



1. MetaSploit

Module 8



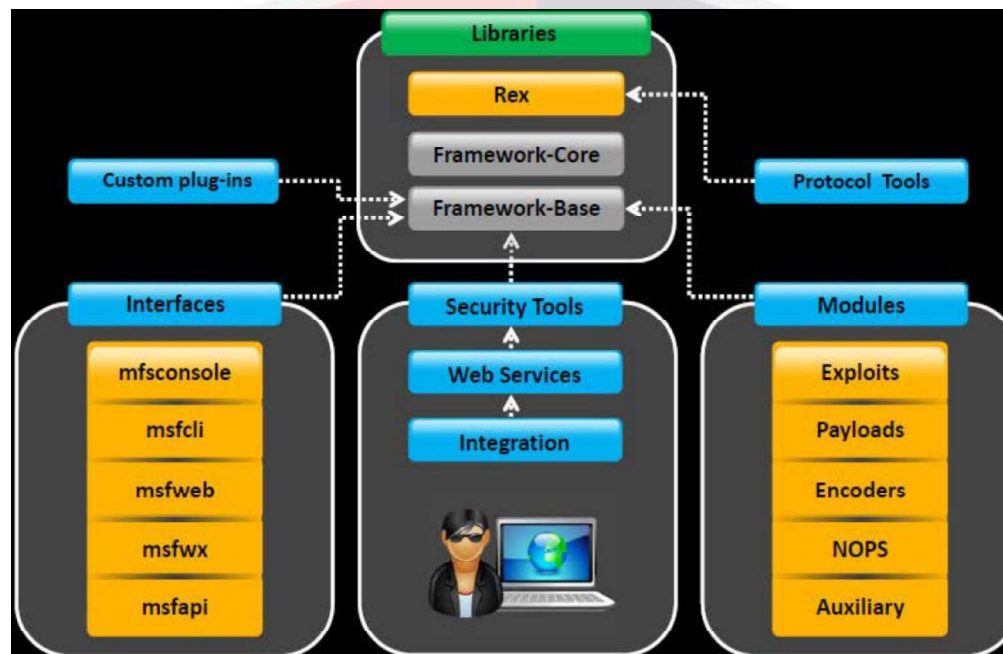
MetaSploit

- The Metasploit Framework is a penetration testing **toolkit**, **exploit development platform**, and **research tool** that includes **hundreds** of working **remote exploits** for a variety of platforms.
- It supports fully **automated exploitation** of web servers, by **abusing known vulnerabilities** and leveraging weak passwords via **Telnet, SSH, HTTP**, and **SNMP**.



MetaSploit

Metasploit Architecture





MetaSploit

Metasploit Exploit Module

- ▷ It is the basic module in Metasploit used to encapsulate an exploit using which users target many platforms with a single exploit.
- ▷ This module comes with simplified meta-information fields.
- ▷ Using a Mixins feature, users can also modify exploit behavior dynamically, brute force attacks, and attempt passive exploits.
- ▷ **Steps to exploit a system follow the Metasploit Framework:**
 - ▷ Configuring Active Exploit
 - ▷ Verifying the Exploit Options
 - ▷ Selecting a Target
 - ▷ Selecting the Payload
 - ▷ Launching the Exploit



MetaSploit

Metasploit Payload Module

- ▶ Payload module **establishes** a **communication** channel between the **Metasploit** framework and the **victim** host.
- ▶ It **combines** the arbitrary **code** that is **executed** as the result of an **exploit** **succeeding**.
- ▶ To **generate** (**stageless**) payloads, first select a payload using the command:
 - ▶ `msf > use windows/shell_reverse_tcp`
 - ▶ `msf payload(shell_reverse_tcp) > generate -h`



