom reporting, combined with an advanced penetration testing workflow.

# Service Listeners

Metasploit Express uses the following service listeners to provide the user interface:

- 0.0.0:3790 – Apache SSL Service – Metasploit Express utilizes Apache as a front end web server for the Rails UI application. This is the primary service you will be interacting with when you use Metasploit Express.
- 127.0.0.1:3001 –Thin Rails Server (bound to localhost) – Metasploit Express utilizes Ruby on Rails, and Thin is used as the glue layer between Apache and Rails.
- 127.0.0.1:7337 – PostgreSQL Database (bound to localhost) – Metasploit Express uses PostgreSQL as the host for the Pro datastore. PostgreSQL was chosen for performance reasons.
- 127.0.0.1:50505 – Metasploit RPC Service (bound to localhost) – The RPC service is similar to that provided with the Metasploit Framework, with additional functionality added. This service makes it possible to communicate directly with the Metasploit Express system through RPC. The Rails UI utilizes RPC on this port to communicate with the Metasploit Express engine.

# Supported Bruteforce Targets

The following chart describes the bruteforce targets that Metasploit Express supports as well as the bruteforce capabilities for the target:

## Windows (2000 -> Latest)

SSH	TELNET	SMB	MSSQL	MYSQL	POSTGRES	TOMCAT	DB2
Session	Session	Session	Session	Crack	Crack	Session	Crack
FTP	FINGER	SNMP	VNC	RLOGIN	RSH	REXEC	
Crack	Crack	Crack	Crack	Crack	Crack	Crack	

## Linux

SSH	TELNET	SMB	MSSQL	MYSQL	POSTGRES	TOMCAT	DB2
Session	Session	Crack	-	Crack	Crack	Session	Crack
FTP	FINGER	SNMP	VNC	RLOGIN	RSH	REXEC	
Crack	Crack	Crack	Crack	Session	Session	Session	

## Other Unix (OS X, Solaris, AIX)

SSH	TELNET	SMB	MSSQL	MYSQL	POSTGRES	TOMCAT	DB2
Session	Session	Crack	-	Crack	Crack	Session	Crack
FTP	FINGER	SNMP	VNC	RLOGIN	RSH	REXEC	
Crack	Crack	Crack	Crack	Session	Session	Session	

# Supported Exploit Targets

Metasploit Express 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

Metasploit Express supports the following browsers:

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

**Note:** Windows XP does not support Internet Explorer 9. Therefore, Windows XP users should use Chrome or Firefox to access Metasploit Express.

# 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 Express, 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 Express provides several payloads that provide IPv6 support for Windows x86, Linux x86, BSD x86, PHP, and cmd.

**Note:** 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. Metasploit Express does not support IPv6 for link local broadcast discovery or pivoting.

# FEATURES OVERVIEW

This chapter covers the following topics:

- [Features Overview 7](#)
- [The Dashboard 7](#)
- [Navigational Tour 8](#)
- [Administration Tour 8](#)
- [Features Tour 10](#)

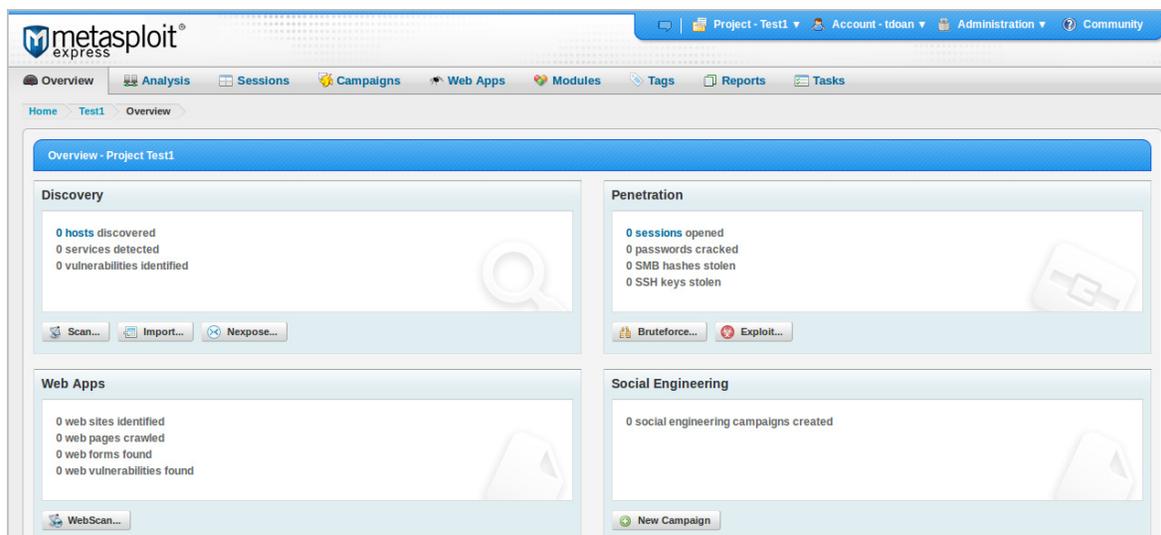
## Features Overview

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

## The Dashboard

The Dashboard provides access to quick tasks and displays a project overview. The project overview shows a numerical breakdown of discovered hosts, opened and closed sessions, and collected evidence. Use the Dashboard for a high level overview of the project.

