Metasploit Community

Getting Started Guide
Release 4.4

RAPID7

TABLE OF CONTENTS

About this Guide

Before you Begin

Metasploit Community Tour

Getting Started

ABOUT THIS GUIDE

This guide provides information and instructions to get you started with Metasploit Community. 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 Community as a penetration testing solution.

Organization

This guide includes the following chapters:

- About this Guide
- Before You Begin
- Metasploit Community Tour
- Getting Started

Document Conventions

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

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

Support

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

Support for Metasploit Pro and Metasploit Express

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

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

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

Support for the Metasploit Framework and Metasploit Community

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

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

BEFORE YOU BEGIN

Read the following sections carefully before you install and run Metasploit Community.

Precautions and Warnings

Before installing Metasploit Community, please read the following information:

- Antivirus (AV) software such as McAfee, Symantec, and AVG will cause problems with installation and at run-time. You **MUST** disable your AV before you install and use Metasploit Community.
- Local firewalls, including the Windows Firewall, **MUST** be disabled in order to run exploits successfully. Alternatively, the "bind" connection type may be used, but some exploits still need to receive connections from the target host.
- The RPC service (:50505) on Metasploit Community runs as ROOT, so any Metasploit Community account has privileged access to the system on which it runs. In malicious hands, this can lead to system or network damage. Please protect the service accordingly.
- Metasploit Community is intended only for authorized users. Run Metasploit Community only on machines you own or have permission to test. Using this software for criminal activity is illegal and could result in jail time.
- Local firewalls, including the Windows Firewall, will need to be disabled in order to run exploits successfully. Alternatively, the "bind" connection type may be used, but some exploits still need to receive connections from the target host.

System Requirements

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

Supported Operating Systems

- Windows XP SP2+
- Windows Vista
- Windows 7
- Windows 2003 Server SP1+
- Windows 2008 Server
- RHEL 5+
- Ubuntu 10.04+

Metasploit Community may work on other operating systems, but those operating systems are not officially supported.

User Accounts and License Key Activation

Before you can get started, you must create a user account. The first time you launch Metasploit Community, the system prompts you to create a user account. Complete the new user form to create a user account.

After you create a user account, the license key activation page appears. Enter the license key information that you received from Rapid7 to activate the license key.

Setting up a Vulnerable Virtual Machine

One of the first things you must do is set up a vulnerable target system. The easiest way to set up a vulnerable machine is to use Metasploitable. Metasploitable is an Ubuntu 8.04 server that runs on a VMware image. The Metasploitable virtual machine contains a number of vulnerable services and an install of Apache Tomcat 5.5, DistCC, Tiki Wiki, and MySQL.

Metasploitable provides you with a vulnerable target machine that you can use to work with Metasploit Pro, Metasploit Express, Metasploit Community, and the Metasploit Framework. For information on how to set up Metasploitable, visit the Metasploitable Set Up Guide.

Additionally, you can use UltimateLAMP, which focuses more on web vulnerabilities. To use UltimateLAMP, browse to port 80 on the IP address that you assigned to the virtual machine.

Note: If you already have a workstation or server installed, you can use it as a virtual host. If you want to set up a VM, you can get the free VMWare Player at http://www.vmware.com/products/player/.

Metasploitable Services

Metasploitable runs the following services:

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

UltimateLAMP Services and Applications

UltimateLAMP runs the following services:

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

Downloading the Vulnerable VMs

To access and download Metasploitable, visit http://www.metasploit.com/community/ for the public BitTorrent link.

Setting up the Vulnerable VMs

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

Once the VM is available on your desktop, open the device and run with VMWare Player. Alternatively, you can also use VMWare Workstation or VMWare Server.

After you have a vulnerable machine ready, you can start working with Metasploit Community.

System Requirements for Host and Guest Systems

For a typical host system that will run Metasploit Community and VMware, you should use a 2GHz or faster processor and a minimum of 3GB of memory.

