Metasploit Framework

Armitage - GUI for Metasploit Framework

** Metasploit Console **

First need to start postgresql database to run metasploit on,

In terminal, type to start the database service:
    service postgresql start

Then to run metasploit type,

    msfconsole

Basic Commands

help - (Gives you access to a menu to explain the commands you can use with the Framework)

search [<options>] [<keywords>] - (Allows you to find a module based on what keyword knowledge you give)
                                                Ex:
                                                    search type:exploit platform:windows flash

use <name | term | index> - (Allows you to load a module (exploit))
                                        Ex:
                                            use exploit/windows/browser/adobe_flash_avm2

show all - (Displays all the information about the module loaded)

show options - (Displays the options we can change about the module, changes depend on the how and method of exploitation)
                    - (Options include: Number of Retries, Server Host, Server Port, SSL/SSLCert (enable/disable), URI Path)

set [option] [value] - (Allows you to change a specific option about the module)
                            - (Options include: Retries, SRVHOST, SRVPORT, SSL, SSLCert, URIPATH)

show payloads - (Displays all of the payloads that you can load, different way of approaching an attack)

show targets - (Displays the exploitable targets)

show info - (Gives you information about the exploit)

back - (Takes you a step back in the msfconsole)

exit - (Terminates the msfconsole framework)

Understanding Metasploit Modules

Modules usually saved in the following directory:

    cd /usr/share/metasploit-framework/modules

Exploits - A module that will take advantage of a system's vulnerability and it will install/plant a payload onto the victim machine

Payloads - Files left onto the victim machine that gives you access or control over the system
- Ex: Rootkits / reverse shell

- Divided into 3 groups:
1. Singles - (Designed to do one single action)
Ex: Keylogging
2. Stagers - (Used for creating a communication link between the attacker and the victim machine)
- (Can be used to deliver another payload)
3. Stages - (Very large payloads, can give very good control over the target)
Ex: VNC connections, meterpreter shell, reverse shell

Auxiliary - Unique types of modules that perform scanning, fuzzing, sniffing, etc. to find vulnerabilities about the target

Encoders - Used to re-encode payloads and exploits to get by security systems such as anti-viruses

Nops (No Operation) - Causes the system's CPU to do nothing for 1 clock cycle which can allow you to remotely execute a specific file/code after you've exploited the buffer overflow

Post - Used after the target system has been exploited, allows you to perform further attacks once the system has been owned
Ex: Keyloggers, webcam, browser information