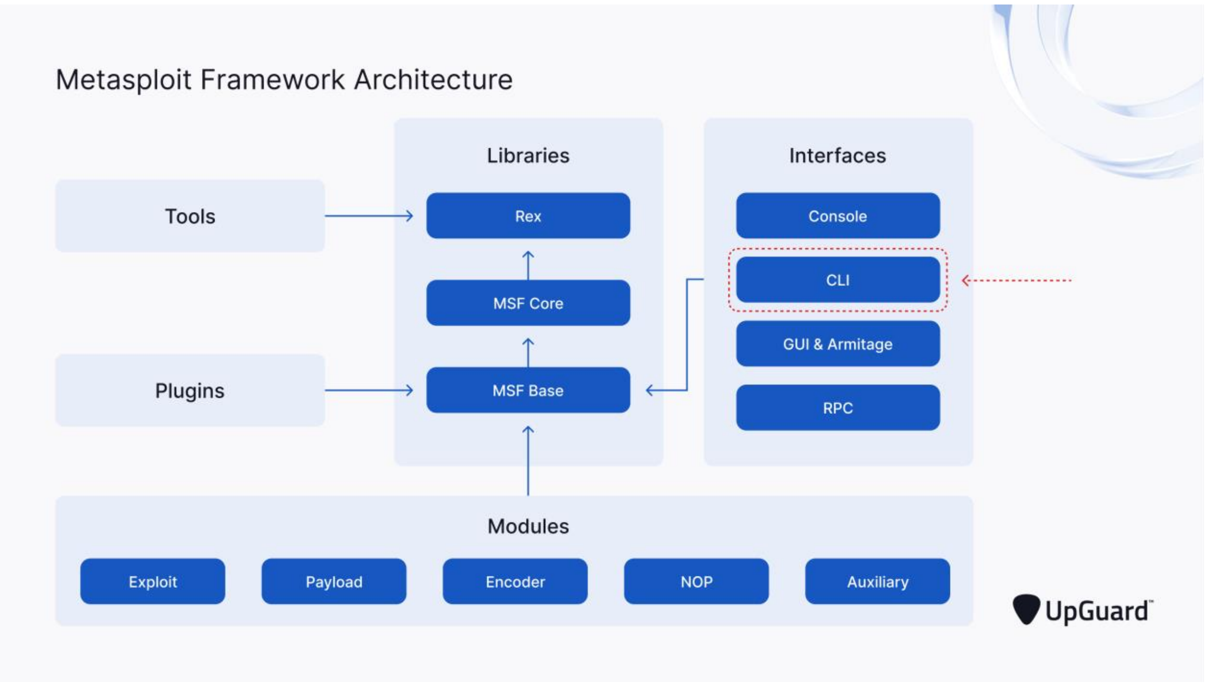
What is Metasploit Framework?

Metasploit is an open-source penetration testing framework used by security researchers as a penetration testing system and a development platform that allows creation of security tools and exploits.

The purpose of Metasploit is to help security researchers identify weaknesses before exploitation by attackers.

How Does Metasploit Work?

The Metasploit framework operates using the functions highlighted in the diagram below.



Now let us learn more about each of the highlighted functions in the Metasploit framework Architecture.

- **Interfaces**

Interfaces in Metasploit are the different platforms through which users can access the Metasploit Framework. The following are the four available interfaces in Metasploit.

1. **MSFConsole (Metasploit Framework Console):** Regarded as the most widely used Metasploit interface, the Metasploit Console allows users to access the Metasploit Framework through an interactive command line interface.

2. **MSFWeb**: Msfweb is the web-based interface that gives users access the Metasploit framework through a browser.

3. **Armitage**: Armitage is a Java-based GUI interface that allows collaboration among red teamers in Metasploit. It helps to display targets, exploit recommendations, and expose advanced post-exploitation features within the framework.

4. **RPC (Remote Procedure Call):** RPC enables users the privilege to remotely make use Metasploit Framework functions using HTTP-based remote procedure call (RPC) services.

   You can use the RPC interface to locally or remotely execute Metasploit commands to perform basic tasks like running modules, communicating with databases, interacting with sessions, and more.

