Metasploit

Metasploit is an open-source penetration framework that is used by security engineers to find vulnerabilities on servers and networks. Once vulnerabilities are found the user can take that information to address the weaknesses within a system and find a solution. Metasploit is easily customizable and can be used with most operating systems because it is open-source.

Metasploit has over 1677 exploits organized over 25 platforms. THis framework consists of 5 parts which are:

- Interfaces- different platforms used to access the metasploit framework
- Libraries- contains different functions that allow users to run exploits without the need of having to write additional code themselves
- Modules- software used to perform task like target exploitation and scanning
- Tools & Plugins - an addon to the framework that is used to extend its functionality

According to “Simplilearn.com” Metasploit provides you with varied use cases, and its benefits include:

Open Source and Actively Developed – Metasploit is preferred to other highly paid penetration testing tools because it allows accessing its source code and adding specific custom modules.

Ease of Use – it is easy to use Metasploit while conducting a large network penetration test. Metasploit conducts automated tests on all systems in order to exploit the vulnerability.

Easy Switching Between Payloads – the set payload command allows easy, quick access to switch payloads.

Cleaner Exits – Metasploit allows a clean exit from the target system it has compromised.

Friendly GUI Environment – friendly GUI and third-party interfaces facilitate the penetration testing project.

If you are using kali Linux metasploit is preinstalled in your system so there is no need to download it. Github helps to download and install metasploit on both Windows and Linux systems.

Basic Commands for the Msfconsole

- Help- will show you every command that is available within the msfconsole
- Show exploits- shows you various exploits that you are able to execute
- Set TARGET- let’s you choose a specific target application and OS when permitted by exploits
- Exit- allows u to exit the metasploit console