The following figure shows the Dashboard:



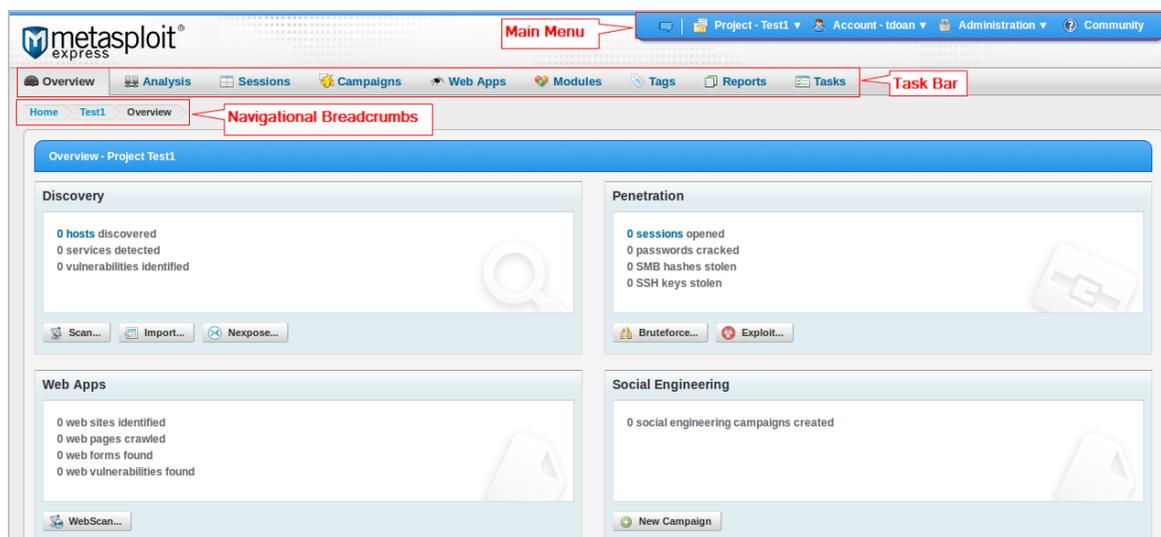
# Navigational Tour

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

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.

The following figure shows the navigational features:



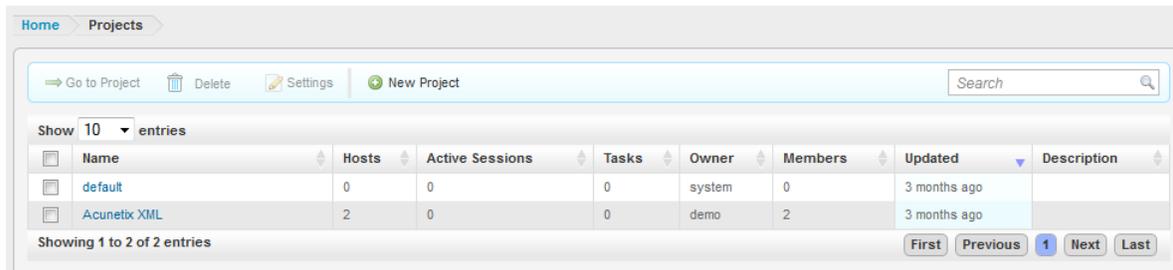
# Administration Tour

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

## Project Management

A Metasploit Express 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.

The following figure shows the project management area:

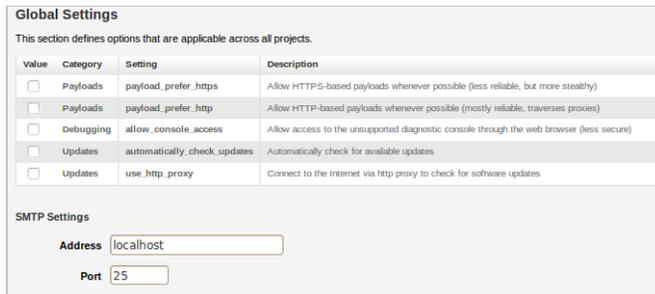


## Global Settings

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.