• Libraries

The library contains the available Metasploit Framework features which allow users to perform exploits without the need to write additional codes.

Below are the three available libraries in Metasploit framework.

1. **REX**: This function enables the most basic tasks, it contains Base64, HTTP, SMB, SSL, and Unicode.
2. **MSF CORE:** This feature defines the Metasploit Framework and also Provides Basic API.

3. **MSF BASE:** This feature Provides simplified APIs for use in the Framework

Modules

Most of the interactions in Metasploit Framework happens through its various modules classified by the actions they perform.

The core functionalities that Metasploit framework provides can be summarized by the modules listed below.

Let me explain further the meaning of each modules.

1. **Exploits:** The Metasploit framework has a large database of exploits. Exploits are used to execute command sequences that takes advantage of system or application weaknesses in order to gain access to target systems.

2. **Payloads:** Payload performs various tasks after the exploit is launched. There are several types of payloads that can be used in the modules. For example, you can use a reverse shell payload. This basically creates a **shell/terminal/cmd** on the victim's computer and connects back to the attacker's computer.

3. **Auxiliaries:** Auxiliary modules are built for providing custom functionalities in Metasploit. this includes port scanners, fuzzers, sniffers, etc

4. **Encoders:** Encoders provide users with the ability to use encoders to obscure the code so that threat detection programs cannot easily understand it. After execution, it decrypts itself into the original code.

5. **Posts (Post-Exploitation Modules):** Post allow users to gather more detailed information and further infiltrate the target system after an exploit. For example, Post can be used to perform service enumeration.

6. **NOPs (No Operation):** Nops help maintains a consistent payload size across all exploit attempts. This also helps avoid detection.

What is the difference between an exploit and a payload?

- **Exploit:** Exploits are codes or programs designed to exploit vulnerabilities in a system, software, application or networks etc.
- **Payload:** payloads are codes written to maliciously execute an exploit.

What are the different kinds of payloads?

Payloads in Metasploit are three types.

- **Singles**: payloads are very small and designed to create one type of connection. A single payload is as simple as adding a user to the target system or running badfile.exe.

- **Stages:** Stage payloads can be invoked by stagers, can be of bigger size, and allow external coding. Staging makes it possible to deliver a variety of payloads with just a few stagers.

- **Stagers:** A stager is a small piece of code that performs an action and passes control and data to another payload. Stagers establish communication and transfer data to other payloads.

Components of Metasploit Framework

Metasploit is an open-source program written in Ruby. It is an extensible framework where users can build custom features of their choices using Ruby.

At the core of the Metasploit framework, below are the key components.

1. **Msfconsole:** This is the command line interface used by the Metasploit Framework. This allows you to easily browse all Metasploit databases and use the modules you need.
2. **Msfdb:** Metasploit framework allows users to store and access data quickly and efficiently using PostgreSQL databases. For example, scan results can be stored and organized in a database for later access using msfdb.

3. **Msfvenom:** This helps users create payloads just like its name implies (venoms to inject in your victim machine). It is used to generate and output all of the various types of shellcode that are available in Metasploit.

4. **Meterpreter:** Meterpreter is an advanced payload with many built-in features. It communicates using encrypted packets. Meterpreter is quite difficult to track and locate once in the system. It can take screenshots, generate password hashes, and many more.

What is listener in Metasploit?

Listeners are special handlers in the Metasploit infrastructure that interact with sessions created by payloads.

A listener can either be embedded in a bind shell and listen for connections, or it can be actively listening to incoming connections on the security tester's machine. Without the listener, back and forth communication would not be possible.

Conclusion:

There are so many vectors from which targets could be attacked, but Metasploit Framework makes it much easier with several advanced features, this is why it remains one of the most popular tools in a security researcher's arsenal.

References:

https://www.sciencedirect.com/topics/computer-science/metasploit-framework

https://www.upguard.com/blog/metasploit

https://www.offensive-security.com/metasploit-unleashed/

https://www.systranbox.com/what-is-payload-in-kali-linux/#4

https://nooblinux.com/metasploit-tutorial/