Applied Cyber Security Industry Led-Course

Instructor: XYZ

Lab Instructor: Moeez Javed

Lab 1: Overview of Ethical Hacking & Installation of Kali Linux in a Virtual Machine and its configurations

Availability:
Monday to Friday: 9 AM – 5 PM (at CUST)
After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

Phone: +92 333 8744696
Email: moeezjavedmj@gmail.com

Overview of the Lab's:

Week 1: Set up a penetration testing lab by installation of kali linux in virtual machine, understand ethical hacking concepts, and update kali linux .

Week 2: Perform reconnaissance, network scanning, vulnerability assessment, and basic exploitation.

Week 3: Explore web security, OWASP Top 10 vulnerabilities, and exploit web application flaws.

Week 4: Learn and practice SQL Injection, Command Injection, and LDAP Injection techniques.

Week 5: Understand authentication flaws, session hijacking, and execute social engineering attacks.

Week 6: Dive into Cross-Site Scripting (XSS) and insecure deserialization vulnerabilities.

Week 7: Secure APIs, identify misconfigurations, and exploit weak API implementations.

Week 8: Perform privilege escalation, post-exploitation, and anti-forensics techniques.

Week 9: Conduct wireless attacks, crack Wi-Fi security, and apply mitigation strategies.

Week 10: Study cryptography, hashing techniques, and break weak encryption methods.

Week 11: Automate penetration testing tasks using scripting and exploit development.

Week 12: Analyze and secure mobile applications, focusing on Android and iOS vulnerabilities.

Week 13: Conduct Android penetration testing, malware analysis, and reverse engineering.

Week 14: Perform iOS penetration testing, exploit vulnerabilities, and analyze malware.

Week 15: Write professional pentesting reports and prepare for Capture The Flag (CTF).

Week 16: Participate in a final CTF project, document findings, and complete the program.

Lab Objectives

Download and Configure Kali Linux

Understand the process of downloading Kali Linux from the official website.

Identify the appropriate system requirements for installation.

Install Kali Linux on a virtual machine using VirtualBox or VMware.

Setting Up a Virtual Machine

Create and configure a VirtualBox instance for Kali Linux.

Allocate appropriate hardware resources (RAM, CPU, and disk space).

Configure essential VM settings like network adapters and shared clipboard options.

Installing Kali Linux

Perform a step-by-step installation of Kali Linux using the graphical installer.

Configure system hostname, user accounts, and passwords.

Partition the hard disk and install the GRUB bootloader.

Exploring the Kali Linux Environment

Familiarize yourself with key features of the Kali Linux desktop.

Learn about the Application Menu, File Manager, Terminal, and System Options.

Set up a network connection and manage multiple virtual desktops.

Updating and Securing Kali Linux

Update Kali Linux packages and repositories using the terminal.

Set up a firewall using UFW (Uncomplicated Firewall) for enhanced security. Enable SSH service for secure remote access.

Introduction to Kali Linux

Kali Linux is a Debian-based operating system specifically designed for cybersecurity professionals, ethical hackers, and penetration testers. Developed and maintained by Offensive Security, Kali Linux provides a comprehensive suite of tools for security assessments, digital forensics, and network analysis.

Unlike traditional operating systems, which prioritize user experience and general-purpose computing, Kali Linux is built with security in mind. It offers a lightweight, customizable, and highly secure environment tailored for ethical hacking and penetration testing. With its vast array of pre-installed tools and robust security features, Kali Linux remains the go-to choice for cybersecurity professionals worldwide.

Why Kali Linux is Best for Ethical Hacking

Pre-Installed Penetration Testing Tools

Kali Linux comes with 600+ pre-installed security tools for penetration testing, vulnerability assessment, and digital forensics. These include industry-standard tools like:

Metasploit (for exploit development)

Nmap (for network scanning)

Wireshark (for network packet analysis)

Aircrack-ng (for wireless network security testing)

John the Ripper (for password cracking)

Having these tools pre-installed saves valuable time compared to manually setting them up on other operating systems, allowing cybersecurity professionals to focus on security assessments.

Regular Updates and Community Support

Kali Linux is actively maintained by Offensive Security, ensuring it receives frequent updates with the latest security tools, exploits, and bug fixes. This keeps ethical hackers ahead of cyber threats.

Additionally, Kali Linux has a large and active community, providing extensive documentation, troubleshooting guides, and forum discussions. This strong community support helps both beginners and experts stay updated and resolve issues efficiently.

Lightweight and Customizable

Kali Linux is designed to be lightweight and highly adaptable, making it suitable for various hardware configurations. It can be installed on:

Virtual Machines (VMs) for sandboxed testing

USB drives for live testing without installation

Users can also choose different desktop environments, including:

XFCE (lightweight and fast)

KDE and GNOME (modern UI options for better visuals)

This flexibility allows users to tailor their setup to their needs, ensuring efficient performance even on low-resource systems.

Strong Security and Privacy Features

Kali Linux is built with security in mind, offering features that enhance privacy and secure testing environments:

Root user privileges (in earlier versions) for direct access to system resources

Anonymous mode to mask identity and browsing history

Metasploit framework for penetration testing and exploit development

Secure SSH access for remote operations with encrypted connections

These features make Kali Linux ideal for ethical hacking, allowing users to conduct security assessments while maintaining privacy and control.

Permission Grants and Flexibility

Kali Linux provides granular permission control, allowing users to execute privileged commands seamlessly using sudo. Unlike other operating systems that restrict access to certain security tools, Kali Linux allows:

Full system control for ethical hacking operations

Kernel-level security patches for better system protection

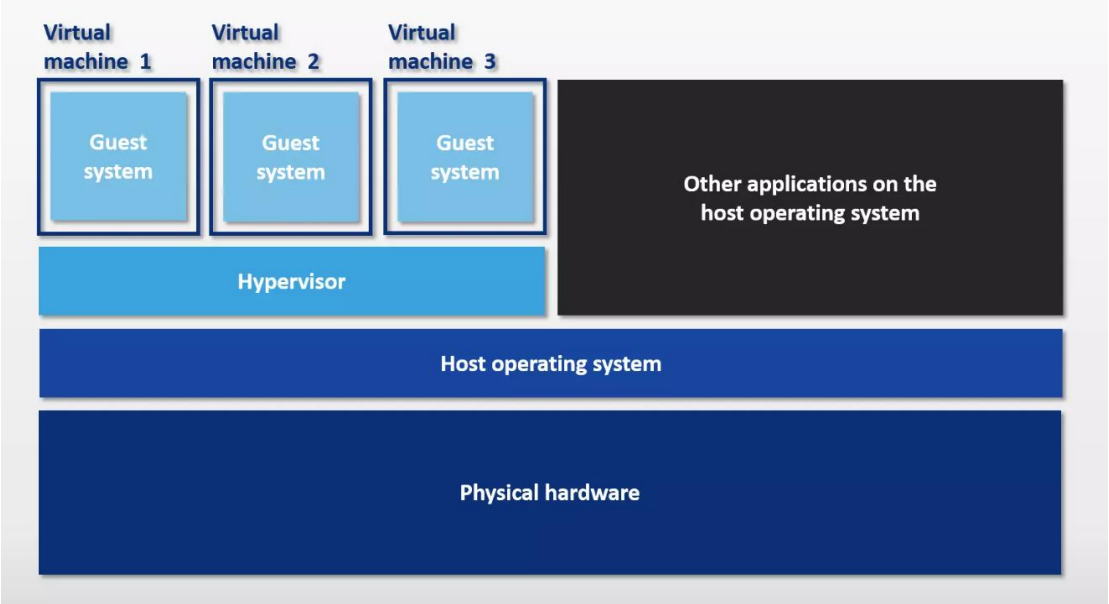
Custom security configurations to enhance penetration testing setups

This flexibility ensures ethical hackers can modify and execute commands without unnecessary restrictions, making security testing more efficient.

Open-Source and Free to Use

Kali Linux is completely open-source, meaning cybersecurity professionals can modify, contribute, and improve the system as needed. Unlike paid security tools, Kali Linux provides free access to its vast cybersecurity toolkit, allowing ethical hackers to perform advanced penetration testing without financial barriers.