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

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

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

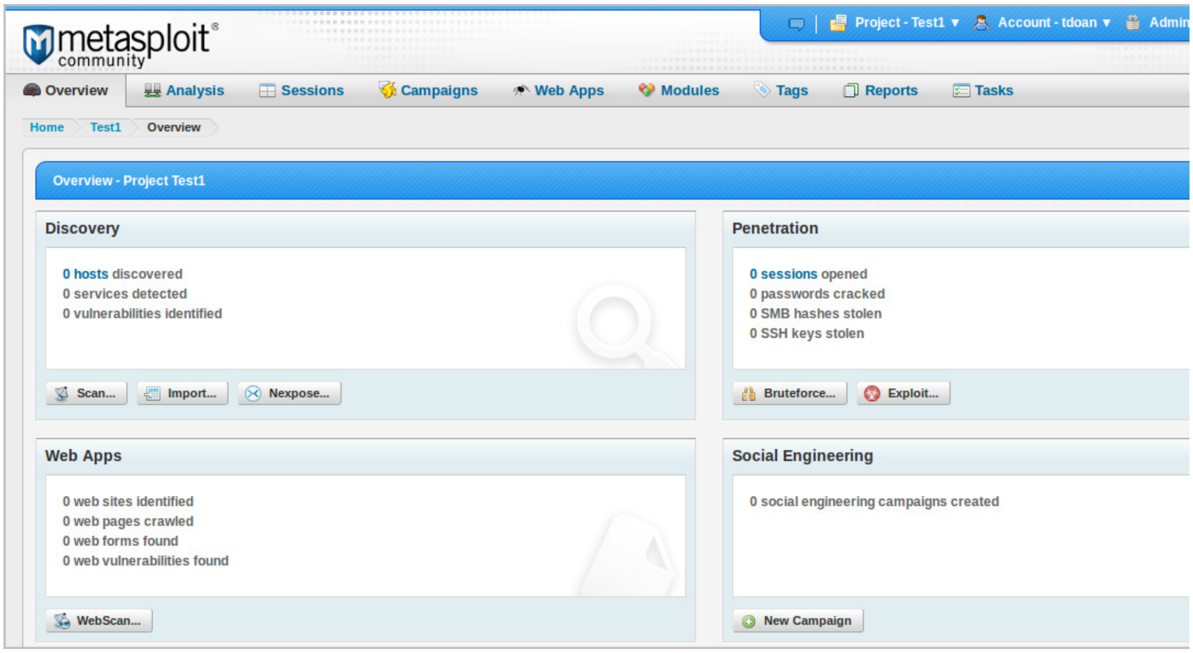
Metasploit Community Tour

Metasploit Community provides a comprehensive and intuitive workspace that you can use to perform administrative tasks and to configure penetration tests. The following sections describe the main areas of the Web UI and the main features for Metasploit Community.

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:



Overview - Project Test1

Discovery

0 hosts discovered
0 services detected
0 vulnerabilities identified

Penetration

0 sessions opened
0 passwords cracked
0 SMB hashes stolen
0 SSH keys stolen

Web Apps

0 web sites identified
0 web pages crawled
0 web forms found
0 web vulnerabilities found

