

[Home](#) » [Ubuntu](#) » [How to Install Metasploit Framework on Ubuntu 22.04 | 20.04](#)

How to Install Metasploit Framework on Ubuntu 22.04 | 20.04

Last Updated on Saturday, April 22, 2023 by Joshua James

Metasploit Framework is an open-source platform that has become a powerful tool for penetration testing and vulnerability assessment in today's cybersecurity landscape. It is designed to help security professionals perform comprehensive testing of their network's security posture, identify potential weaknesses, and mitigate them before attackers can exploit them.

If you are in the field of information security or work in a related area, installing Metasploit Framework on your system can offer several benefits, including:

- **Robust Exploitation Capabilities:** With over 1,500 exploits, Metasploit Framework provides a vast library of exploits that can test various operating systems, applications, and devices. It allows you to conduct automated attacks to pinpoint system vulnerabilities, test patch effectiveness, and provide detailed reports.
- **Flexible Payload Options:** Payloads are used to deliver a malicious payload to a victim's system. Metasploit Framework offers a wide range of payloads that can be customized for different scenarios. Payload options include reverse shell, meterpreter, and VNC, among others.
- **Multiple Interfaces:** Metasploit Framework supports multiple interfaces, making it easy for users to choose the most comfortable environment to work in. The web interface is the most user-friendly and can be accessed from any device with a web browser.
- **Collaborative Environment:** Metasploit Framework provides a collaborative platform where users can share their exploits, payloads, and modules. This encourages collaboration among security professionals, enhances

knowledge sharing, and ensures everyone stays updated with the latest vulnerabilities and mitigation strategies.

- **Scripting Support:** The framework allows creating custom scripts to automate tasks and workflows, making it an ideal choice for complex and time-consuming processes.

However, installing Metasploit Framework on your main computer production environment should be done cautiously. Some of the risks to consider include the following:

- Metasploit is a powerful tool that can cause serious damage if used incorrectly, especially in a production environment. An accidental click of the wrong button can result in a system becoming unstable, resulting in loss of data, loss of productivity, and in extreme cases, lawsuits.
- The framework is also often used by cybercriminals to launch attacks. Installing Metasploit in a production environment with no protective measures can create more security risks than benefits.

Now that we have introduced the topic, this guide will explain the process of installing the Metasploit Framework on a Ubuntu 22.04 Jammy Jellyfish or Ubuntu 20.04 Focal Fossa system through the command line terminal.

Additionally, it will provide step-by-step instructions for setting up the graphical interface for the first time.

Table of Contents

- Step 1: Install Dependencies
- Step 2: Import Metasploit Repository
- Step 3: Install Metasploit
- Metasploit Framework Terminal Commands
- Using Meterpreter
- Conclusion

Step 1: Install Dependencies

Update and Upgrade Ubuntu

Before installing the dependencies, we need to update and upgrade the Ubuntu system. Run the following commands in your terminal:

```
sudo apt update
sudo apt upgrade
```

Install Dependencies

Once the system is updated, we can now install the required dependencies. Run the following command to install all the necessary packages:

```
sudo apt install curl ca-certificates apt-transport-https software-properties-common lsb-release postgresql -y
```

Step 2: Import Metasploit Repository

Once you have installed the necessary dependencies, importing the Metasploit repository is next. To ensure that the packages in the repository are genuine and have not been tampered with, you must import the GPG key associated with the repository. This key will be used to verify the authenticity of the packages during installation.

```
curl -fsSL https://apt.metasploit.com/metasploit-framework.gpg.key |
sudo gpg --dearmor | sudo tee /usr/share/keyrings/metasploit.gpg >
/dev/null
```

Now that you have imported the GPG key, you can import the Metasploit repository by executing the following command in your terminal or command prompt.

```
echo "deb [signed-by=/usr/share/keyrings/metasploit.gpg]
http://downloads.metasploit.com/data/releases/metasploit-
framework/apt lucid main" | sudo tee /etc/apt/sources.list.d
/metasploit.list
```

Step 3: Install Metasploit

After importing the GPG key and repository, refresh your APT cache. This will update your system's package list and ensure the latest Metasploit Framework version is available for installation.

```
sudo apt update
```

To install the Metasploit framework, execute the following command in your terminal or command prompt. This command will initiate the installation process for the framework and configure it to work on your system.

