

Forum:[Hack Forums](#)

Thread: [\[TuT\] Introduction to the Metasploit Framework - Modules, Interfaces & Setup](#)

Raymond Reddington - June 30, 2022, 2:00 pm

Introduction to Metasploit
Man's second best friend.

I.) Introduction

The Metasploit framework is a leading exploitation framework used by penetration testers, ethical hackers, and even black-hat hackers to probe and exploit vulnerabilities on systems, networks, and servers. It is an open-source utility developed by Rapid7. For anybody aspiring to enter the realm of cybersecurity, you need to master the Metasploit framework to prosper within it. Metasploit comes with over 1677 exploits for over 25 platforms. These include Android, Windows, Linux, PHP, MySQL, Java, etc.

Within this tutorial, we shall operate Metasploit within the Kali Linux OS distribution. If you're not familiar with it or setting it up, I recommend you to check out my [tutorial thread](#) that guides you through the Kali Linux installation process.

II.) Modules

Before we get started, I'd like you to familiarize yourself with the five main modules of Metasploit:

Exploit: A code that exploits a found vulnerability.

Payload: A code that helps you achieve the goal of exploiting a vulnerability. It runs inside the target system to access the target data, like maintaining access via Meterpreter or a reverse shell.

Auxiliary: The auxiliary module contains a set of programs such as fuzzers, scanners, and SQL injection tools to gather information and get a deeper understanding of the target system.

Encoders: Encoders encrypt the payloads/exploits to protect them against signature-based antivirus solutions. As payloads or exploits contain null or bad characters, there are high chances for them to be detected by an antivirus solution.

Post: The post-exploitation module will help you gather further information about the system. For instance, it can help you dump the password hashes and look for user credentials for lateral movement or privilege escalation.

III.) Interfaces

Metasploit is available in four interfaces currently:

msfcli: Single command-line interface for the Metasploit framework.

msfconsole: Most popular Metasploit interface for the Metasploit framework. It gives you an interactive shell where you can execute commands and run exploits.

msfweb: Web interface of Metasploit that allows you to set up projects and carry out penetration testing tasks.

armitage: Graphical User Interface (GUI) front-end for Metasploit developed in Java.

Before tools like Metasploit existed, pentesters and hackers had to perform a vast majority of tasks manually using various tools and scripts coded manually and from scratch before being able to infiltrate their target networks. However, with the introduction of Metasploit, the game had vastly changed and before we know it, we were able to observe a great increase of talent in the cybersecurity sector.

IV.) System Requirements

The minimum hardware requirements for MetaSploit as per Rapid7's recommendations are:
2 GHz+ processor.

4 GB RAM available (8 GB recommended)

1 GB available disk space (50 GB recommended)

V.) Setup Tutorial

To get started with Metasploit, we will have to initialize the PostgreSQL database system. This system will allow quick and easy access to information and help us with conducting faster searches while scanning for a vulnerability or exploit.

Run the following command to install PostgreSQL if your distribution does not have it preinstalled. If you're using Kali Linux, this step is optional.

Code `sudo apt install postgresql -y`

Proceed to run the PostgreSQL service with the following commands

Code `sudo service postgresql start`
`sudo msfdb init`

We shall proceed with launching Metasploit by running the following command:

Code msfconsole

Fun Fact: msfconsole is the most popular interface to the Metasploit Framework (MSF). It provides an “all-in-one” centralized console and allows you efficient access to virtually all of the options available within MSF.

You can also access the Metasploit framework via the Kali GUI as follows:

You should now have access to the Metasploit Framework (MSF) and their database of vulnerabilities, payloads, scripts and exploits.

VI.) Conclusion

Thank you for staying tuned, within this thread, we've addressed the steps to initialize and install Metasploit. Our future tutorials shall be refined with the usage of Metasploit within them so we hope that this tutorial shall serve as guidance for the upcoming threads and a refresher/introduction for Metasploit.

The possibilities with Metasploit are endless, you can search for exploits for a particular platform and service, use & set payloads and exploit vulnerabilities within record time. Such examples include MySQL injection/exploitation, nmap/port-scanning, bruteforcing MySQL/RDPs, and so on. My future tutorials will only include activity that has been permissible by HF's [Help Docs](#).

As usual, thanks for devoting your time towards this tutorial. This tutorial suite has been strictly for educational purposes and imparting knowledge to fellow members and I do not condone any abuse or misuse arising from it.

Zexo - June 30, 2022, 2:20 pm

Nice tutorial can't wait for the next few. hoping I can follow along with them ;)

miket1212 - October 17, 2022, 3:41 pm

this for sure is a nice tut

oodieLiquor - October 17, 2022, 4:46 pm

Simple, but clear and well explained, thanks for sharing with the community