

Metasploit Installation and Setup

Prepared by: Nirmiti Dhawade

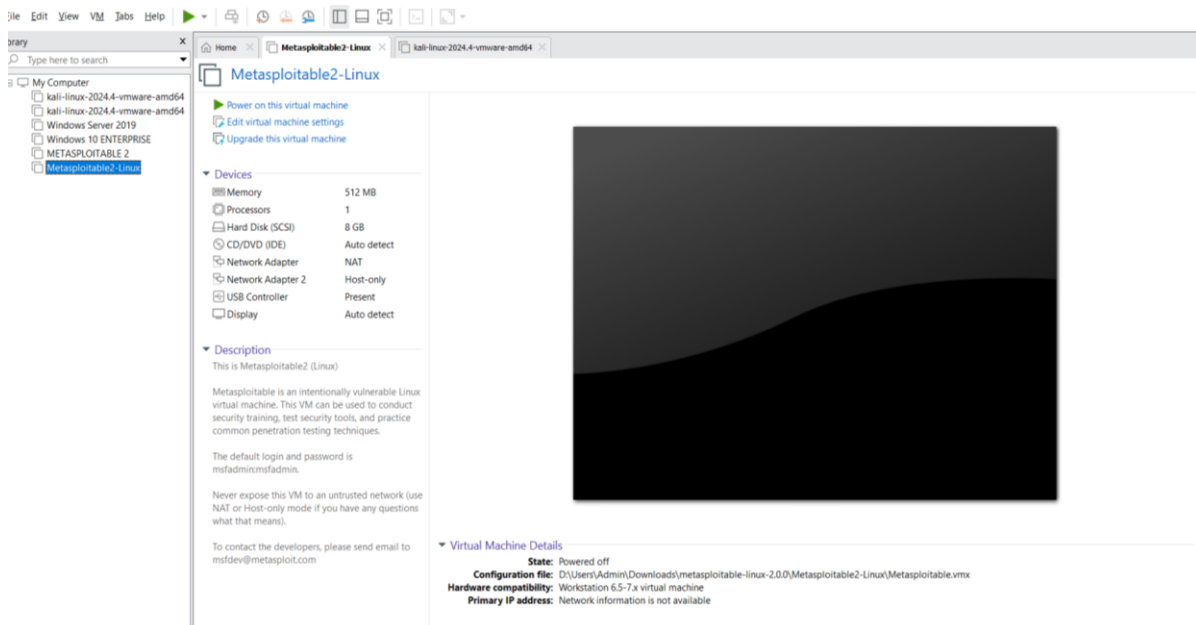
Date: [28-08-2025]

This document explains how to set up and verify the Metasploit Framework on Kali Linux. Each step also suggests screenshots you can add for documentation or project submission.

1. Requirements Before You Start

To begin the setup, ensure you have:

- Kali Linux installed (in VirtualBox or VMware).
- A working internet connection.
- Access to the terminal with sudo privileges.



2. Installing Metasploit on Kali Linux

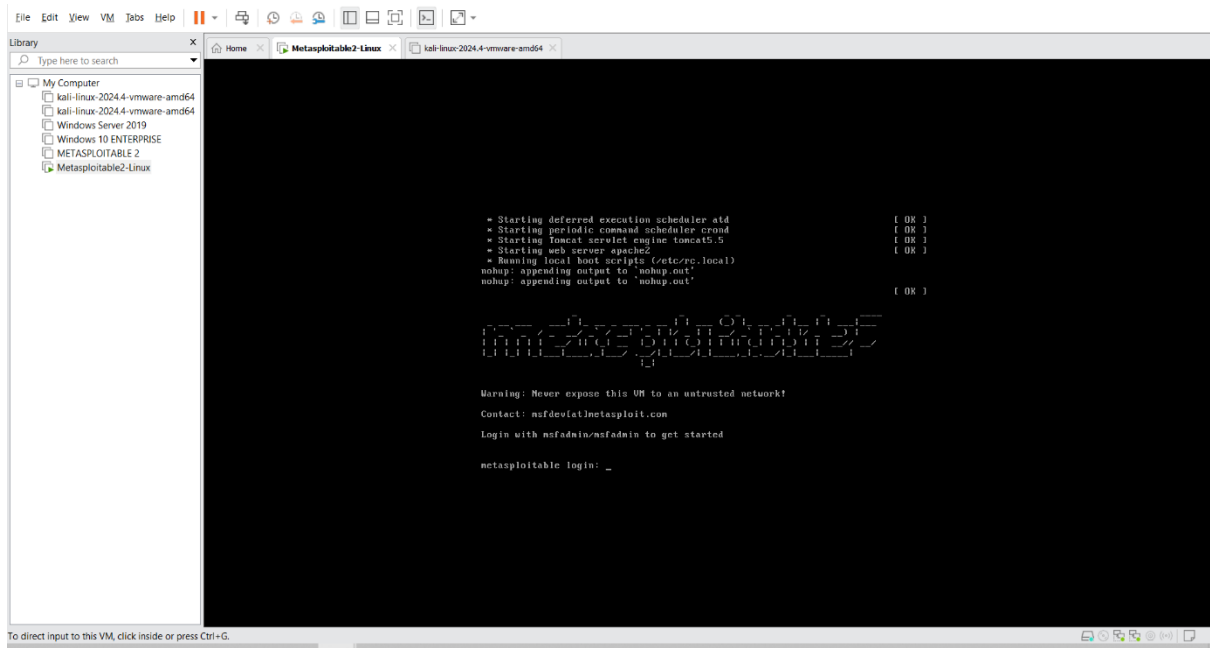
Open your terminal and run these commands to update your system and install Metasploit:

```
sudo apt update
```

```
sudo apt install metasploit-framework
```

Once installed, test it by launching:

```
msfconsole
```



3. Setting Up the Metasploit Database

Metasploit uses PostgreSQL to manage and store data. Start it with:

```
sudo systemctl start postgresql
```

```
sudo systemctl enable postgresql
```

4. Confirming Everything Works

To make sure the setup is successful, just run:

msfconsole

You should see Metasploit loading and the prompt (msf6 >) where you can enter commands.

```

kali@kali: ~
File Actions Edit View Help

kali@kali: ~ x kali@kali: ~ x

zsh: corrupt history file /home/kali/.zsh_history
kali@kali: ~
msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

To boldly go where no
shell has gone before

+ [ metasploit v6.4.34-dev ]
+ -- [ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- [ 1468 payloads - 49 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

~[A*][A*][A*][A*][A*][Amsf0 >

```

5.Try a Simple Scan (Optional)

Here's a basic example of using a Metasploit scanner module to check open ports:

```
use auxiliary/scanner/portscan/tcp
```

```
set RHOSTS [Target-IP]
```

```
run
```