Social Engineering

0 social engineering campaigns created

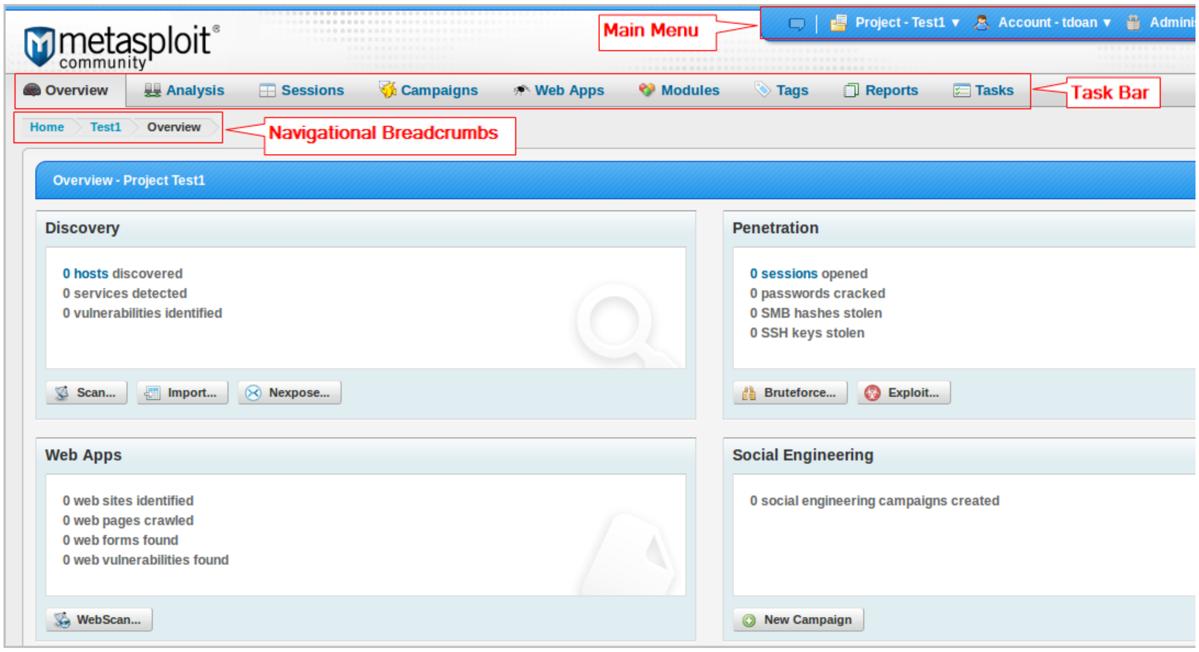
Navigational Tour

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

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:



0 hosts discovered
0 services detected
0 vulnerabilities identified

0 sessions opened
0 passwords cracked
0 SMB hashes stolen
0 SSH keys stolen

0 web sites identified
0 web pages crawled
0 web forms found
0 web vulnerabilities found

0 social engineering campaigns created

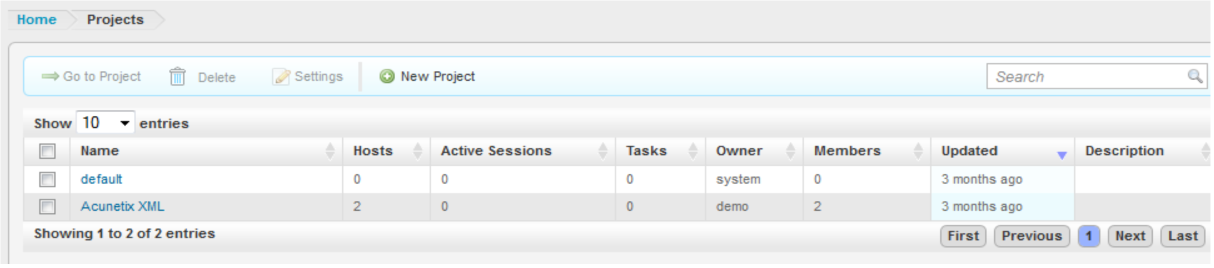
Administration Tour

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

Project Management

A Metasploit Community 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:



Show 10 entries

☐	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updated	Description
☐	default	0	0	0	system	0	3 months ago	
☐	Acunetix XML	2	0	0	demo	2	3 months ago	

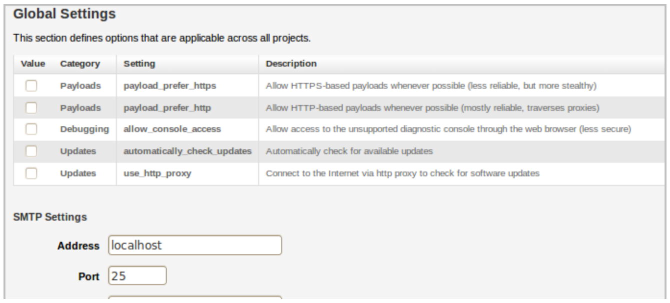
Showing 1 to 2 of 2 entries

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:



Global Settings

This section defines options that are applicable across all projects.