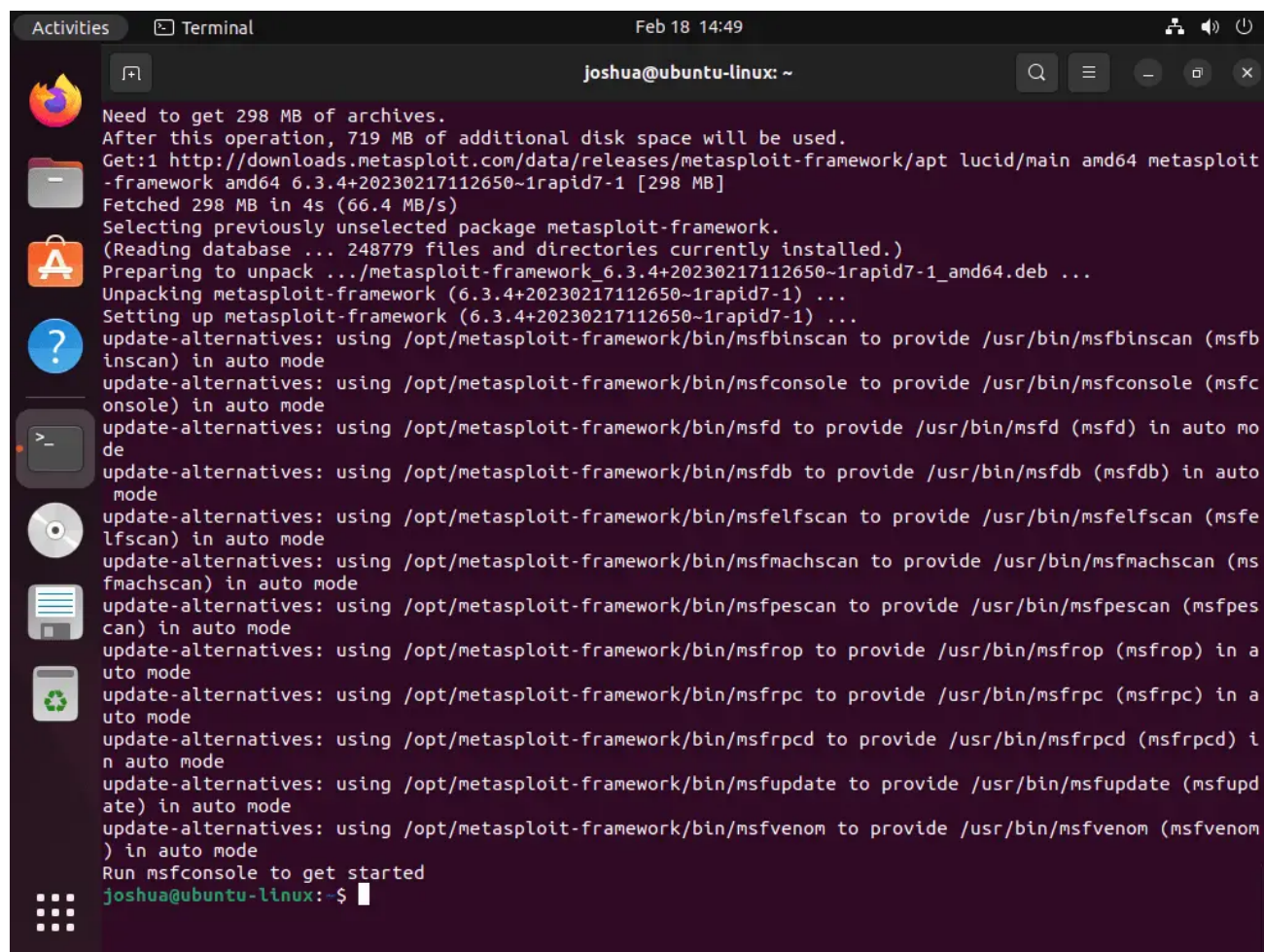
```
sudo apt install metasploit-framework
```

After installing the Metasploit Framework, you must complete the first-time setup process. This involves following a series of prompts in your terminal to configure and prepare the framework for use.