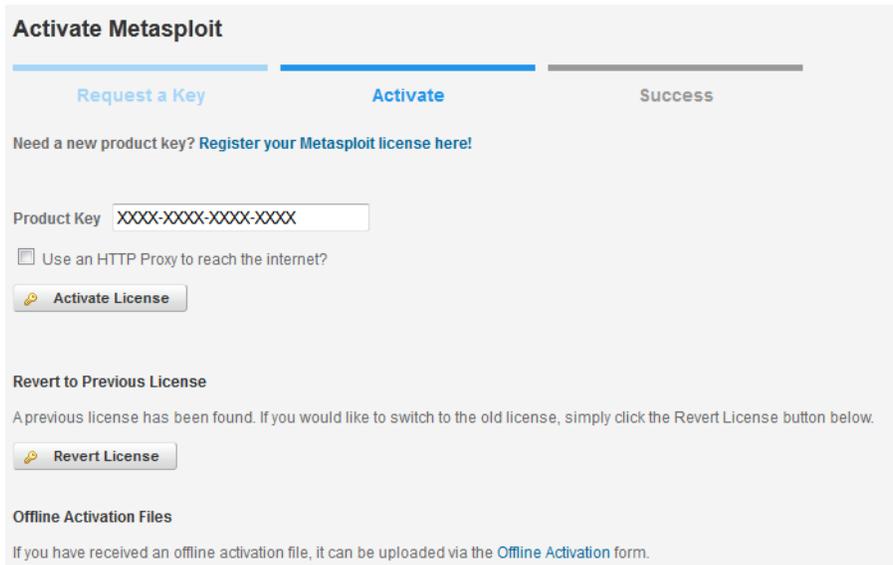
The following figure shows the global settings area:



## 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

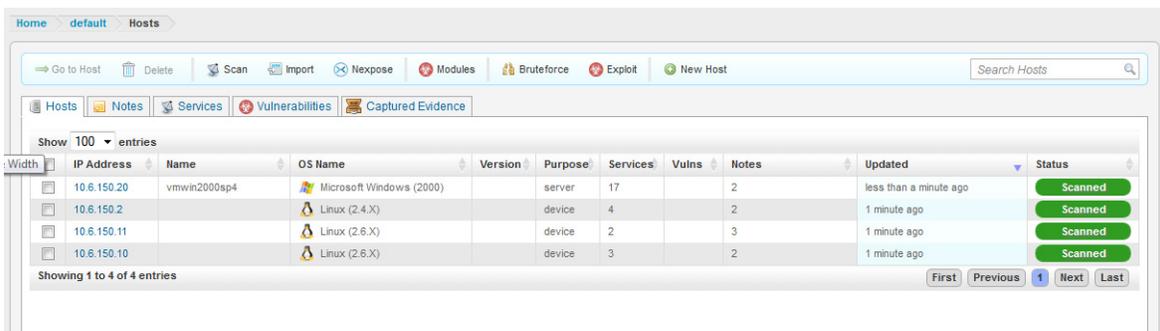
Metasploit Express provides a comprehensive penetration testing system that you can use to scan for target hosts, open and control sessions, exploit vulnerabilities, and generate reports.

### Host Scan

A host scan identifies vulnerable systems within the target network range that you define. When you perform a scan, Metasploit Express 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 Express 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 Express 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 Express 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 Express 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:

The screenshot displays the 'Modules' section of the Metasploit Express interface. At the top, there are navigation tabs for 'Home', 'default', and 'Modules'. Below this is a 'Search Modules' input field. The main content area is divided into two tables: 'Module Statistics' and 'Search Keywords'.

Stat	Value	Keyword	Description	Example
Total Modules	1067	name	Search within the module's descriptive name	name:Microsoft
Exploit Modules	741	path	Search within the module's path name	path:windows/smb
Auxiliary Modules	321	platform	Search for modules affecting this platform/target	platform:linux
Post Modules	101	type	Search for modules that are of a specific type (exploit, auxiliary, or post)	type:exploit
Server-Side Exploits	433	app	Search for modules that are either client or server attacks	app:client
Client-Side Exploits	212	author	Search for modules written by author	author:hdm
		cve	Search for modules with a matching CVE ID	cve:2009
		bid	Search for modules with a matching Bugtraq ID	bid:10078
		osvdb	Search for modules with a matching OSVDB ID	osvdb:875

Below the search keywords table, there is a section titled '10 most recent disclosures'. This section contains a table with the following columns: 'Module Type', 'OS', 'Module', 'Disclosure Date', 'Module Ranking', 'CVE', 'BID', and 'OSVDB'.