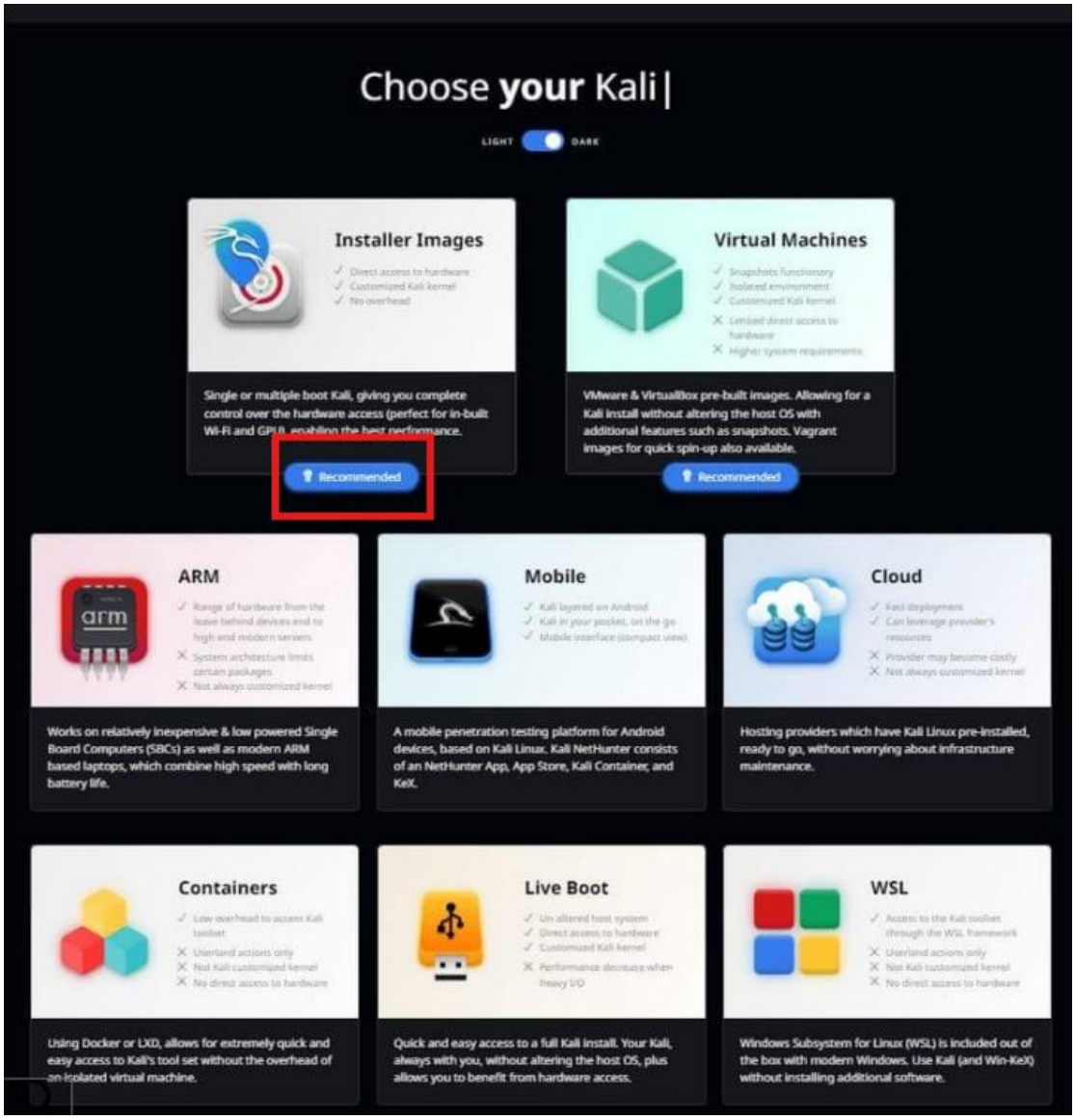
With its open-source nature, regular updates, and robust security tools, Kali Linux remains the most powerful and reliable operating system for ethical hacking and cybersecurity research.



Download Kali Linux

The first step is to visit the official Kali Linux website and navigate to the downloads page. You can choose the platform you want to install it on, such as virtual machines or a bootable USB drive.

This flexibility makes Kali accessible to many users with different hardware preferences and needs.



Before installing Kali Linux, you must meet the appropriate system requirements.

You should have:

- At least 2 GB of RAM, although we recommend 4 GB or more.
- At least 20 GB of free disk space.

How to Install Kali Linux

Now that you have downloaded Kali, decide where to install it. We have articles on installing Kali on VMware, VirtualBox and Raspberry Pi.

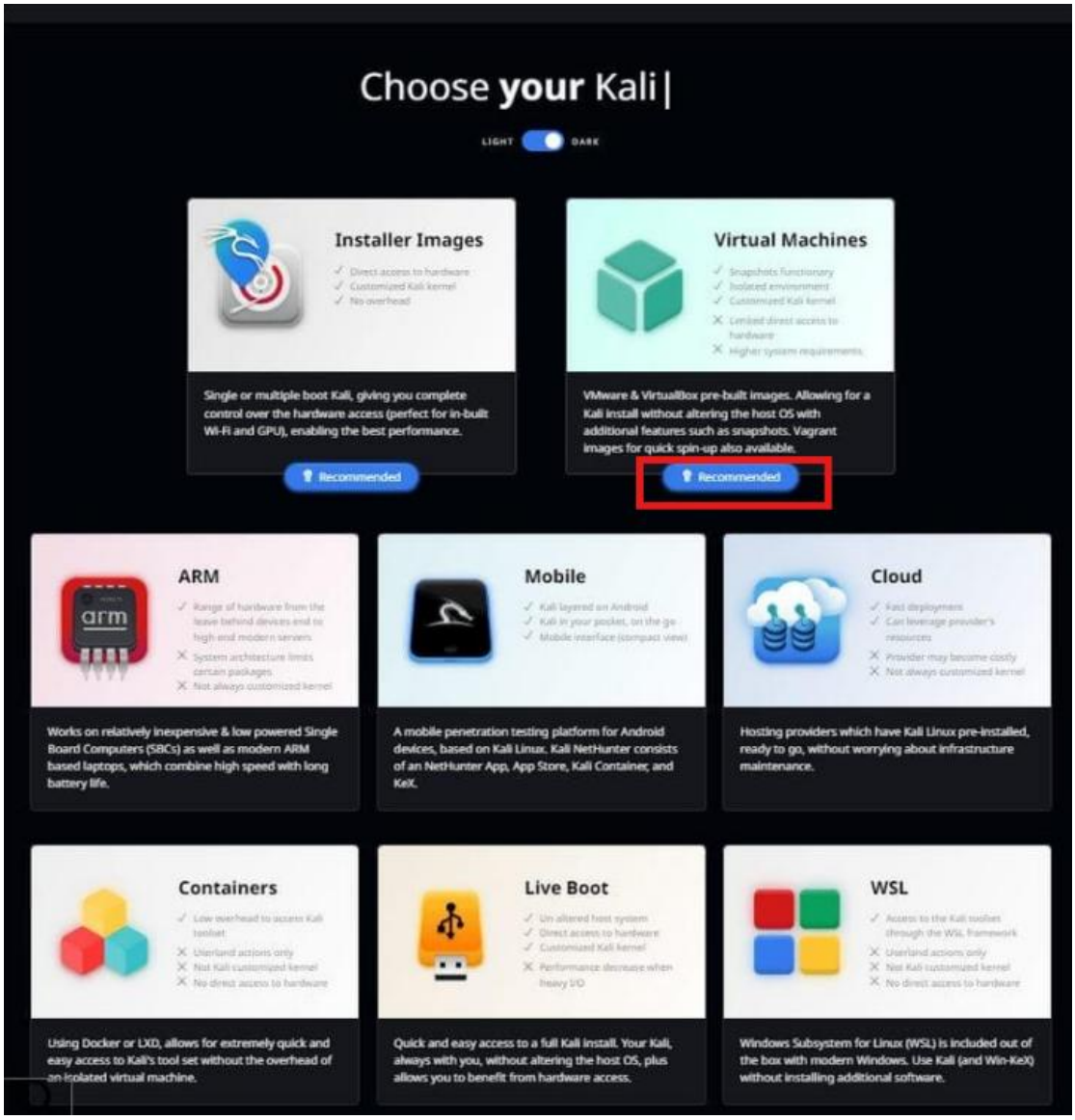
Step 1: Download Kali Linux ISO Image

Kali Linux offers ISO images for 32-bit, 64-bit, and ARM64 architectures. To download an ISO file:

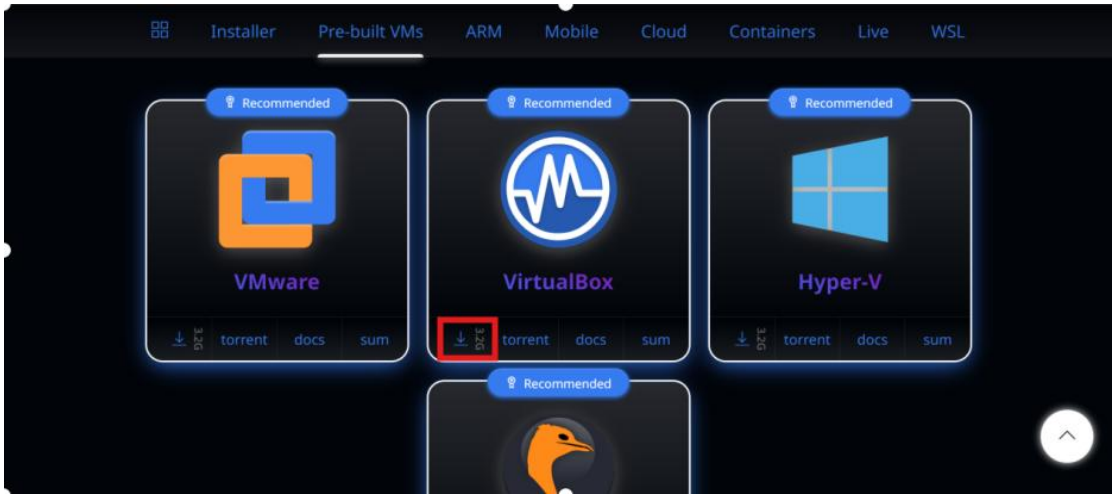
1. Visit the **installer section** of the Kali Linux official website.

2. Select the system architecture of the host OS and download the ISO file by clicking the button in the bottom-left corner of the installer card.

Or

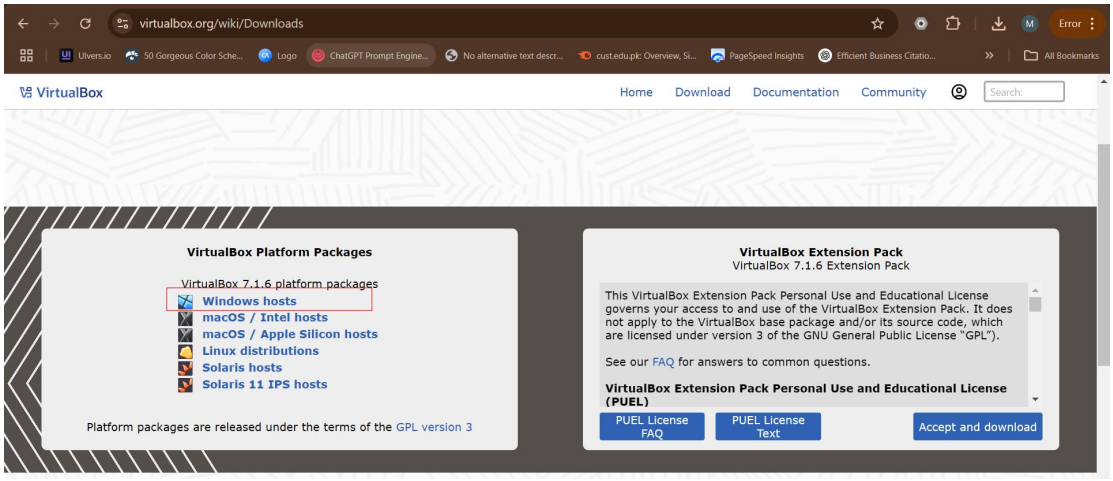


Download the software directly from the official VMware website. Then, choose either **VMware** or **VirtualBox** for installation; however, **VirtualBox** is the preferred option.



