Metasploit

Metasploit -Introduction

- Metasploit is one of the most powerful tools used for penetration testing.
- It is owned by Boston, Massachusetts-based security company **Rapid7**
- https://www.metasploit.com.
- **Metasploit Pro**: The *commercial* version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).
- **Metasploit Framework**: The open-source version that works from the command line.
- Metasploit community version(free) embedded in Kali along with other ethical hacking tools.

Metasploit Framework

- The Metasploit Framework is a set of tools that allow information gathering, scanning, exploitation, exploit development, post-exploitation, and more.

The main components of the Metasploit Framework can be summarized as follows;

- **msfconsole**: The main command-line interface.
- **Modules**: supporting modules such as exploits, scanners, payloads, etc.
- **Tools**: Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing.
- Some of these tools are msfvenom, pattern_create and pattern_offset.

Metasploit -Modules

- **Exploit modules—**allow testers to target a specific, known vulnerability.
- **Auxiliary modules—**allow testers to perform additional actions required during a penetration test which are not related to directly exploiting vulnerabilities
- **Post-exploitation modules—**allow testers to deepen their access on a target system and connected systems.
- **Payload modules—**provide shell code that runs after the tester succeeds in penetrating a system.
- **No Operation (NOPS) generator—**produces random bytes that can pad buffers, with the objective of bypassing intrusion detection and prevention (IDS/IPS) systems.
- **Datastore**—central configuration that lets testers define how Metasploit components behave.

Metasploit - Commands

Command	Description
search	Allows you to search from the Metasploit database based on the given protocol/application/parameter
use	Allows you to choose a particular module and changes the context to module-specific commands
info	Provides information about the selected module
show	Displays information about the given module name and options for the current module
check	Checks if the target system has a vulnerability
set	It's a context-specific variable that configures options for the current module
unset	Removes previously set parameters
run	Execute the current module

Metasploit - Advantages and disadvantages

Advantages

- Metasploit is open source, and hence free!
- There is a huge community that will enable you to use the features in much better way.
- This framework is mostly up to date as it gets updated frequently.
- User-specific exploit can be easily deployed

Disadvantages

- Learning Metasploit can be a challenging task.
- There is very limited GUI based utility, as it is mostly CLI driven.
- If not handled safely, it can crash the system.
- In case your system has antivirus, it might be difficult to install Metasploit.