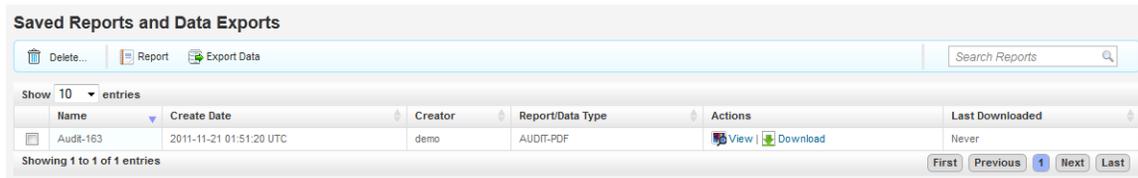
Module Type	OS	Module	Disclosure Date	Module Ranking	CVE	BID	OSVDB
Server Exploit	Windows	Java RMI Server Insecure Default Configuration Java Code Execution	October 14, 2011	★★★★★★			
Client Exploit	Mac OS	Apple Safari file:// Arbitrary Code Execution	October 11, 2011	★★★	2011-3230		
Server Exploit	Windows	myBB 1.6.4 Backdoor Arbitrary Command Execution	October 5, 2011	★★★★★★		49993	

# Reports

A report provides comprehensive results from a penetration test. Metasploit Express 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.

The following figure shows the reports area:



# ADMINISTRATION

This chapter covers the following topics:

- [Administration Overview 13](#)
- [User Account Management 13](#)
- [System Management 15](#)
- [Project Management 19](#)

## Administration Overview

As an administrator, you manage user accounts, perform system maintenance, and manage projects.

## User Account Management

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 Express 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 Express 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 Express 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 the Metasploit Express user 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 Express.

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

1. From the Start menu, choose **All Programs > Metasploit > Password Reset**. The Password Reset window appears. Wait for the environment to load and prompt you to continue.
2. Type **yes** to continue. 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 Express.
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 Express. You can change the password after you log in to Metasploit Express.
4. Exit the console.

## 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.

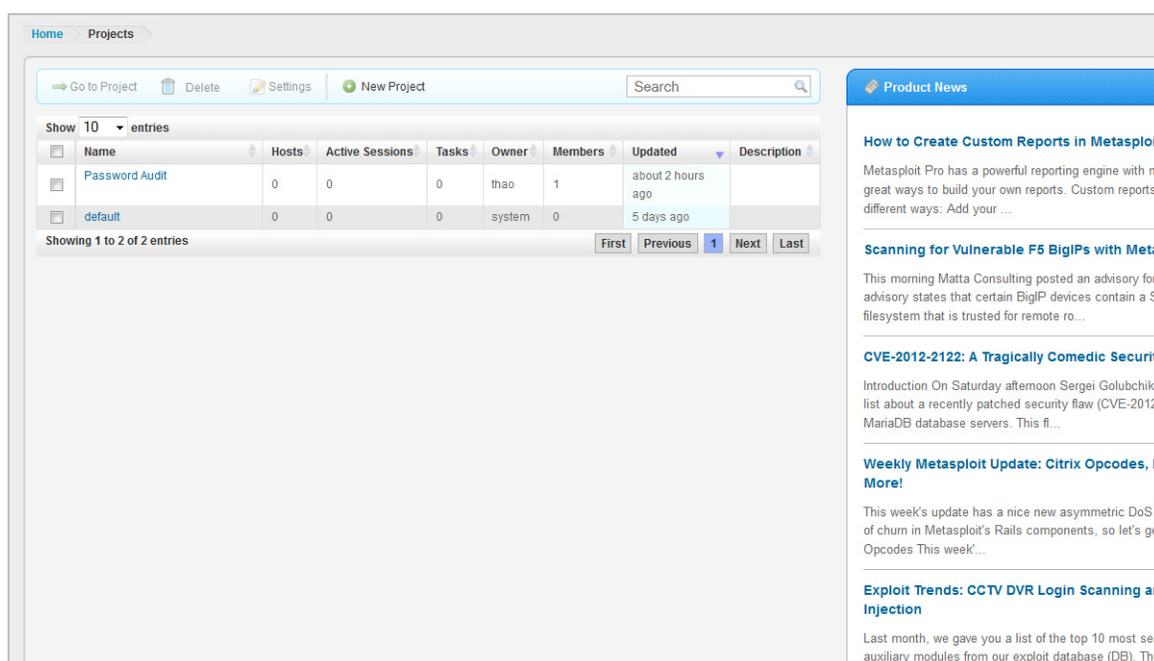
# System Management

The administrator can configure the global settings for projects, create API keys, manage license keys, and update the system.

## Product News

When you access the Projects page, the Product News displays and lists the latest blog posts from the Metasploit Community site. You can click on any of the blog links to access the blog entry.

The figure below shows the Product News:



## Configuring Global Settings

Metasploit Express 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 Express.