After download ISO File

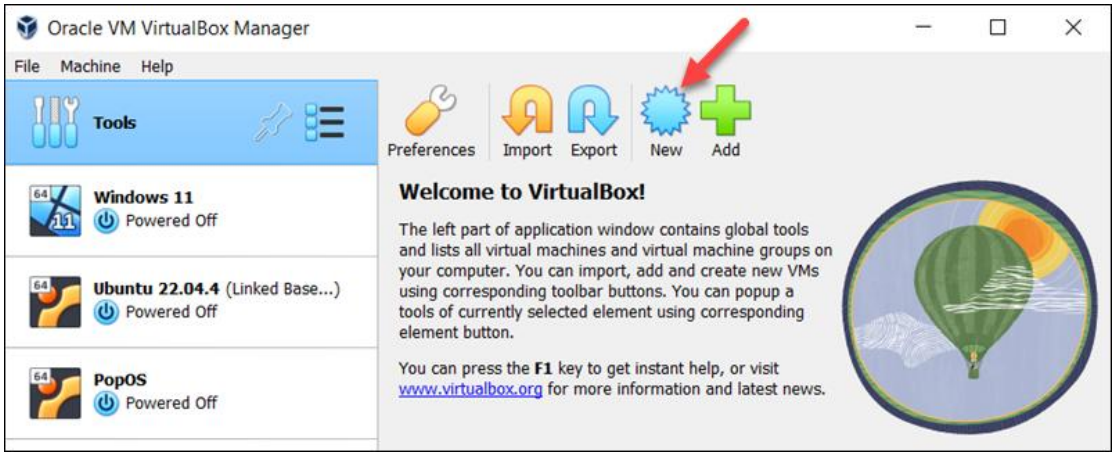
Than download virtual Box



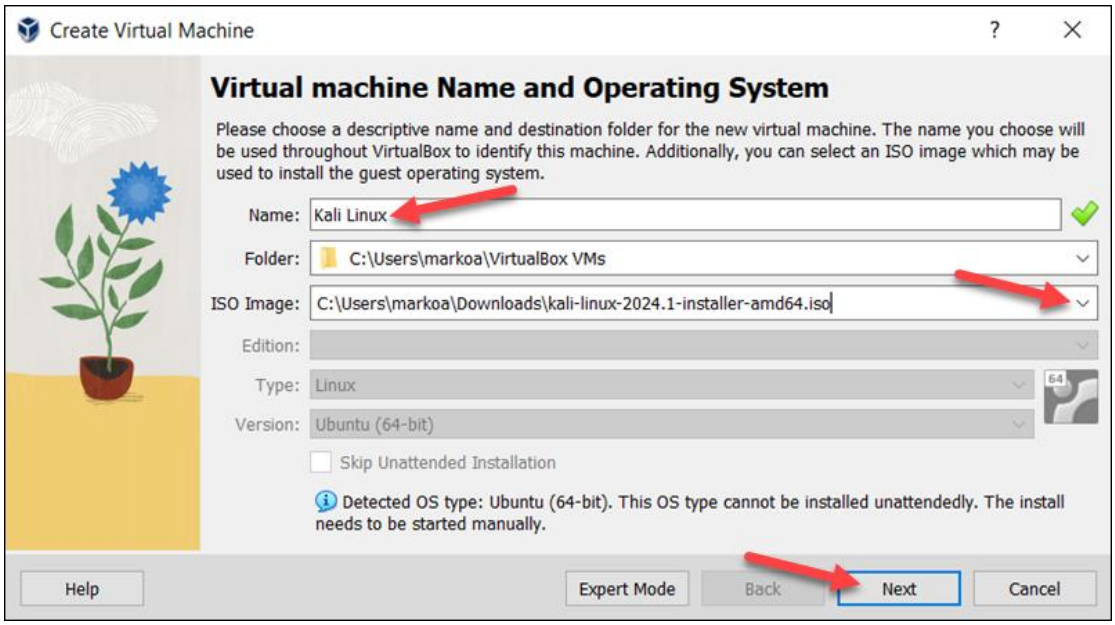
Step 2: Create Kali Linux VirtualBox Instance

Create a new virtual machine and configure it to run Kali Linux. Proceed with the steps below to correctly set up a Kali Linux VM in VirtualBox:

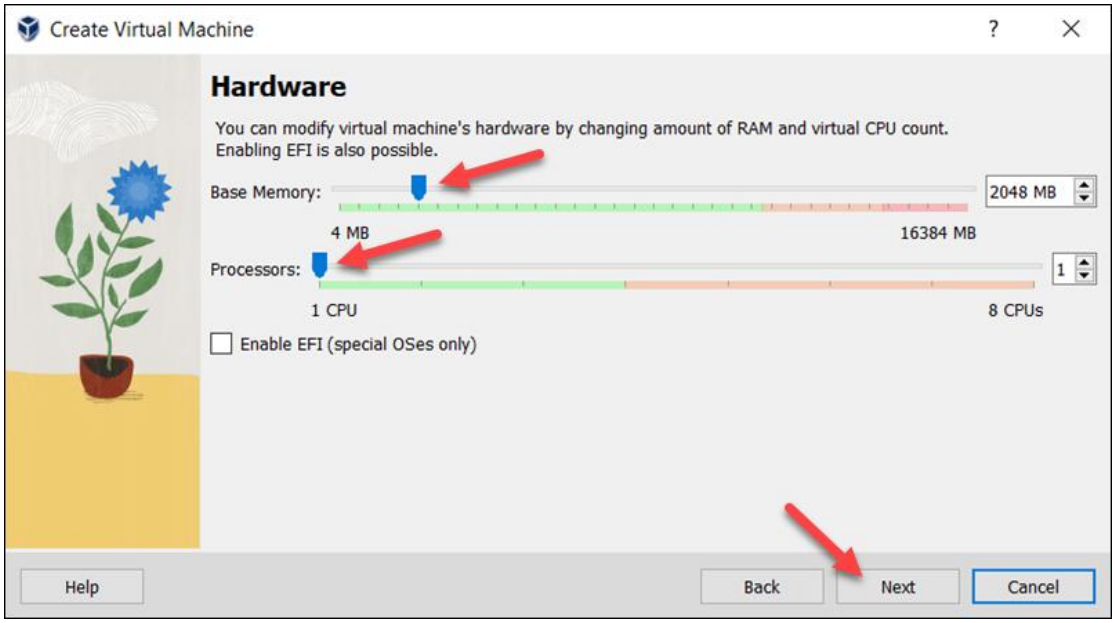
1. Launch **VirtualBox Manager** and click the **New** icon.



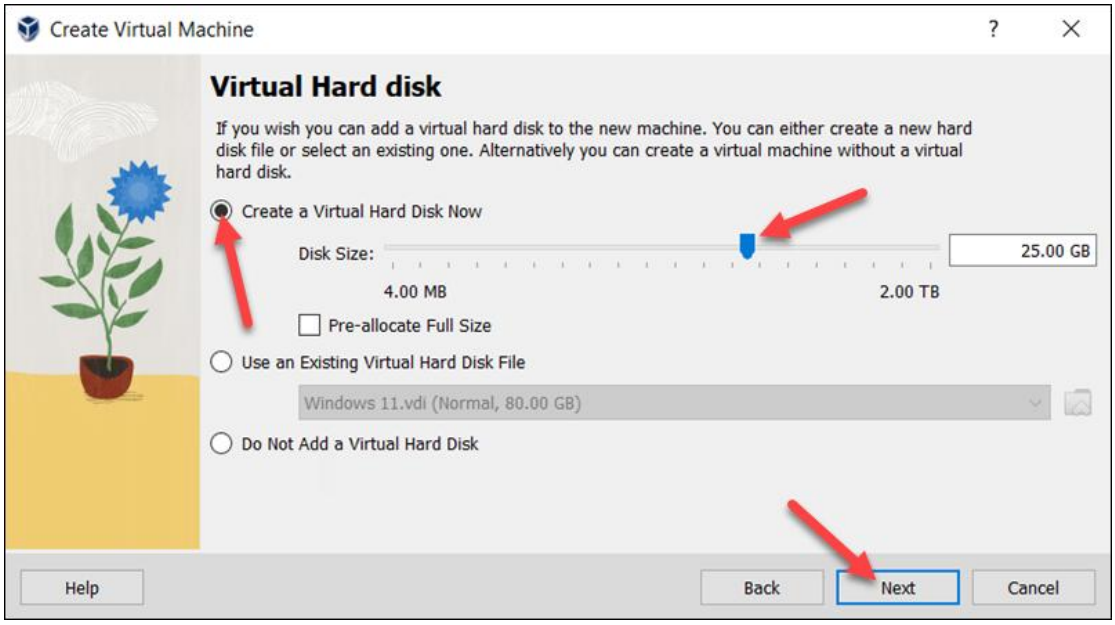
2. Specify a name for the VM and provide the path to the ISO image. Select **Next**.



