05 System Hacking

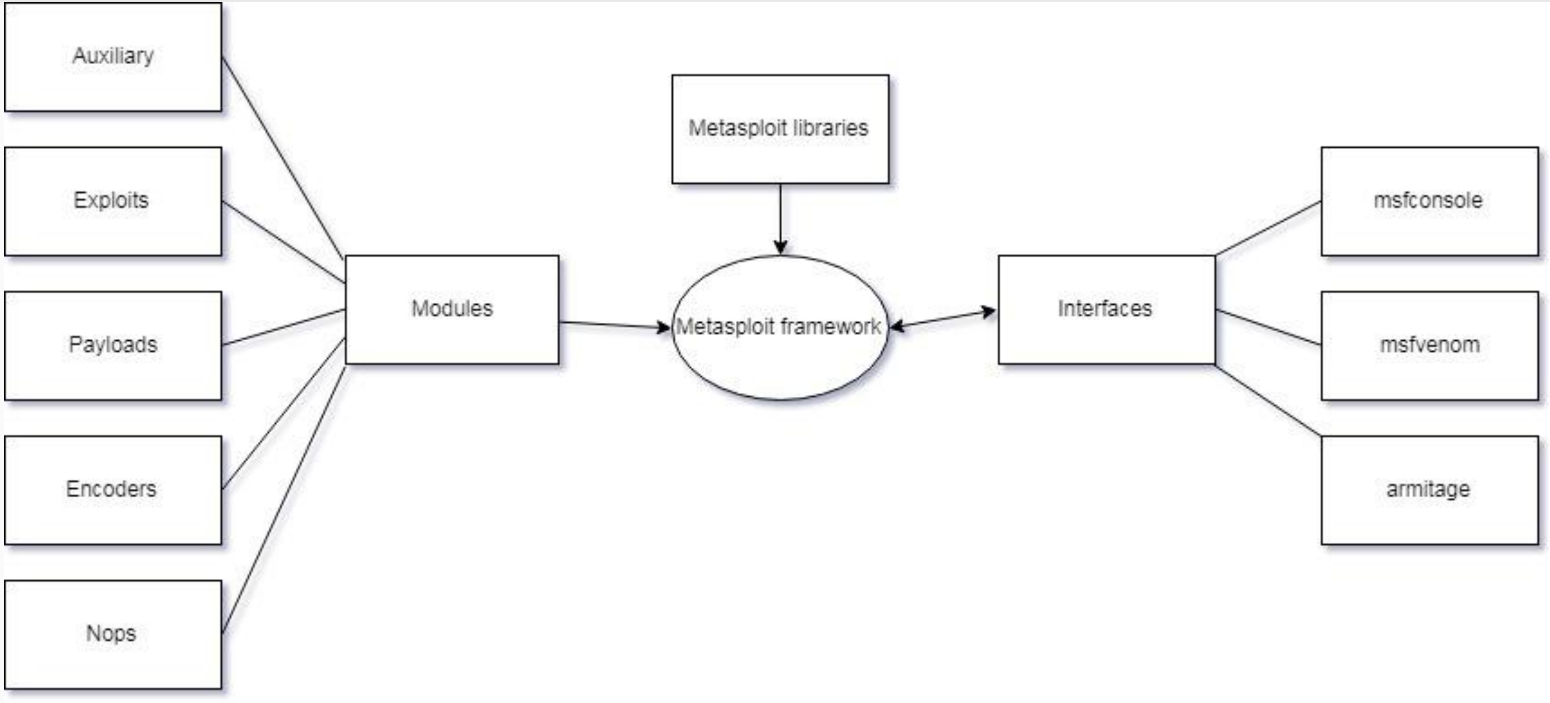
Quick recap of techniques we’ve learnt

- Introduction to ethical hacking, basic linux OS and networking concepts
- Footprinting & Reconnaissance
- Scanning
- Enumeration

Introduction to Metasploit Framework

Metasploit framework is an open source penetration testing project that helps you to find out systems and application vulnerabilities and exploit these weak points into the system. It has the world's largest database of public, tested exploits

Metasploit Framework Layout



Metasploit Architecture

- Modules

  Exploits & Auxiliary

  - Exploits are code that take advantage of vulnerabilities to compromise target system for delivering payload
  - An exploit without payload is auxiliary module

  Payloads, Encoders and Nops

  - Payload consist of code that runs remotely.
  - Encoders ensure that payload makes it to their destination.
  - Nops keep the payload sizes consistent

Metasploit Interface

Accessing the metasploit interface (msfconsole)

The msfconsole is probably 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 options available in MSF. Msfconsole may seem intimidating at first, but once you learn the syntax of commands you will learn to appreciate the power of utilizing this interface

Vulnerability, Exploit and Payload revisited

Vulnerability

A weakness which allows an attacker to break into or compromise a system's security.

Like the main gate of a house with weak lock(can be easily opened), a glass window of a house(can be easily broken) etc can be vulnerabilities in the systems which make it easy for an attacker to break into

Exploit

Code which allows an attacker to take advantage of a vulnerability in system.

The set of different keys, which he can try one by one to open the lock, the hammer with him which he can use to break the glass window etc can be exploits

Payload

Actual code on the system that runs after exploitation

Now, finally after exploiting the vulnerability and breaking in he can have different things to do. He can steal money, destroy the things or just give a look and come back. Deciding this is what we mean by setting the payload

Some more wiki on payloads

There are three different types of payload modules in the metasploit framework : Singles, Stager and Stages or Inline and staged

Whether or not a payload is staged, is represented by ‘/’ in the payload name. For example, “windows/shell_reverse_tcp” is a single payload with no stage, whereas “windows/shell/bind_tcp” consists of a stager(bind_tcp) and a stage(shell)

Single or Inline

Singles are payloads that are self contained and completely standalone. A single payload can be something as simple as adding a user to the target system or running a calc.exe

Stager

Stagers setup a network connection between the attacker and victim and are designated to be small and reliable.

Stages

Stages are payload components that are downloaded by stagers modules. The various payload stages provide advanced features with no size limits such as meterpreter, vnc injection etc

After gathering information about target system

- Select the right exploit, and then set the target
- Verify the exploit options to determine whether the target system is vulnerable to the exploit
- Select a payload
- Execute the exploit

Let’s combine all and see how it actually works

Let us assume a scenario where an attacker executes exploit+payload against a victim against vulnerable service on his machine.

We will compromise a victim running Windows XP

Frequently used commands

- show
- search
- info
- use
- set
- unset
- kill
- sessions
- jobs

Some useful options

RHOST	Remote Host(Victim) IP address
RPORT	Remote (Victim) port number
LHOST	Local Host(Attacker) IP address
LPORT	Local (Attacker)port to connect back on
SRVHOST	Local Host(Attacker) IP address
SRVPORT	Local (Attacker)port to connect back on
URIPATH	/

IP -> all IP addresses discussed can be public or private IP