Value	Category	Setting	Description
☐	Payloads	payload_prefer_https	Allow HTTPS-based payloads whenever possible (less reliable, but more stealthy)
☐	Payloads	payload_prefer_http	Allow HTTP-based payloads whenever possible (mostly reliable, traverses proxies)
☐	Debugging	allow_console_access	Allow access to the unsupported diagnostic console through the web browser (less secure)
☐	Updates	automatically_check_updates	Automatically check for available updates
☐	Updates	use_http_proxy	Connect to the Internet via http proxy to check for software updates

SMTP Settings

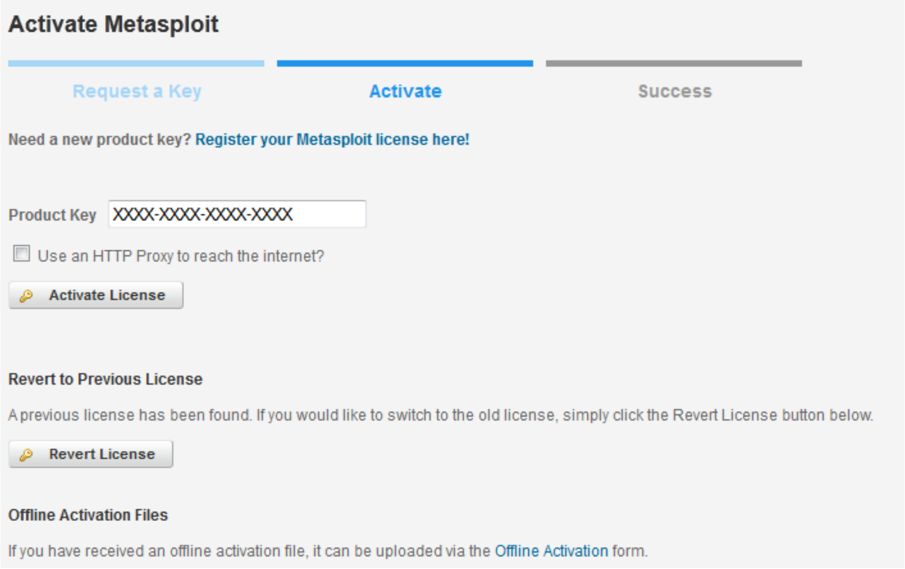
Address: localhost

Port: 25

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:



Need a new product key? Register your Metasploit license here!

Product Key XXXX-XXXX-XXXX-XXXX

□ Use an HTTP Proxy to reach the internet?

Revert to Previous License

A previous license has been found. If you would like to switch to the old license, simply click the Revert License button below.

Offline Activation Files

If you have received an offline activation file, it can be uploaded via the Offline Activation form.

Features Tour

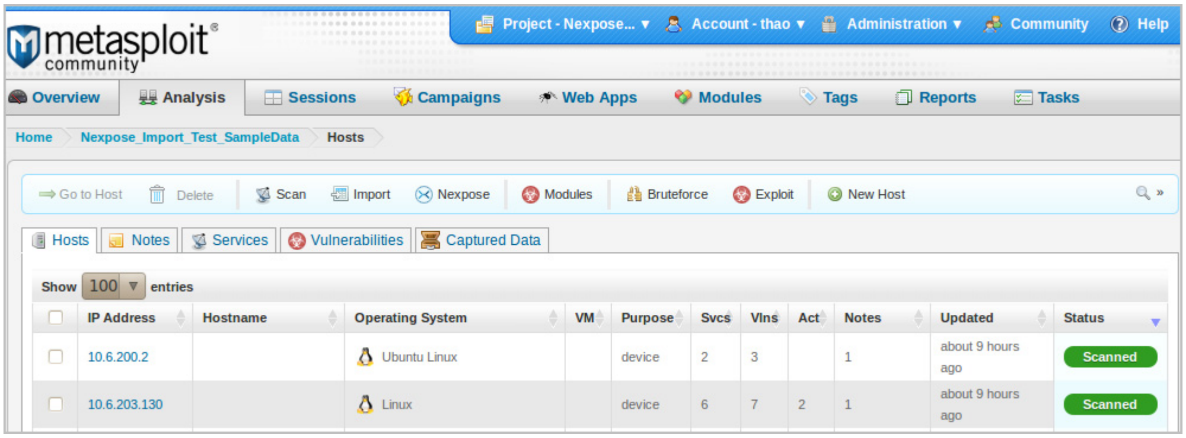
Metasploit Community provides a comprehensive penetration testing system that you can use to scan for target hosts, open and control sessions, exploit vulnerabilities, and generate reports.