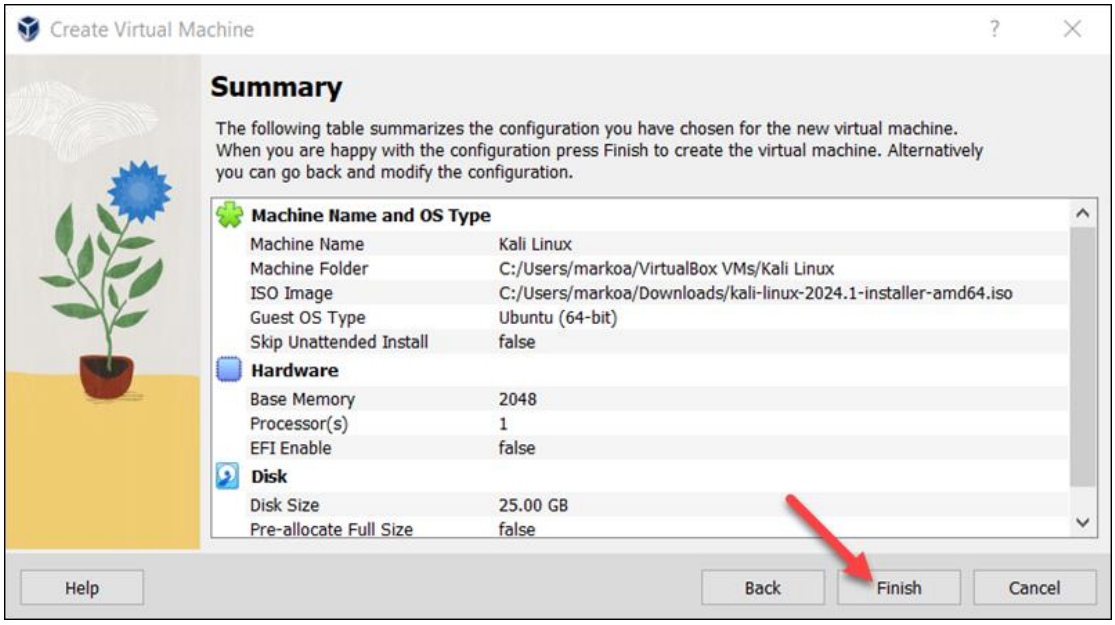
3. Select the amount of memory and the number of **virtual CPUs** to allocate to the VM. The minimum recommended values for Kali Linux are **2 GB of RAM** and **1 CPU**. Select **Next** when you finish setting up the VM hardware.



4. Create a virtual hard disk for the new VM. The recommended hard disk size is at least **25 GB**. Alternatively, you can use an existing virtual hard disk file or decide not to add one. Click **Next** to proceed to the next step.



5. Review the new VM setup on the **Summary** page. Select **Finish** to create the virtual machine.

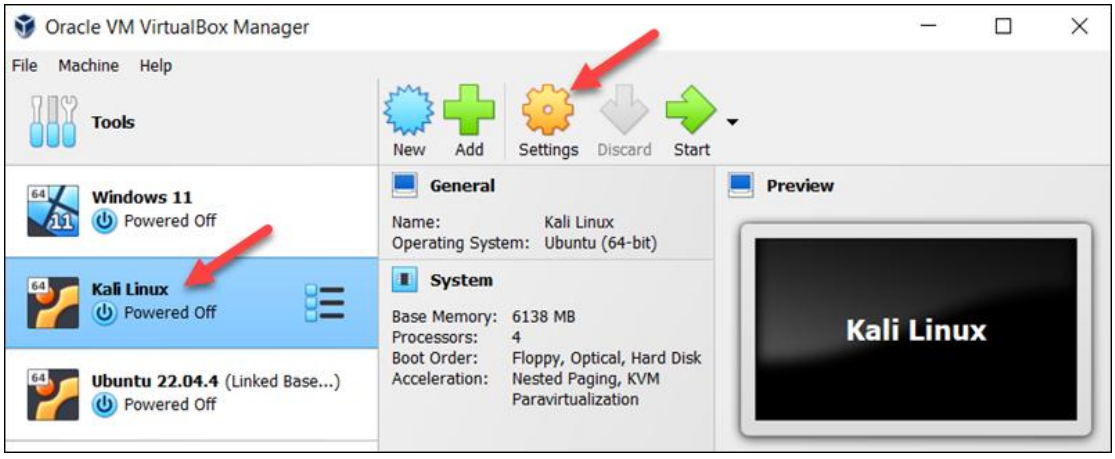


The VM appears on the list in VirtualBox Manager.

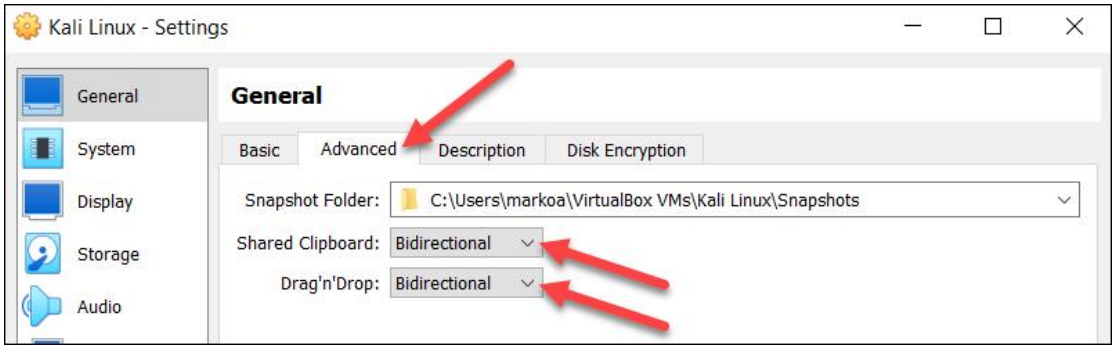
Step 3: Configure Virtual Machine Settings and Start VM

Before starting the VM and beginning the installation process, follow the steps below to perform additional adjustments on the VM:

1. Select the Kali Linux VM and click the **Settings icon**.

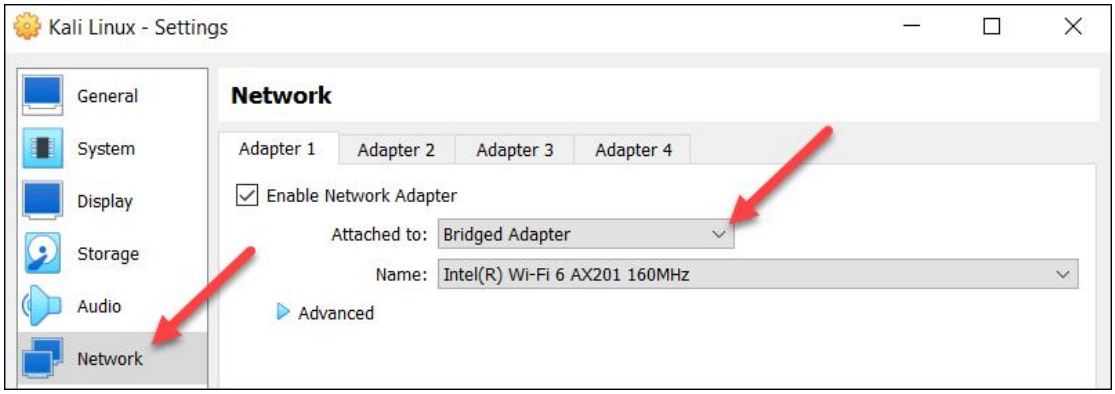


2. Select the **Advanced** tab in the **General** section and change the **Shared Clipboard** and **Drag'n'Drop** settings to **Bidirectional**. This feature allows the host and the guest machine to exchange files.

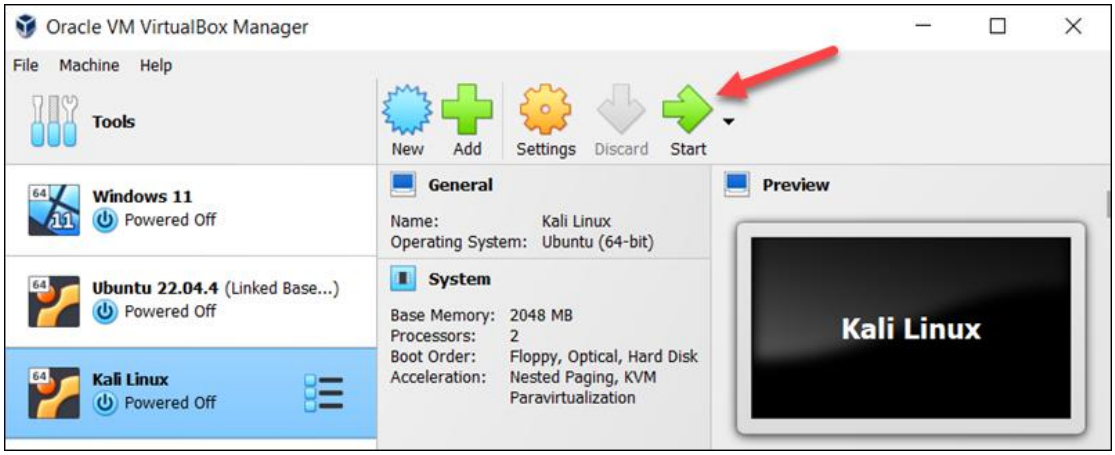


Warning: Connecting the host and VM clipboards breaks VM isolation. Use this option with caution.

3. Select **Network** from the menu on the left side. Change the **Attached to** field to **Bridged Adapter**. Select **OK** at the bottom of the window to return to the main window.