The following image shows the Global Settings:

Global Settings			
This section defines options that are applicable across all projects.			
Value	Category	Setting	Description
<input type="checkbox"/>	Payloads	payload_prefer_https	Allow HTTPS-based payloads whenever possible (less reliable, but more stealthy)
<input type="checkbox"/>	Payloads	payload_prefer_http	Allow HTTP-based payloads whenever possible (mostly reliable, traverses proxies)
<input type="checkbox"/>	Debugging	allow_console_access	Allow access to the unsupported diagnostic console through the web browser (less secure)
<input type="checkbox"/>	Updates	automatically_check_updates	Automatically check for available updates
<input type="checkbox"/>	Updates	use_http_proxy	Connect to the Internet via http proxy to check for software updates

SMTP 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.

## Managing License Keys

License keys define the product edition and the registered owner of Metasploit Express. Metasploit Express 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 Express. 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 Express 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 Express reverts to the previous version.

## Managing the System

Administrators can update, maintain, and uninstall Metasploit Express.

### *Updating the System*

If you are an administrator, you must regularly check for available updates to Metasploit Express. When you check for updates, Metasploit Express alerts you when a newer version is available for you to install. If a newer version of Metasploit Express 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 Express prompts you to restart the back end services. If you restart the services, Metasploit Express terminates active sessions and requires up to five minutes to restart.

## Update Notifications

Metasploit Express alerts you when there is a software update available. The notification appears in the main menu of the interface. The figure below shows the update notification.



## Maintaining the System

Metasploit Express 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

Log File	Log File Location
License log	<code>\$INSTALL_ROOT/apps/pro/engine/license.log</code>

## ***Uninstalling Metasploit Express on Linux***

When you uninstall Metasploit Express, you remove the components and modules from the system and the data stored within the penetration tests.

1. Navigate to the root installation directory and enter `./ctlscript.sh.stop` to stop all Metasploit Express services.
2. Enter `./uninstall`.
3. Click **Yes** to confirm that you want to uninstall Metasploit Express components and modules.
4. Click **Yes** to confirm that you want to delete the data saved in the penetration tests. If you click **No**, the `$INSTALLER_ROOT/apps` directory remains intact, and you can access Metasploit Express data stored in this directory.

## ***Uninstalling Metasploit Express 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 uninstall completes.

# **Project Management**

A project is a penetration test. Use projects to define the target systems that you want to test and to configure tasks for the penetration 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 Express 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 Express 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.

# PROJECTS

This chapter covers the following topics:

- [Project Overview 21](#)
- [Working with a Project 21](#)

## 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 Express. 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. Create the project.

## Editing a Project

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

## Showing a List of All Projects

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

# DISCOVERING HOSTS

This chapter covers the following topics:

- [Discovery Overview 23](#)
- [Discovery Scan 23](#)
- [Nexpose Scan 27](#)
- [Imported Scan and Vulnerability Data 33](#)
- [Host Data 34](#)
- [Vulnerability Management 35](#)
- [Host Management 36](#)
- [Host Badges 37](#)

## Discovery Overview

Host discovery is the process that Metasploit Express uses to identify live valid hosts within a target network address range. You can use the Metasploit Express 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 Express with a valid target range.

## IPv6 Addresses for Target Hosts

Metasploit Express 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 Express. 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
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:  <pre>-o -i -resume -script -datadir -stylesheet</pre>
Additional TCP ports	Appends additional TCP ports to the existing Nmap scan ports. Discovery scan appends the ports to <code>-p</code> .
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.  For example, if you specify ports 1-20, the following Nmap command is returned:  <pre>/nmap -sS - -PS1-20 -PA1-20 -PU51094 -PP - PE -PM -PI -p1-20 --host-timeout=5m -O --max-rtt-timeout=300 -- initial-rtt-timeout=100 --max-retries=2 -- stats-every 10s --min-rate=200</pre> 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.

Option	Description
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.
Portscan speed	<p>Controls the Nmap timing option (-T). Choose from the following timing templates::</p> <p><b>Insane (5)</b> - Speeds up the scan. Assumes that you are on a fast network and sacrifices accuracy for speed. Scan delay is less than 5 ms.</p> <p><b>Aggressive (4)</b> - Speeds up the scan. Assumes that you are on a fast and reliable network. Scan delay is less than 10 ms.</p> <p><b>Normal (3)</b> - The default portscan speed. Does not affect the scan.</p> <p><b>Polite (2)</b> - Uses less bandwidth and target resources to slow the scan.</p> <p><b>Sneaky (1)</b> - Use this portscan speed for IDS evasion.</p> <p>Paranoid (0) - Use this portscan speed for IDS evasion.</p>
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.