Host Scan

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



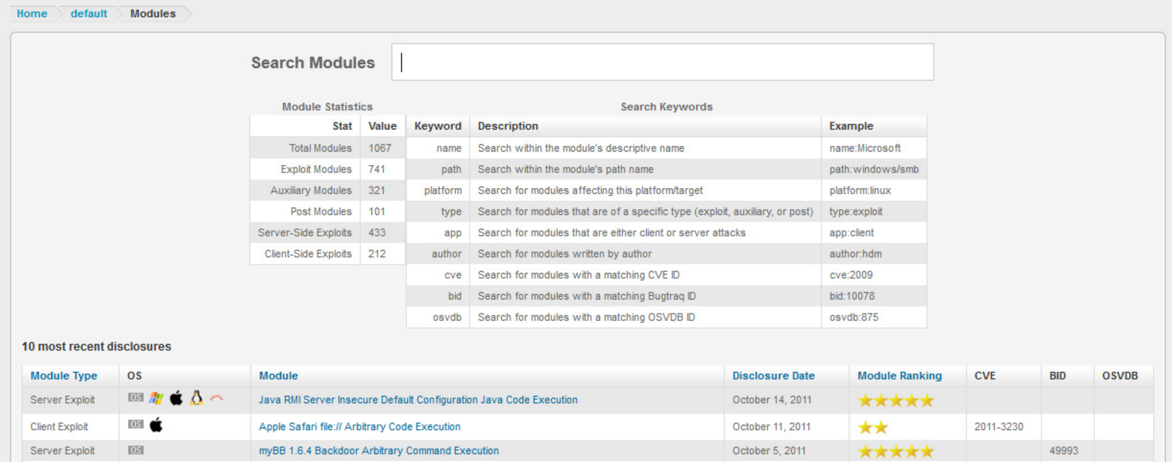
Show 100 entries

□	IP Address	Hostname	Operating System	VM	Purpose	Svcs	Vlns	Act	Notes	Updated	Status
□	10.6.200.2		Ubuntu Linux		device	2	3		1	about 9 hours ago	Scanned
□	10.6.203.130		Linux		device	6	7	2	1	about 9 hours ago	Scanned

Exploitation

Modules expose and exploit vulnerabilities and security flaws in target systems. Metasploit Community offers access to a comprehensive library of exploit modules, auxiliary modules, and post-exploitation modules. 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:



Module Statistics

Stat	Value
Total Modules	1067
Exploit Modules	741
Auxiliary Modules	321
Post Modules	101
Server-Side Exploits	433
Client-Side Exploits	212

Search Keywords

Keyword	Description	Example
name	Search within the module's descriptive name	name:Microsoft
path	Search within the module's path name	path:windows/smb
platform	Search for modules affecting this platform/target	platform:linux
type	Search for modules that are of a specific type (exploit, auxiliary, or post)	type:exploit
app	Search for modules that are either client or server attacks	app:client
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

10 most recent disclosures

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

GETTING STARTED

The following sections show you how to get started with Metasploit Community. This chapter explains how to launch Metasploit Community and create a project. After you create a project, you can run a discovery scan, bruteforce attack, and exploit. For information on how to perform other tasks within Metasploit Community, view the Metasploit Community *User Guide*.

Launching Metasploit Community

You can run Metasploit Community on Windows or Linux. The following sections explain how to launch Metasploit Community in both operating systems.

Launching Metasploit Community in Windows

To access Metasploit Community in Windows, navigate to **Start > All Programs > Metasploit**. To run the Web client, select **Access Metasploit Web UI**.

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

Launching Metasploit Community in Linux

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

To run the web client for Metasploit Community in Linux, browse to https://localhost:3790. If you changed the default port for Metasploit Pro during installation, use that port instead of 3790.

Projects

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

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

Creating a Project

1. Select **Project > Create New Project** from the main menu.
2. Enter the project name.
3. Enter a description for the project.
4. Define the network range (optional).
5. Select **Restrict to network range** if you want to enforce network boundaries on the project.
6. Create the project.

Discovery Scan

A discovery scan is the process that Metasploit Community uses to identify live valid hosts within a target network address range. 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 Community with a valid target range.

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.

   Note: Metasploit Community 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. Click **Show Advanced Options** to verify and configure the advanced options for the scan. If you do not configure additional options, Metasploit Community uses the default configuration for the scan.
5. Run the scan.

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.

Running a Manual Exploit Against All Target Systems

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.