4. Click **Start** to begin installing Kali Linux.



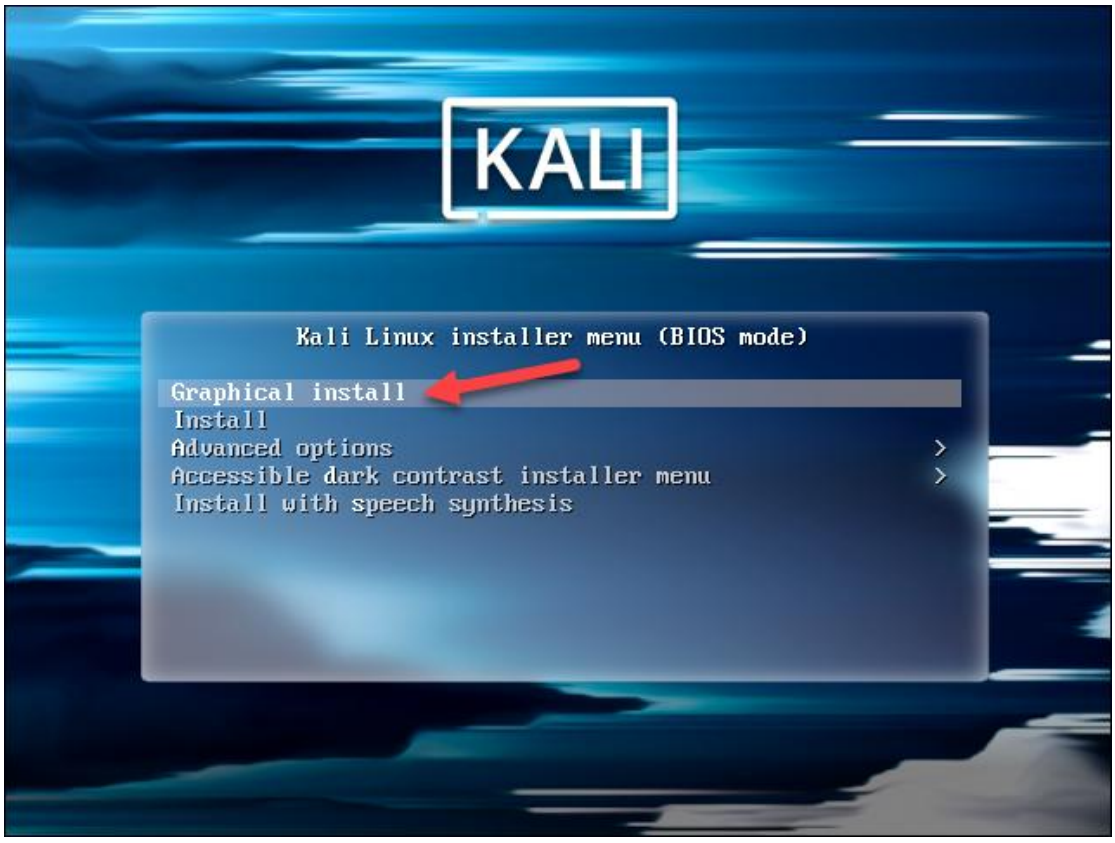
How to Install Kali Linux on VirtualBox

Kali Linux uses the Debian installer to set up the operating system. The sections below provide a detailed walkthrough of the installer and offer advice on configuring Kali Linux.

Step 1: Perform Initial Configuration

When the new VM is started, the Kali Linux installer menu appears. Start the installation procedure by following the steps below:

1. Select the **Graphical install** option.



2. Choose the system's **default language**, which will also be used during installation.

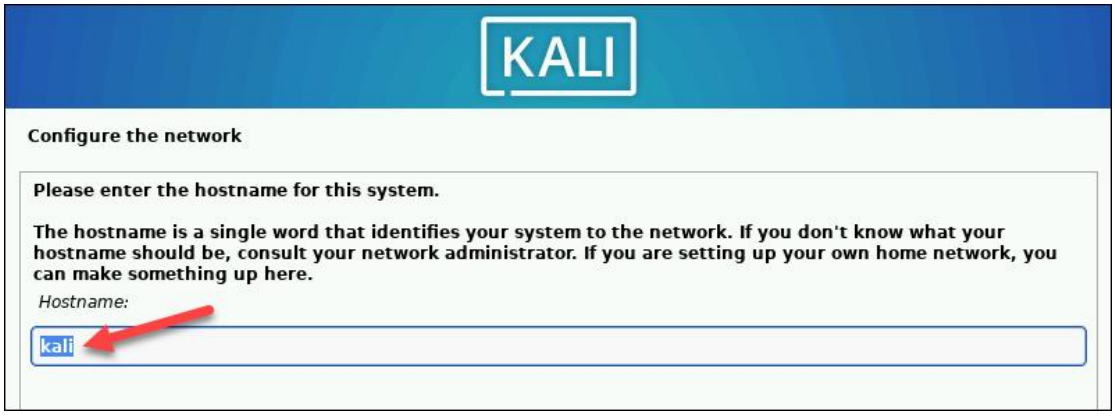
3. Find and select your **country** from the list, or choose **other**.

4. Decide which **keyboard mapping** to use.

Step 2: Configure Host, User, and Time Zone

The following installer steps set up the hostname and domain of the system and configure the user:

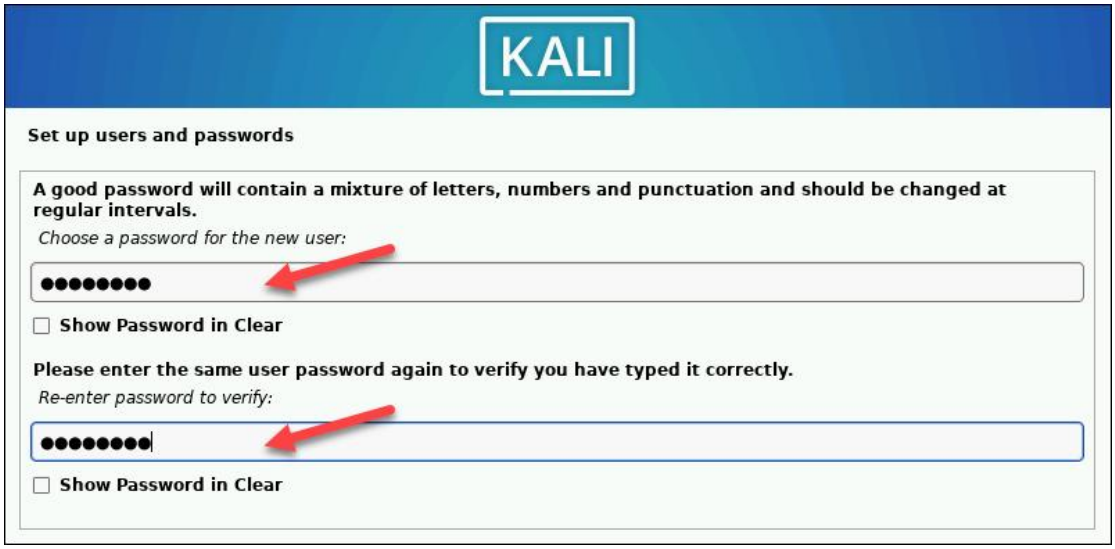
1. In the **Configure the network** section, enter a **system hostname**.



2. Empty the domain name

3. Create a **user account** by providing the user's full name and username.

4. Create a **strong password** for the user account.

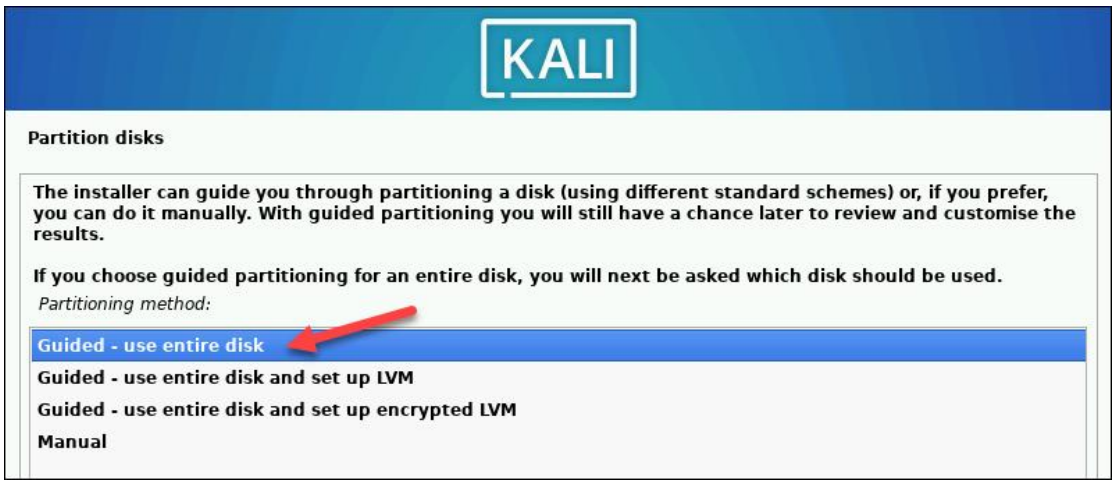


5. Select the correct **time zone** from the available options.

Step 3: Create Hard Disk Partitions

Proceed with the following steps to create a bootable partition on the virtual hard disk:

1. Select how to partition the hard disk. The default option is **Guided - use entire disk**.

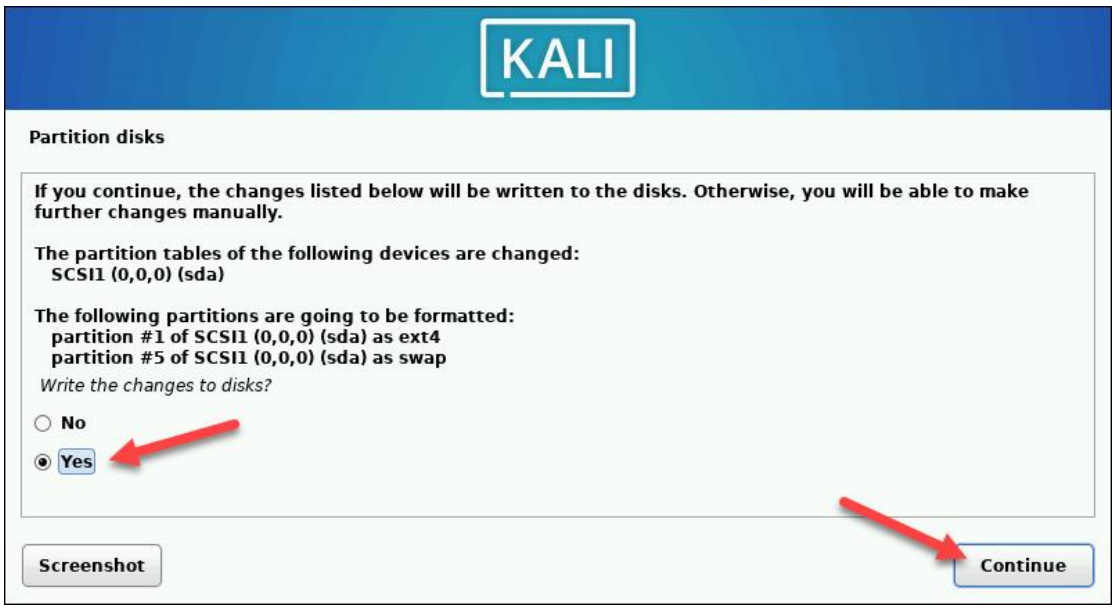


2. Select the disk you want to use for partitioning. The only available option is the disk created during the VM creation.

3. Select the **partitioning scheme**. The default option is **All files in one partition**.

4. The wizard provides an overview of the configured partitions. Ensure that the **Finish partitioning and write changes to disk** option is selected.

5. Confirm the choice by selecting **Yes** on the next screen.

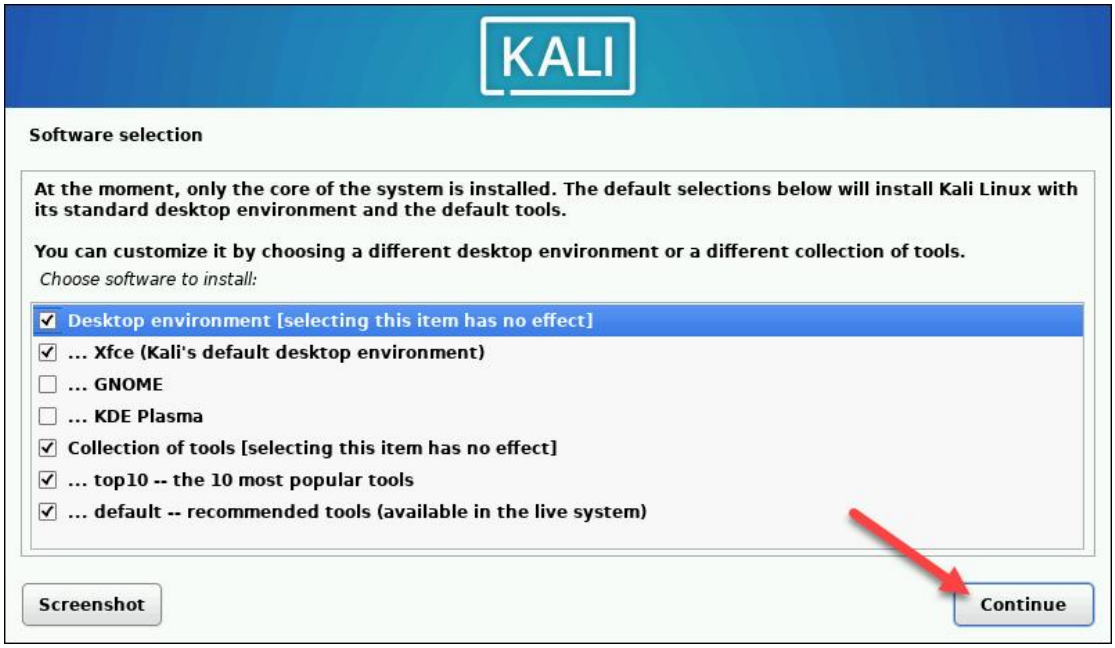


The wizard starts installing Kali.

Step 4: Customize Kali Linux Installation

After installing the system's core, Kali enables users to customize the OS further. Choose the components to install by executing the following steps:

1. Select the desktop environment and the tools you want, or click **Continue** to proceed with the default options.



2. Select whether you want to use a network mirror.

3. If you use an **HTTP proxy**, enter the necessary information. Otherwise, leave the field blank.

4. Install **the GRUB bootloader** on the hard disk. Select **Yes** and **Continue**.

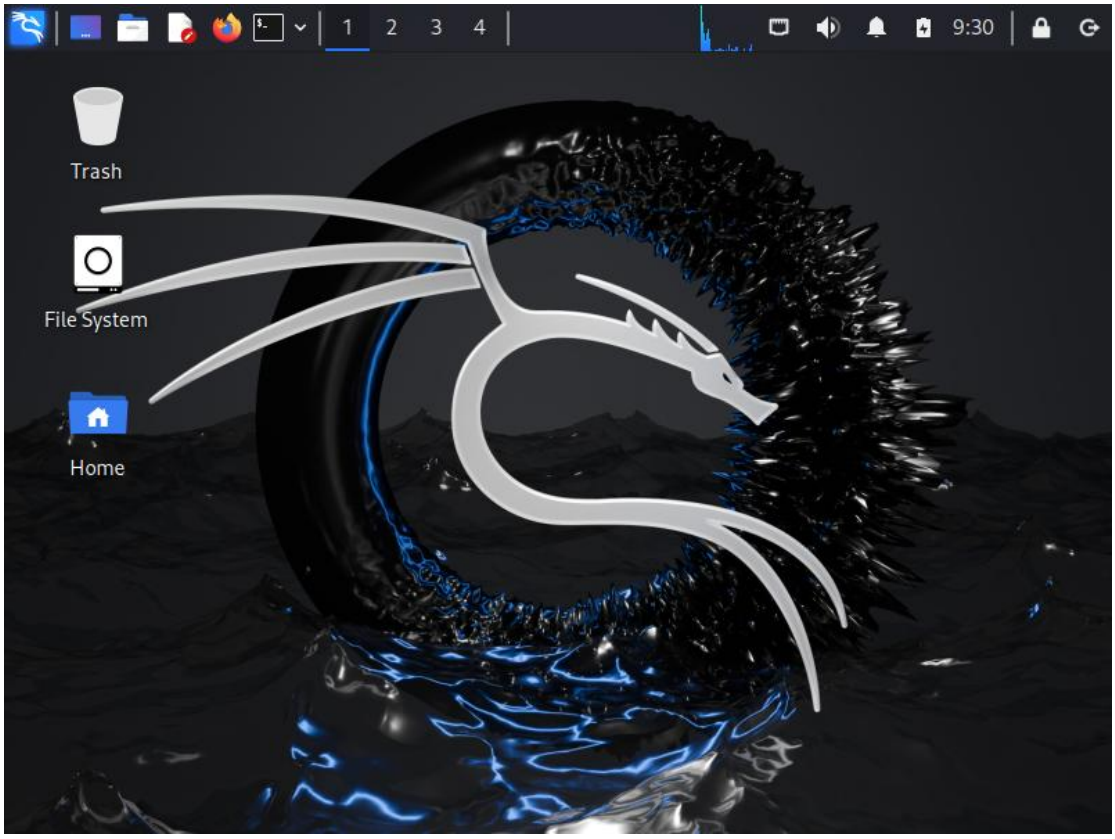
5. Select a bootloader device to ensure the newly installed system is bootable.

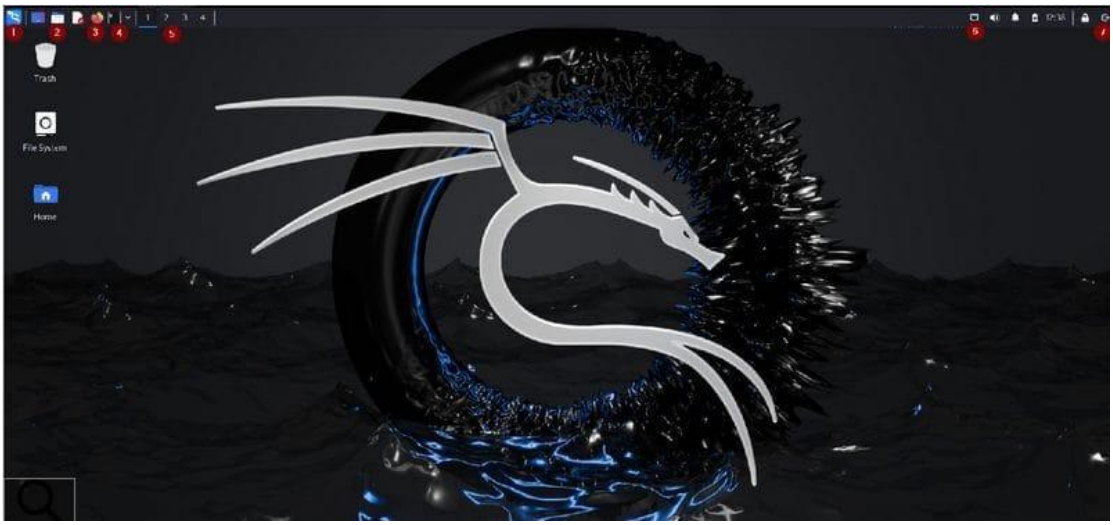
When Kali finishes installing, the Installation is complete message appears.

6. Click **Continue** to reboot your VM. After rebooting, the Kali login screen appears.

7. Enter the username and password created in the previous steps.

The Kali Linux desktop appears on the screen.