Option	Description
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.
4. Click **Show Advanced Options** to verify and configure the advanced options for the scan. If you do not configure additional options, Metasploit Express uses the default configuration for the scan.
5. Run the scan.

## Discovering Virtual Hosts

When you perform a discovery scan, Metasploit Express automatically discovers guest operating systems on the target system. Metasploit Express 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 Express supports the following guest operating systems:

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

### ***Supported Host VM Servers***

Metasploit Express 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 runs a virtual environment, Metasploit Express captures screenshots of the guest operating systems on the host system. To view the screenshots of the guest operating systems, go to **Analysis > Hosts > 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.

## **Nexpose Scan**

You can use the Community and Enterprise editions of Nexpose to discover and scan devices for known vulnerabilities. After you complete a Nexpose scan, you can import the scan data into Metasploit Express. Metasploit Express imports the scan data and enables you to validate and test the scan results.

Metasploit Express provides a connector that allows you to run and automatically import the results of a Nexpose scan into a project.

Before you can run a Nexpose scan, you must download, install, and configure Nexpose. Additionally, you must configure a Nexpose console through Metasploit Express.

Metasploit Express only supports the number of hosts that you have licenses for in Nexpose. If you provide more hosts than you have licenses for, 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>.

## Nexpose Scan Options

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

Option	Description
Nexpose scan targets	Defines the target address range for the Nexpose 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.
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.

Option	Description
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 Express 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 Express 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.

## 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 sites into a project.

After you set up the Nexpose console, you can access and use the console for a Nexpose scan. Configured Nexpose consoles are automatically available for you to use.

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.
7. Enter the console port.
8. Enter the console user name.
9. Enter the console password.
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.

## 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.

## Passing the Hash from Metasploit Express

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 Express collects data, such as password hashes, from the exploited system. After Metasploit Express collects password hashes from a target system, you can pass the hash and run a Nexpose scan to perform a credentialed scan.

Before you can pass the hash in Metasploit Express, 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 Express 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 Express 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 Express 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 Express 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.

## Imported Scan and Vulnerability Data

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

### Supported Scan Data Formats

Metasploit Express supports the following data file formats:

- Metasploit PWDump Export
- 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

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

**Note:** Metasploit Express 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 Express 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 Express 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 Express collects additional host information that you can view from the Analysis page. Metasploit Express collects information from notes, services, vulnerabilities, and captured evidence.

You can view host data through 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 Express 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 Express identifies any known vulnerabilities for the target hosts.

If Metasploit Express 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 Express 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 Express 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 Express 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 Badges

A host badge identifies the status of each discovered host. Use the host badge to determine whether Metasploit Express 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:

<b>Host Badge</b>	<b>Description</b>
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.

# GAINING ACCESS

This chapter covers the following topics:

- [Gaining Access Overview 39](#)
- [Bruteforce Attacks 39](#)
- [Modules 53](#)
- [Exploits 55](#)
- [Post-Exploitation 60](#)

## 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 Express 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 Express 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 Express color codes bruteforce task logs to help you identify successful and unsuccessful attacks. Metasploit Express 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 Express 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	<p>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:</p> <p>Admin:admin Admin:admin1 Admin:admin! Test:test Test:test1234 Test123:test123 cisco:cisco user:user administrator:administrator root:root root:toor</p> <p>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.</p> <p>The system generates approximately 20 credentials in order to bruteforce all services.</p>

Option	Description
Bruteforce Depth: Defaults Only	<p>Attempts a small number of known default and user names and passwords.</p> <p>The default only mode generates the following credentials:</p> <ul style="list-style-type: none"> <li>16 credentials for postgres</li> <li>29 credentials for DB2</li> <li>141 credentials for SSH</li> <li>141 credentials for Telnet</li> <li>22 credentials for MSSQL</li> <li>150 credentials for HTTP</li> <li>4 credentials for HTTPS</li> <li>13 credentials for SMB</li> <li>21 credentials for FTP</li> </ul>
Bruteforce Depth: Normal	<p>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 Express tries after known good credentials on other services.</p> <p>The normal mode generates the following credentials:</p> <ul style="list-style-type: none"> <li>4,000 credentials for postgres</li> <li>3,000 credentials for DB2</li> <li>10,000 credentials for MySQL</li> <li>1,000 credentials for SSH</li> <li>1,000 credentials for Telnet</li> <li>10,000 credentials for MSSQL</li> <li>6,000 credentials for HTTP</li> <li>1,000 credentials for HTTPS</li> <li>4,000 credentials for SMB</li> <li>1,000 credentials for FTP</li> </ul> <p>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.</p>

Option	Description
Bruteforce Depth: Deep	<p>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.</p> <p>For the few protocols that support fast enough guesses, passwords are subject to a fixed set of transformations. For example, 1 for l and 0 for O.</p> <p>The deep mode generates the following credentials:</p> <p>12,000 credentials for postgres:5432  9,000 credentials for DB2:50000  30,000 credentials for MYSQL:3306  132 credentials for SSH:22  132 credentials for Telnet:23  30,000 credentials for MSSQL:13013  18,000 credentials for HTTP:8080 (tomcat)  3,000 credentials for SMB:445 (Microsoft)</p> <p>SSH and Telnet are not subject to the deep multiplier because these credentials take longer to test than the other services.</p>
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.

