Metasploit Basics

Metasploit Pro is an exploitation and vulnerability validation tool that helps you divide the penetration testing workflow into smaller and more manageable tasks. With Metasploit Pro, you can leverage the power of the Metasploit Framework and its exploit database through a web based user interface to perform security assessments and vulnerability validation.

Metasploit Pro enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

Metasploit Pro is also multi-user, collaborative tool that lets you share tasks and information with the members of a penetration testing team. With team collaboration capabilities, you can divide a penetration test into multiple parts, assign members a specific network segment to test, and let members leverage any specialized knowledge that they may have. Team members can share host data, view collected evidence, and create host notes to share knowledge about a particular target.

The overall process of penetration testing can be broken down into a series of steps or phases. Depending on the methodology that you follow, there can be anywhere between four and seven phases in a penetration test. The names of the phases can vary, but they generally include reconnaissance, scanning, exploitation, post-exploitation, maintaining access, reporting, and cleaning up.

The Metasploit Pro workflow follows the general steps of a penetration test. Besides reconnaissance, you can perform the other penetration testing steps from Metasploit Pro.

1. **Create a project** - Create a project to store the data that you collect from your targets.
2. **Gather information** - Use the Discovery Scan, Nexpose scan, or import tool to supply Metasploit Pro with a list of targets and the running services and open ports associated with those targets.
3. **Exploit** - Use smart exploits or manual exploits to launch attacks against target machines. Additionally, you can run bruteforce attacks to escalate account privileges and to gain access to exploited machines.
4. **Perform post-exploitation** - Use post-exploitation modules or interactive sessions to interact gather more information from compromised targets. Metasploit Pro provides you with several tools that you can use to interact with open sessions on an exploited



information about the compromised systems.

5. **Clean up open sessions** - Use the *Clean Up* option to close any open sessions on an exploited target and to remove any evidence of any data used during the penetration test. This step restores the original settings on the target system.
6. **Generate reports** - Use the reporting engine to create a report that details the findings of the penetration test. Metasploit Pro provides several types that let you to determine the type of information that the report includes.

Accessing Metasploit Pro from the Web Interface

To access the web interface for Metasploit Pro, open a browser and go to https://localhost:3790 if Metasploit Pro runs on your local machine. If Metasploit Pro runs on a remote machine, you need to replace localhost with the address of the remote machine.

To log in to the web interface, you will need the username and password for the account you created when you activated the license key for Metasploit Pro. If you can't remember the password you set up for the account, you'll need to reset your password.

Supported Browsers

If the user interface is not displaying all of its elements properly, please make sure that you are using one of the supported browsers listed below:

- Google Chrome 10+
- Mozilla Firefox 18+
- Internet Explorer 10+
- Iceweasel 18+

Accessing Metasploit Pro from the Command Line

The Pro Console provides the functionality of Metasploit Pro through a command line interface and serves as an alternative to the Metasploit Web UI. If you have traditionally been a Metasploit Framework user, the Pro Console provides you with something similar to msfconsole.

You can use the Pro Console to perform the following tasks:

- Create and manage projects.
- Scan and enumerate hosts.

- View information about hosts.
- Collect evidence from exploited systems.

> You cannot perform all Metasploit Pro tasks through the Pro Console. Tasks that are not supported include reporting, social engineering, running MetaModules, configuring task chains, running bruteforce attacks, and scanning web applications.

Launching the Pro Console on Windows

To launch the console on Windows, select **Start > Metasploit > Metasploit Console**.

You can also start the console from the command line. To launch the console from the command line, enter the following:

```
$ cd /metasploit
$ console.bat
```

```
$ cd /opt/Metasploit/
$ sudo msfpro
```

Did this page help you?

YES NO

Welcome
Getting Started

Welcome
What is Penetration Testing?

SALES SUPPORT

+1-866-772-7437 (Toll Free)

Need immediate help with a breach?

CLICK HERE

SOLUTIONS

All Solutions

Industry Solutions

Compliance Solutions

SUPPORT & RESOURCES

Product Support

Resource Library

Customer Stories

Events & Webcasts

Training & Certification

IT & Security Fundamentals

Vulnerability & Exploit Database

ABOUT US

News & Press Releases

Public Policy

Open Source

Investors

CONNECT WITH US

Contact

Blog

Support Login

Careers