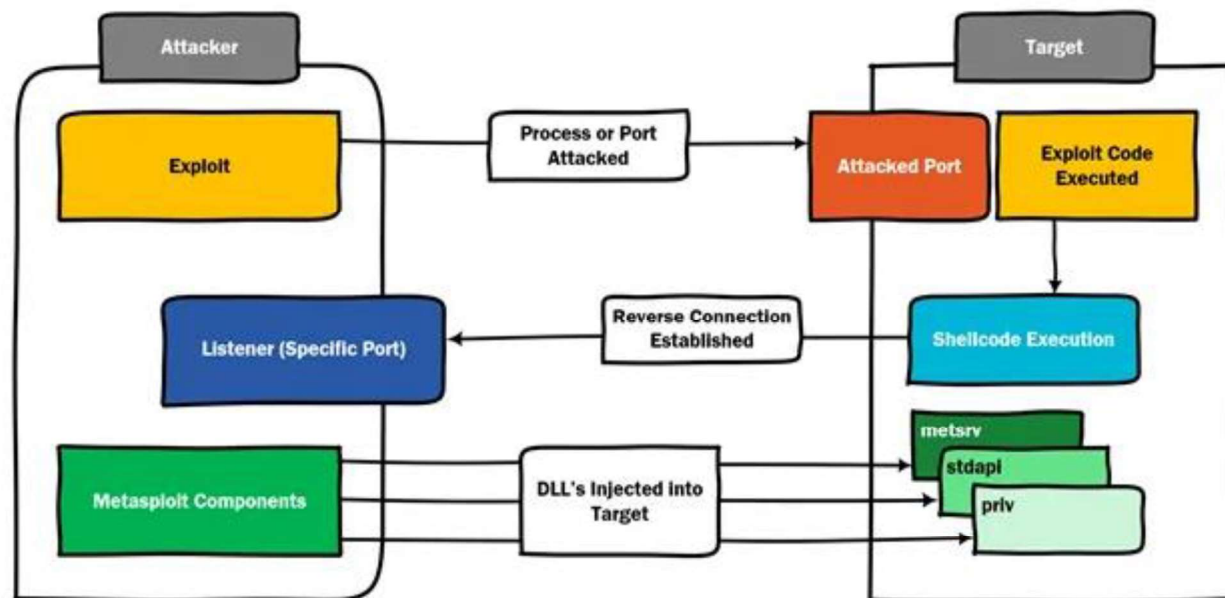
MetaSploit

Metasploit Payload Module

- There are **three types** of **payload** modules provides by the Metasploit:
 - **Singles**: It is **self-contained**, **fire-and-forget**, completely **standalone**.
 - **Stagers**: It **sets** up a network **connection** between the **attacker** and **victim**.
 - **Stages**: It is **downloaded** by **stagers** modules.
 - **Stageless(New)**: The **entire** payload is **sent** in **one hit** and executed on the target machine.



MetaSploit





MetaSploit

Payload	Staged	Stageless
Reverse TCP	windows/meterpreter/reverse_tcp	windows/meterpreter_reverse_tcp
Reverse HTTPS	windows/meterpreter/reverse_https	windows/meterpreter_reverse_https
Bind TCP	windows/meterpreter/bind_tcp	windows/meterpreter_bind_tcp
Reverse TCP IPv6	windows/meterpreter/reverse_ipv6_tcp	windows/meterpreter_reverse_ipv6_tcp



MetaSploit

■ Metasploit Auxiliary Module

- Metasploit's auxiliary modules can be used to perform arbitrary, one-off actions such as port scanning, denial of service, and even fuzzing.
- To run auxiliary module, either use the run command, or use the exploit command.



MetaSploit

Metasploit NOPS Module

- ▶ NOP modules generate a **no-operation instructions** used for **blocking out buffers**.
- ▶ Use **generate** command to generate a NOP **sled** of an **arbitrary size** and display it in a given format OPTIONS:
 - ▶ **-b < opt>**: The list of characters to avoid: '\x00\xff'
 - ▶ **-h**: Help banner
 - ▶ **-s < opt>**: The comma separated list of registers to save
 - ▶ **-t < opt>**: The output type: ruby, perl, c, or raw msf nop(opty2)>



MetaSploit

Generates a NOP sled of a given length

```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```



Command to generate a 50 byte NOP sled

```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x
66\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x
84\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\xa9\xb0\xb7\x
2f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```