Option	Description
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 Express 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.
Additional credentials	<p>Defines the user name and password combinations that the bruteforce attack uses. Use commas to separate user name and password combinations.</p> <p>For domain-specific user name and password combinations, use the following format: domain/username.password.</p> <p>For user names with no password, define the user name only.</p> <p>For user names with multiple passwords, use the following format: username password1, password2, password 3.</p>
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.

Option	Description
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.
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.

Option	Description
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.
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 Express 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 Express. 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 Express 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 Express 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 Express 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 Express. Use imported credentials when you run the scan in normal, deep, or imported only mode.

If you import multiple files, Metasploit Express 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 Express supports:

Format	Description
PWDump	<p>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.</p> <p>When you use a PWDump file, you must define the SMB domains to target services that accept Windows authentication.</p> <p>When you use a PWDump file, use the <b>imported only</b> bruteforce depth to test only this list of credentials.</p> <p>Use this format if you have an exported a Metasploit PWDump.</p> <p>Example:            administrator:501:de8130a284642c74523fa0f66c35ef02:421a1c7abc7b160c20ed78a2e06e09c8:::</p>
User names and passwords	<p>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.</p> <p>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.</p> <p>When you use a user name and password file, use the <b>imported only</b> bruteforce depth to test only this list of credentials.</p> <p>Use this format if you have a list of user names and passwords.</p> <p>Example:            username1 passwordA            username2 passwordA passwordB            username3 passwordA passwordB passwordC</p>

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

### **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,

Username, Password, 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 Express 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 Express 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 Express compromises a target system.

## Excluded Modules

Most modules that are available in the Metasploit Framework are available in Metasploit Express. 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.

Keyword Tag	Description
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 stagers/windows/reverse_ipv6_https stagers/windows/reverse_ipv6_tcp stagers/windows/bind_ipv6_tcp
Linux x86	singles/linux/x86/shell_bind_ipv6_tcp stagers/linux/x86/reverse_ipv6_tcp stagers/linux/x86/bind_ipv6_tcp
BSD x86	singles/bsd/x86/shell_reverse_tcp_ipv6 singles/bsd/x86/shell_bind_tcp_ipv6 stagers/bsd/x86/reverse_ipv6_tcp stagers/bsd/x86/bind_ipv6_tcp
Shell	singles/cmd/windows/bind_perl_ipv6 singles/cmd/unix/bind_netcat_ipv6 singles/cmd/unix/bind_perl_ipv6 singles/cmd/unix/bind_ruby_ipv6
PHP	singles/php/bind_perl_ipv6 singles/php/bind_php_ipv6 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 Express 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 Express builds an attack plan based on the service, operating system, and vulnerability information that it has for the target system. Metasploit Express 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 Express 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 Express 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 Express 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.

Option	Description
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.
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	<p>This option enables you to send small TCP packets and insert delays between them.</p> <p>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.</p> <p>Medium – Transmits small TCP packets; payloads are fragmented into 15 byte payloads.</p> <p>High – Combines the Low and Medium settings by transmitting small TCP packets and inserting delays between them.</p>

Option	Description
Application Evasion	<p>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.</p> <p>DCERPC</p> <p>Low – Adds fake UUIDs before and after the actual UUID that the exploit targets. High – Sets the maximum fragmentation size of DCERPC calls to a value between 4 and 64.</p> <p>SMB</p> <p>Low – Obscures the PIPE string, places extra padding between SMB headers and data, and obscures path names. Medium – Segments SMB read/write operations. High – Sets the max size for SMB reads and writes to 4-64 bytes.</p>
Application Evasion	<p>HTTP (Client-Server Attacks Only)</p> <p>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. Medium – Adds 1-64 fake query strings to get requests. Adds 1-64 white space characters between tokens. Adds 1-64 POST parameters. High – Encodes some characters as percent-u unencoded characters (half, randomly), adds a fake "end" to HTTP requests before the attack, and uses backslashes instead of forward slashes.</p>
Obtain one session per target	<p>Opens one session per target and bypasses any targets that have a session open.</p>
Dry run	<p>Performs a dry run on the exploit, which provides you with details of the exploit, but does not run the exploit.</p>

### **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 Express 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 want 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 Express 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 Express opens a session on a target system.