Here are some of the most important areas of the Kali desktop:

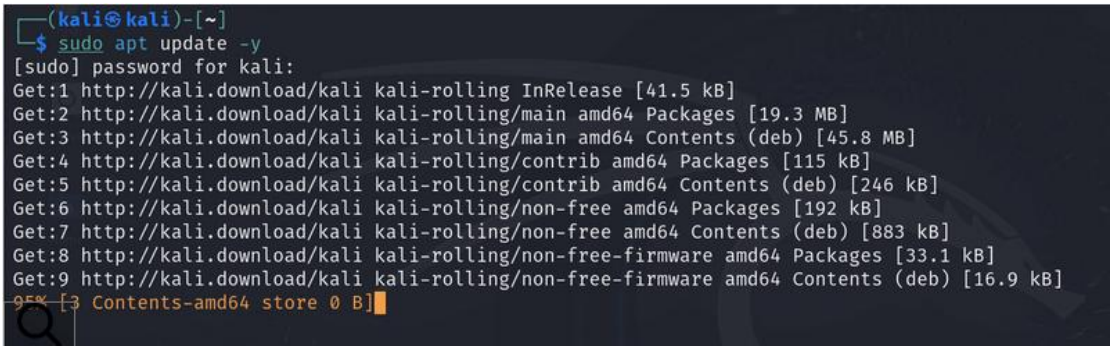
- **Application Menu:** Click here to access all available Kali Linux applications, system settings and utilities.
- **File Manager:** This icon opens the file manager, where you can browse and manage your system files and directories.
- **Web Browser:** This shortcut opens your default web browser, Firefox.
- **Terminal:** The terminal icon directs you to the command line to perform various system tasks and functions.
- **Workplace Selector:** This area allows you to switch between multiple virtual desktops or workspaces and organize your windows.
- **Network Connections:** It shows your current network status and allows you to manage your network connections.
- **System Options:** From here, you can log out, lock the screen, reboot or turn off the system.

How to Update Kali Linux

Before using Kali Linux — and every two to four weeks afterward — it's important to update your local package lists with the latest versions from the repositories, and then upgrade all installed packages, including tools, utilities, software, and security updates .

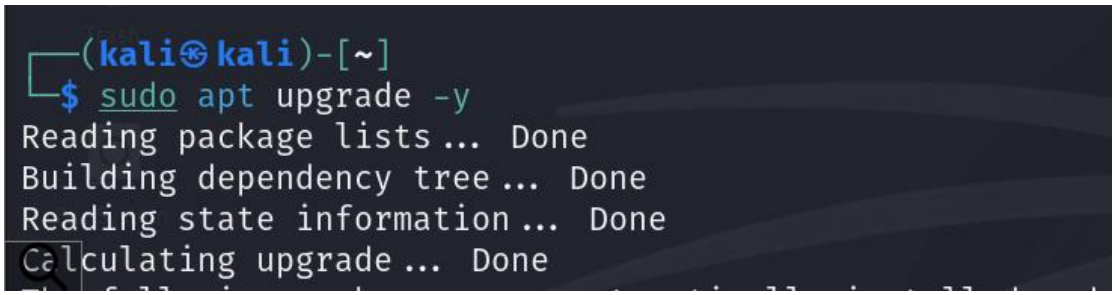
The first step is to update the repositories, and you can do this by opening a terminal and typing the command:

sudo apt update -y



Then, to perform the upgrade, use the command:

sudo apt upgrade -y



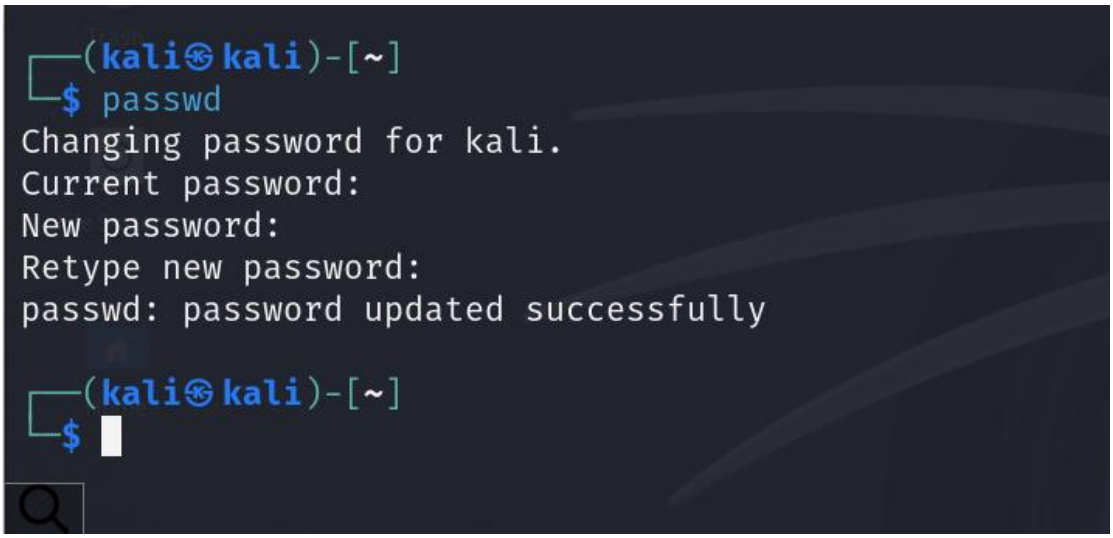
Basic Kali Setup

Now that everything is updated and ready, it's a good time to do some basic setup before using Kali. We will show you some important steps to follow.

Change Kali Password

You will want to change the default password for the "kali" user, which is also the password used to run commands as the root user.

To do this, open a terminal and type the command:



Firewall Setup in Kali

It is highly recommended that you set up a firewall when using Kali. Enabling a firewall is a fundamental security practice that helps prevent unauthorized access to your system. Firewall rules can be configured based on your specific usage requirements.

We will show you how to install and configure UFW (Uncomplicated Firewall) in Kali, which makes installing a firewall very easy.

Take yourself to the terminal and type the command:

sudo apt install ufw

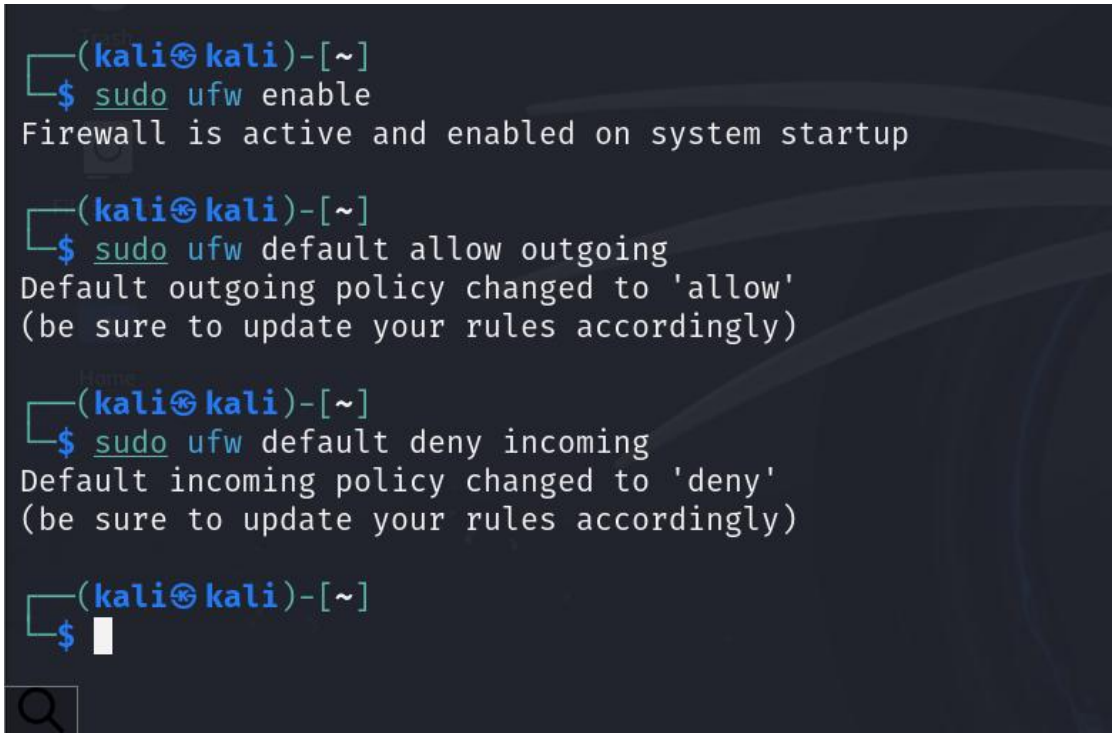
After the installation is complete, you can enable the firewall with the command:

sudo ufw enable

We recommend allowing all outgoing connections and denying all incoming connections to begin with. You can activate the necessary ports as required. To do this, type:

sudo ufw default allow outgoing

sudo ufw default deny incoming



Remember: You will need to open ports to catch reverse shells. This can be done with the command:

sudo ufw allow port/protocol

For example, to open TCP port 4444, use the command:

sudo ufw allow 4444/tcp

Opening ports can introduce security risks, so only open the ports you need and close them when they are no longer needed.

Enable SSH in Kali

You'll want to enable the SSH service if you need secure remote access to your Kali machine. This allows you to create encrypted command line connections over a network. We'll quickly walk you through the steps to enable SSH on your system.