In your terminal output, you should see "Run msfconsole to get started."

```
msfconsole
```

Example:



```
Need to get 298 MB of archives.  
After this operation, 719 MB of additional disk space will be used.  
Get:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid/main amd64 metasploit-  
framework amd64 6.3.4+20230217112650~1rapid7-1 [298 MB]  
Fetched 298 MB in 4s (66.4 MB/s)  
Selecting previously unselected package metasploit-framework.  
(Reading database ... 248779 files and directories currently installed.)  
Preparing to unpack .../metasploit-framework_6.3.4+20230217112650~1rapid7-1_amd64.deb ...  
Unpacking metasploit-framework (6.3.4+20230217112650~1rapid7-1) ...  
Setting up metasploit-framework (6.3.4+20230217112650~1rapid7-1) ...  
update-alternatives: using /opt/metasploit-framework/bin/msfbinscan to provide /usr/bin/msfbinscan (msfb  
inscan) in auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfconsole to provide /usr/bin/msfconsole (msfc  
onsole) in auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfd to provide /usr/bin/msfd (msfd) in auto mo  
de  
update-alternatives: using /opt/metasploit-framework/bin/msfdb to provide /usr/bin/msfdb (msfdb) in auto  
mode  
update-alternatives: using /opt/metasploit-framework/bin/msfelfscan to provide /usr/bin/msfelfscan (msfe  
lfscan) in auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfmachscan to provide /usr/bin/msfmachscan (ms  
fmachscan) in auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfpescan to provide /usr/bin/msfpescan (msfpe  
scan) in auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfrop to provide /usr/bin/msfrop (msfrop) in a  
uto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfrpc to provide /usr/bin/msfrpc (msfrpc) in a  
uto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfrpcd to provide /usr/bin/msfrpcd (msfrpcd) i  
n auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfupdate to provide /usr/bin/msfupdate (msfupd  
ate) in auto mode  
update-alternatives: using /opt/metasploit-framework/bin/msfvenom to provide /usr/bin/msfvenom (msfvenom  
) in auto mode  
Run msfconsole to get started  
joshua@ubuntu-linux:~$
```

During the first-time setup process for the Metasploit Framework, you may encounter various prompts depending on the specific version you are installing. Here is an example of some of the prompts you may encounter:

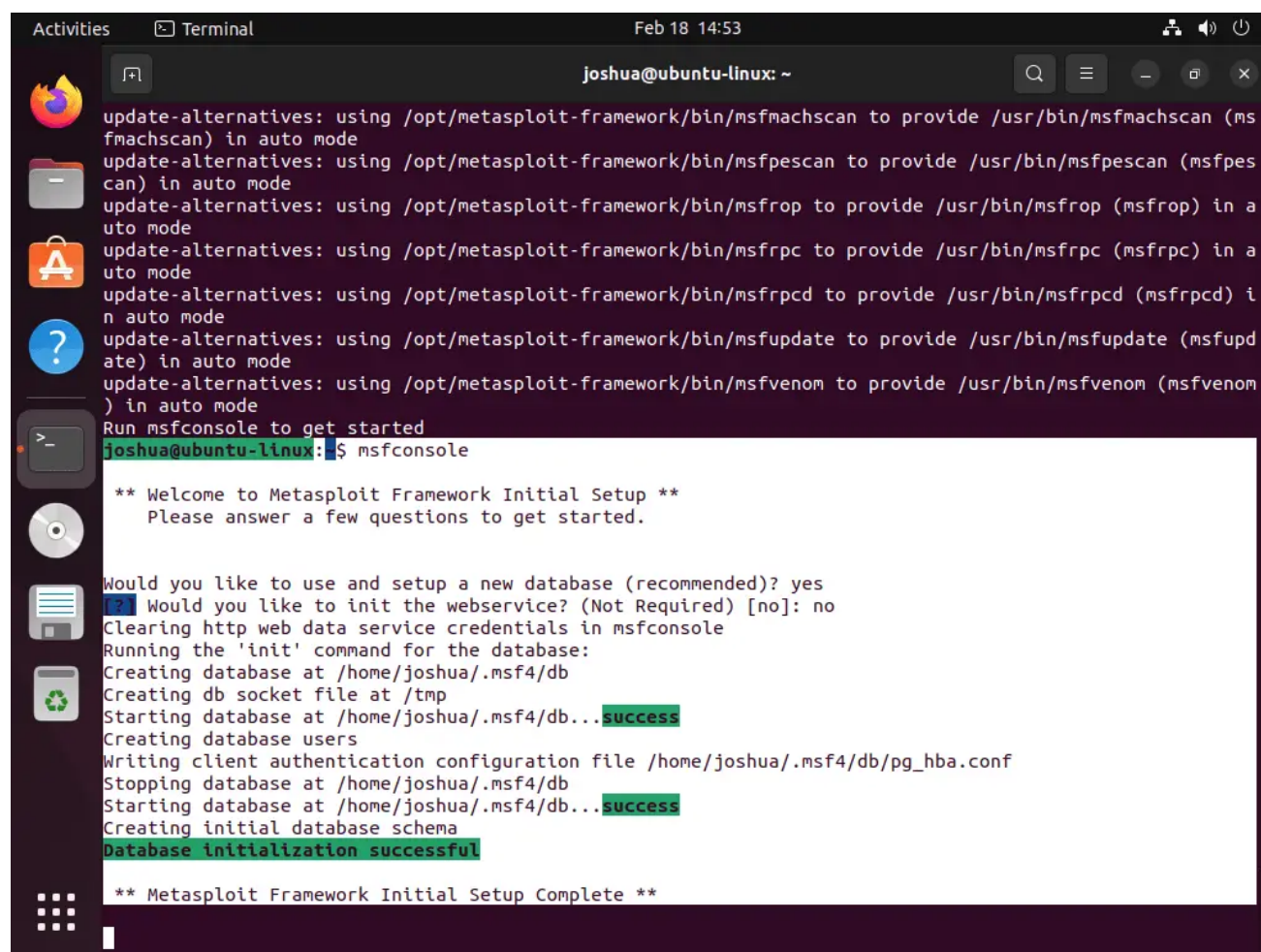
Setting up a new database: During the setup process, you may be prompted to set up a new database for the Metasploit Framework. Setting up a new database is recommended, and you can do so by typing “yes” when prompted.

```
Would you like to use and setup a new database  
(recommended)?
```

Initializing the web service: You may be prompted to initialize the web service during setup. This is not required, and the default response is “no.” However, if you want to enable the web service, type “yes” when prompted.

```
[?] Would you like to init the webservice? (Not Required)
[no]:
```

Final configurations: After you have completed the prompts, you will need to wait for a minute or two while the final configurations are taking place. You may see a terminal screen that provides information on the configuration process, and it may be similar to the following:

A screenshot of a terminal window titled "Terminal" with the username "joshua@ubuntu-linux" and the time "Feb 18 14:53". The terminal shows the output of the "msfconsole" command, which initiates the Metasploit Framework initial setup. The setup process includes updating alternatives for various tools (msfmachscan, msfpescan, msfrpc, msfrpcd, msfupdate, msfvenom) and then running the "msfconsole" command. The setup prompts the user to use and setup a new database (recommended) and to init the webservice (not required). The user answers "yes" to the database prompt and "no" to the webservice prompt. The setup then proceeds to create the database, create database users, write the client authentication configuration file, stop the database, start the database, and create the initial database schema. The setup is successful, and the terminal displays "Database initialization successful" and "** Metasploit Framework Initial Setup Complete **".

```
update-alternatives: using /opt/metasploit-framework/bin/msfmachscan to provide /usr/bin/msfmachscan (msfmachscan) in auto mode
update-alternatives: using /opt/metasploit-framework/bin/msfpescan to provide /usr/bin/msfpescan (msfpescan) in auto mode
update-alternatives: using /opt/metasploit-framework/bin/msfrpc to provide /usr/bin/msfrpc (msfrpc) in auto mode
update-alternatives: using /opt/metasploit-framework/bin/msfrpcd to provide /usr/bin/msfrpcd (msfrpcd) in auto mode
update-alternatives: using /opt/metasploit-framework/bin/msfupdate to provide /usr/bin/msfupdate (msfupdate) in auto mode
update-alternatives: using /opt/metasploit-framework/bin/msfvenom to provide /usr/bin/msfvenom (msfvenom) in auto mode
Run msfconsole to get started
joshua@ubuntu-linux:~$ msfconsole

** Welcome to Metasploit Framework Initial Setup **
Please answer a few questions to get started.

Would you like to use and setup a new database (recommended)? yes
[?] Would you like to init the webservice? (Not Required) [no]: no
Clearing http web data service credentials in msfconsole
Running the 'init' command for the database:
Creating database at /home/joshua/.msf4/db
Creating db socket file at /tmp
Starting database at /home/joshua/.msf4/db...success
Creating database users
Writing client authentication configuration file /home/joshua/.msf4/db/pg_hba.conf
Stopping database at /home/joshua/.msf4/db
Starting database at /home/joshua/.msf4/db...success
Creating initial database schema
Database initialization successful

** Metasploit Framework Initial Setup Complete **
```

Once you have completed the first-time setup process, you will be ready to use the Metasploit Framework.


```

Activities  Terminal  Feb 18 14:54
joshua@ubuntu-linux: ~

Creating initial database schema
Database initialization successful

** Metasploit Framework Initial Setup Complete **

.:ok000kdc'      'cdk000ko:.
.x0000000000000c  c000000000000x.
:000000000000000k,  ,k00000000000000:
'000000000kkk00000: :0000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,o0000000o
d00000000.MMMMMM.c000000c.MMMMMM,00000000x
l00000000.MMMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMMM.MMMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000o0000000.MX'x00d.
,k0l'M.0000000000000.M'dok,
:kk;.00000000000000.;0k:
;k000000000000000k:
,x0000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.3.4-dev- ]
+ -- --=[ 2292 exploits - 1201 auxiliary - 409 post ]
+ -- --=[ 965 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Metasploit Framework Terminal Commands

In this section, the guide delves into the practical applications of using Metasploit Framework terminal commands to perform various tasks in different scenarios. A comprehensive table overview of all available commands will be provided at the end of this section.

Starting Metasploit Framework

To start Metasploit Framework, open a terminal window and enter the following command:

```
sudo msfconsole
```

This will start with Metasploit Framework, and you will see a banner with information about the version, the contributors, and some tips on how to use Metasploit Framework.

Updating Metasploit Framework

Metasploit Framework is constantly updated with new modules, features, and bug fixes. To update Metasploit Framework, enter the following command in the terminal:

```
sudo msfupdate
```

This will update the Metasploit Framework to the latest version available.

Searching for Exploits

One of the main features of Metasploit Framework is the ability to search for exploits. To search for exploits, enter the following command in the terminal:

```
search <search-term>
```

Replace <search-term> with a keyword or phrase related to the exploit you are looking for. For example, if you want to search for exploits related to the Apache Struts vulnerability, you can enter the following:

```
search struts
```

This will display a list of all the available exploits related to the Apache Struts vulnerability.

Using Exploits

Once you have found an exploit that you want to use, you can use the following command to load the exploit module:

```
use <exploit-name>
```


Replace <exploit-name> with the name of the exploit module. For example, if you want to use the Apache Struts exploit module, you can enter the following:

```
use exploit/windows/http/struts2_rest_xstream
```

This will load the exploit module and display information about the module, such as the name, the author, the target platform, and the payload.

Configuring Exploit Options

Before running an exploit, you may need to configure some options, such as the target IP address, the target port, and the payload to use. You can view the options for an exploit by entering the following command:

```
show options
```

This will display a list of all the available options for the exploit module and their current values.

To set an option to a specific value, use the following command:

```
set <option-name> <value>
```

Replace <option-name> with the name of the option and <value> with the value you want to set it to. For example, if you're going to set the RHOST option to the IP address of the target system, you can enter the following:

```
set RHOST 192.168.1.100
```

Running Exploits

Once you have configured the options for an exploit, you can run the exploit using the following command:

```
exploit
```

This will run the exploit and attempt to exploit the target system. If the exploit is successful, you will see a message indicating that the exploit has been completed and that you have a session.

Using Meterpreter

Meterpreter is a powerful post-exploitation tool that allows you to interact with the compromised system in real time. To use Meterpreter, you first need to have a session. To view the available sessions, enter the following command:

```
sessions -l
```

This will display a list of all available sessions and their ID numbers.

To interact with a specific session, use the following command:

```
sessions -i <session-id>
```

Replace <session-id> with the ID number of the session you want to interact with. For example, if you're going to interact with session 1, you can enter the following:

```
sessions -i 1
```

This will start a Meterpreter shell for the selected session. From the Meterpreter shell, you can run various commands to perform actions on the compromised system.

Gathering System Information

One of the first things you may want to do when you have a Meterpreter session is to gather information about the compromised system. You can do this using

the following commands:

```
sysinfo
```

This will display information about the system, such as the operating system version, the CPU type, and the system architecture.

```
getuid
```

This will display the current user ID on the system.

```
getprivs
```

This will display a list of the current user's privileges on the system.

Uploading and Downloading Files

Meterpreter also allows you to upload and download files to and from the compromised system. To upload a file, use the following command:

```
upload <local-file> <remote-file>
```

Replace <local-file> with the path to the local file you want to upload and <remote-file> with the path to the file on the compromised system.

For example, if you want to upload a file called passwords.txt to the C:\Temp directory on the compromised system, you can enter the following:

```
upload /path/to/passwords.txt C:\Temp\passwords.txt
```

To download a file from the compromised system, use the following command:

```
download <remote-file> <local-file>
```

Replace <remote-file> with the path to the file on the compromised system and <local-file> with the path to the local file.

For example, if you want to download a file called passwords.txt from the C:\Temp directory on the compromised system to your local Downloads directory, you can enter the following:

```
download C:\Temp\passwords.txt /path/to/Downloads/passwords.txt
```

Using Metasploit to Exploit Known WordPress Vulnerabilities

WordPress is a widely used content management system (CMS) that powers millions of websites worldwide. Due to its widespread use, WordPress is a common target for hackers looking for potential vulnerabilities. However, with Metasploit, you can use its powerful tools to test your WordPress websites for any known vulnerabilities. It is important to remember that using Metasploit to exploit other websites or systems is illegal and unethical.

Now here's an example of how to use Metasploit to exploit a known vulnerability in WordPress:

Use the search command to find modules related to WordPress vulnerabilities:

```
search type:exploit platform:php app:wordpress
```

This command will return a list of Metasploit modules that can be used to exploit vulnerabilities in WordPress.

Choose a module to use, and configure any necessary options. For example, to exploit the WordPress TimThumb plugin vulnerability, you can use the following module:

```
use exploit/multi/http/timthumb_file_upload
```

Once you have selected the module, you can use the options command to configure any required options. For example, you may need to specify the target host and port and the path to the WordPress installation.

Run the exploit to exploit the vulnerability. For example, to run the TimThumb exploit, you can use the following command:

```
exploit
```

This will run the exploit and attempt to upload a shell to the target system.

Use the Meterpreter payload to gain access to the target system. If the exploit is successful, you can view any active Meterpreter sessions using the session command. You can then use the session command to connect to the session and gain access to the target system.

```
sessions  
session 1
```

Use the Meterpreter shell to gather information or perform actions on the target system. Once you have gained access to the target system, you can use the Meterpreter shell to perform various tasks. For example, you can use the upload command to upload files to the target system or the download command to download files from the target system.