A post-exploitation macro automatically runs after a target system runs an exploit 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 Express 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 Express 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 Express 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 10:10:10:1:47385.

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 Express 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:

- [Active Sessions 64](#)
- [Session Tasks 66](#)

## Session Overview

An active session provides a connection between the target system and the attacker. Metasploit Express 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 Express 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 Express 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 Express 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 Express 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** area.
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 Express.

## 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 Express 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 Express 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 Express 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 Express creates 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 Express initiates.

When Metasploit Express 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 Express 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 Express does not have an existing direct connection to any networks that have the same IP range and netmask as the target network.

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

### ***Virtual Interfaces***

In order to provide VPN pivot functionality on the Windows platform, Metasploit Express 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 Express does not locate the virtual interfaces when MetasploitProSvc starts, Metasploit Express 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 Express 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 Express.

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 Express 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**.

# EVIDENCE COLLECTION

This chapter covers the following topics:

- [Evidence Collection Overview 70](#)
- [Collecting Evidence 70](#)
- [Collected Evidence 71](#)
- [Session Clean Up 72](#)

## Evidence Collection Overview

The system data that Metasploit Express 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 Express automatically performs offline password cracking when it runs the collection task. If Metasploit Express 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 Express tries to crack the word list using a combination of rules and incremental modes in both LANMAN and NTLM formats. Metasploit Express parses any cracked passwords and adds the password to the word list.

## Collected Evidence

Evidence is information that Metasploit Express 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**.

# REPORTS

This chapter covers the following topics:

- [Reports Overview 73](#)
- [Standard Reports 73](#)
- [Replay Scripts 75](#)

## 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 Express provides the following report formats:

- Audit reports – Combines the high-level results from the other reports and presents them in a single comprehensive report.
- Compromised reports – Lists all hosts on which Metasploit Express was able to open a session, successfully run a module, or record a vulnerability.
- Authentication token reports – Lists all cracked hosts and includes all cracked passwords, SMB hashes, and SSH keys discovered.
- Services reports – Lists all network services discovered by Metasploit Express.
- Collected evidence reports – Lists all looted hosts and includes the files and screen shots collected from the compromised hosts.
- Campaigns reports – Lists all Web Campaigns run as part of the project.
- Webapp reports – Lists all websites and the vulnerabilities, forms, and pages associated with the websites.

## 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**.
6. Click the Report button.

# Replay Scripts

A replay script enables you to replay an attack without Metasploit Express. 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.

# INDEX

## A

- active session 64
- audit reports 73
- authentication token reports 73
- automated exploits 56
- auxiliary 53

## B

- bruteforce 11, 39
  - options 40

## C

- campaigns reports 73
- collected evidence reports 73
- command shell 64
- compromised reports 73
- credential files 47
- credential generation switches 50
- credential mutation switches 51
- credentials 47
  - import 49

## D

- Dashboard 7
- data file formats 33
- discovery scan 23

## E

- evidence 70
- exploit 53, 55

## F

- file system 68

## G

- global settings 9, 15

## H

- H.323 27
- hash 32

- host
  - add 37
  - management 36
- host badge 37
- host data 34
- host notes 35
- host services 35
- HTTP payloads 16
- HTTPS payloads 16

## K

- keyword expression 53, 54
- keyword tags 53

## L

- license key
  - revert 17
  - update 17
- license keys 17
- listener 61
  - create 62
- LM 32
- log files 18

## M

- manual exploits 59
- Meterpreter 65
- Meterpreter session 65
- module 53
- module statistics 55
- modules 11
- msftap.sys 67

## N

- network boundaries 19
- network range 20
  - restrict 20
- Nexpose console 30
- Nexpose scan 27
- Nmap arguments 27
- NTLM 32

## O

- offline activation file 17

## P

- password cracking 71
- post-exploitation macro 61
- post-exploitation module 53

- post-exploitation modules 60
- project 19
  - create 21
  - edit 22
- project settings 19
- proxy pivot 66

## R

- replay script 75
- report 12, 73
  - standard 73

## S

- scan template 28, 29
  - aggressive discovery 29
  - discovery 29
  - DoS Audit 29
  - exhaustive audit 29
  - full audit 28
- service listeners 4
- services reports 73
- session 64
  - details 66
- session clean up 72
- standard report 73, 74
- system updates 17

## U

- uninstall
  - Metasploit 19
- updates 17
- user account 13
  - delete 14
  - edit 13
  - reset 14

## V

- virtual interfaces 67
- VNC 65, 68
- VPN pivot 67
- vulnerability 35
  - delete 36
  - edit 36
  - management 35

## W

- webapp reports 73
- word list 49