```
upload /path/to/local/file /path/to/remote/file  
download /path/to/remote/file /path/to/local/file
```

Metasploit Commands Table List

While this guide briefly demonstrates using Metasploit commands, it is important to note that the commands listed here represent only a tiny fraction of what can

be achieved with the framework. The guide will present a table of the most commonly used commands to provide a more comprehensive overview.

Exploit Commands

Exploit commands are used to exploit vulnerabilities in a target system.

Command	Description
search	Search for a specific exploit or payload.
use	Select an exploit or payload to use.
show options	Show the current options for an exploit or payload.
set	Set the value of an option.
exploit	Execute the selected exploit.
sessions	Manage Meterpreter sessions.
back	Exit the current exploit or payload.

Auxiliary Commands

Auxiliary commands perform various tasks such as scanning, fuzzing, and information gathering.

Command	Description
search	Search for a specific auxiliary module.
use	Select an auxiliary module to use.
show options	Show the current options for an auxiliary module.
set	Set the value of an option.
run	Execute the selected auxiliary module.

Command	Description
back	Exit the current auxiliary module.

Post-Exploitation Commands

Post-exploitation commands perform various tasks after gaining access to a system.

Command	Description
sysinfo	Display system information.
getuid	Display the current user ID.
getprivs	Display the current user's privileges.
shell	Drop into a system shell.
ps	List running processes.
migrate	Migrate to another process.
download	Download a file from the target system.
upload	Upload a file to the target system.

Database Commands

Database commands are used to interact with the Metasploit Framework database.

Command	Description
db_status	Check the status of the database.
db_rebuild_cache	Rebuild the cache.
db_nmap	Import a nmap scan into the database.

Command	Description
hosts	List all hosts in the database.
services	List all services in the database.
vulns	List all vulnerabilities in the database.

Module Management Commands

Module management commands are used to manage modules in Metasploit Framework.

Command	Description
load	Load a module into the console.
reload_all	Reload all modules.
unload	Unload a module from the console.
info	Display information about a module.
edit	Edit a module.

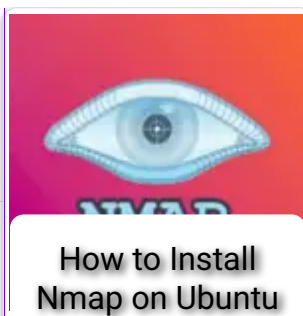
Conclusion

This guide has shown how to install Metasploit through the command line interface by importing the GPG key and repository with CLI commands, then installing Metasploit using the terminal and configuring the necessary steps. We have also explored some of the most commonly used Metasploit terminal commands, organized by their functions, such as searching for vulnerabilities, managing modules, interacting with the Metasploit Framework database, and performing various tasks after gaining access to a system.

You may also like:



How to Install
ModSecurity, Nginx,
OWASP CRS with



How to Install
Nmap on Ubuntu



How to Install
WordPress with
Nginx, MariaDB



How to Install
Jellyfin Media
Server on Ubuntu

Recent Posts



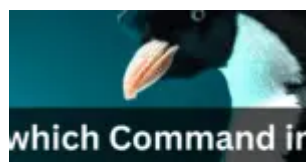
How to Install Ungoogled Chromium on Ubuntu 22.04 or 20.04



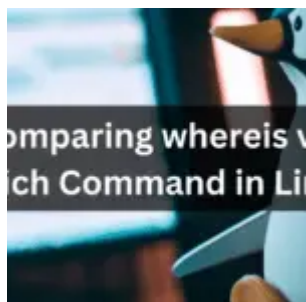
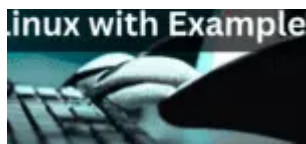
Linux Kernel 6.5: Deep Dive into Features & Enhancements



How to Check System Reboot History in Linux



which Command in Linux with Examples



Comparing whereis vs. which Command in Linux



If you have any legitimate inquiries, such as article suggestions, don't hesitate to contact LinuxCapable. Kindly ensure that your message is written in the English language.

CONTACT US

This website uses the services of Ezoic Inc. ("Ezoic"). Ezoic's privacy policy is [here](#). Ezoic may employ various technologies on this website, including displaying advertisements and enabling advertising to visitors. For additional information about Ezoic's advertising partners, please see Ezoic's Advertising Partner Page [here](#).

© 2023 LinuxCapable. All rights reserved.

[About Us](#)

[Copyright Policy](#)

[Disclaimer](#)

[Privacy Policy](#)

[Terms & Conditions](#)