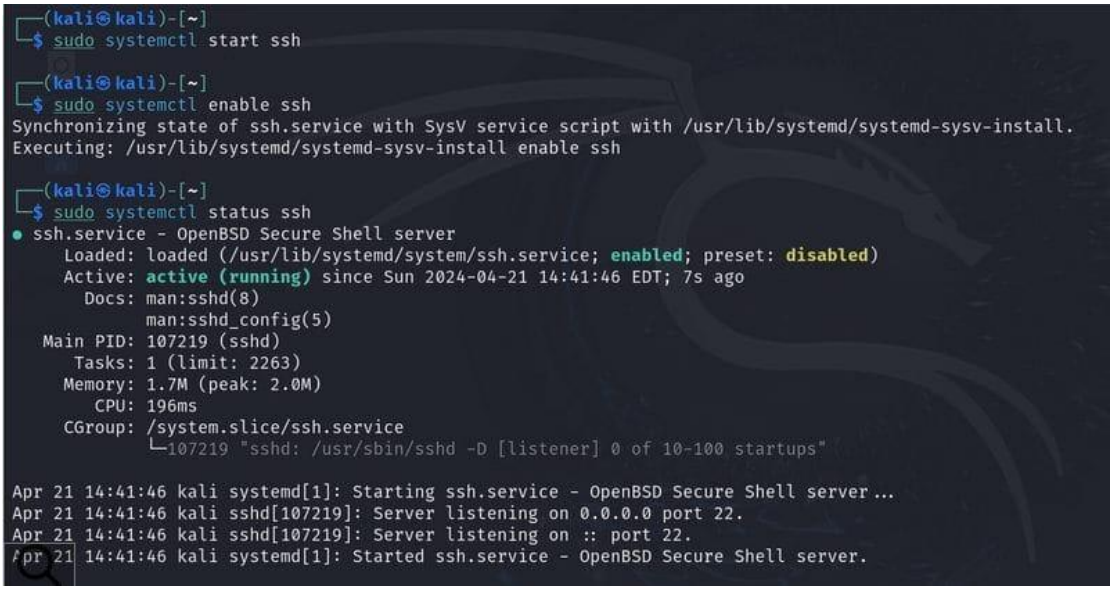
In the terminal, type the following commands:

sudo systemctl start ssh

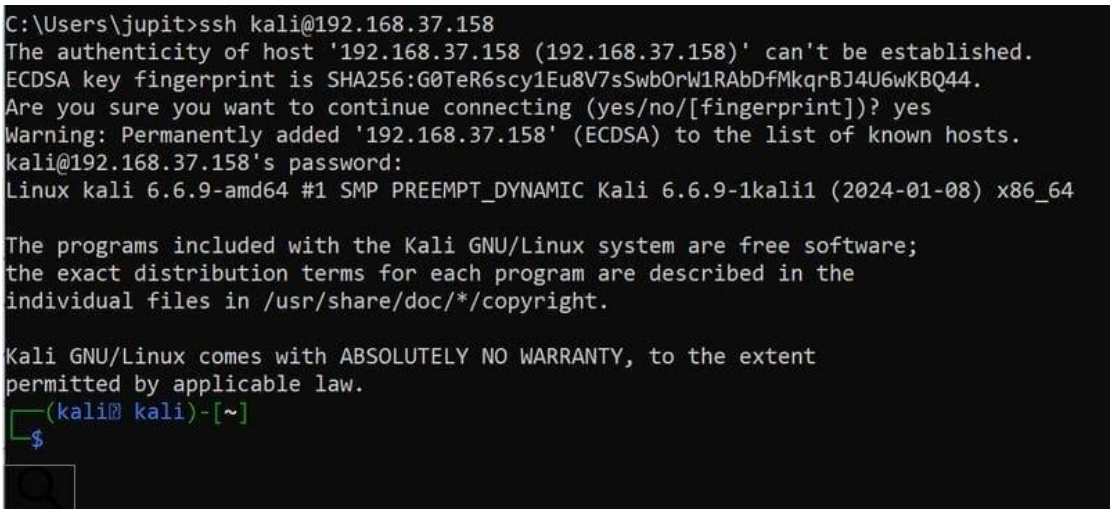
sudo systemctl enable ssh

Then, to confirm if SSH is running, type the command:

sudo systemctl status ssh



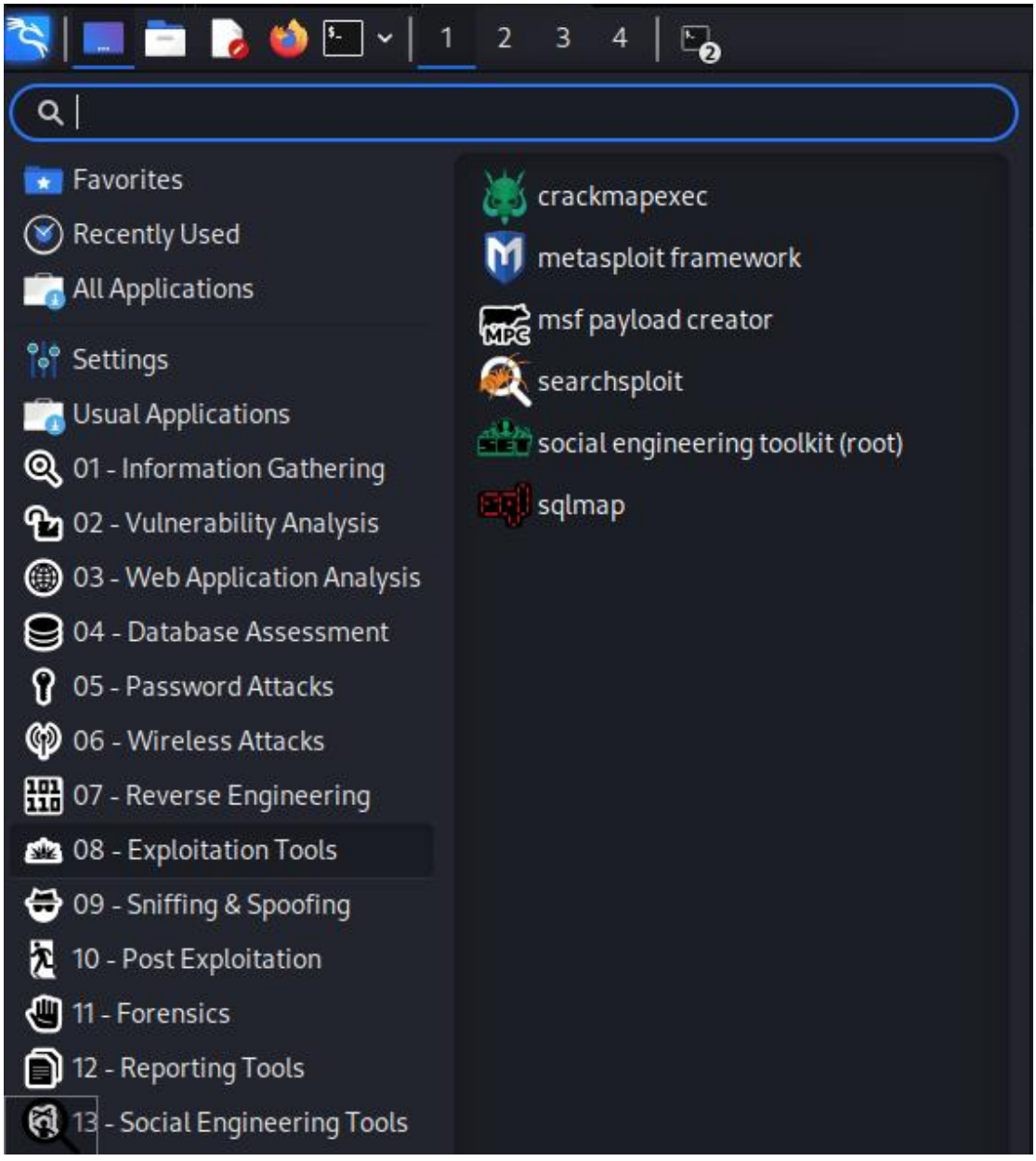
You will now be able to access Kali via SSH.



Finding and Using Kali Linux Tools

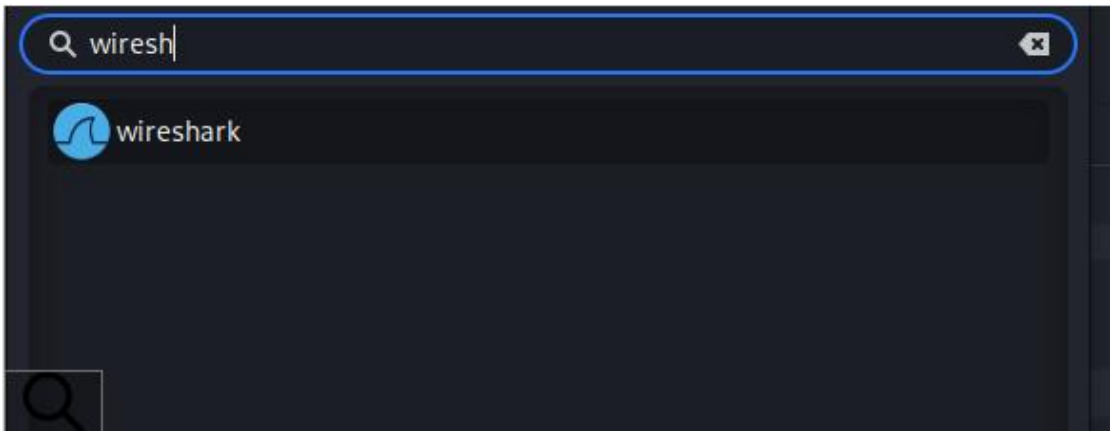
Next, we'll show you how to find the Kali tools and get them up and running easily.

All apps can be found in the apps menu. These are organized into categories for better order.



Hovering over each category will show you the tools that belong to it. The image below shows the tools included in the “Exploitation Tools” category.

To search for tools, use the search bar provided and start typing the tool you are looking for. In the example below, we’re looking for Wireshark.



You can also search for tools through the terminal. If you start typing the tool you're looking for and then press the Tab key, the terminal will search for tools that start with the letters you've typed and show you suggestions.

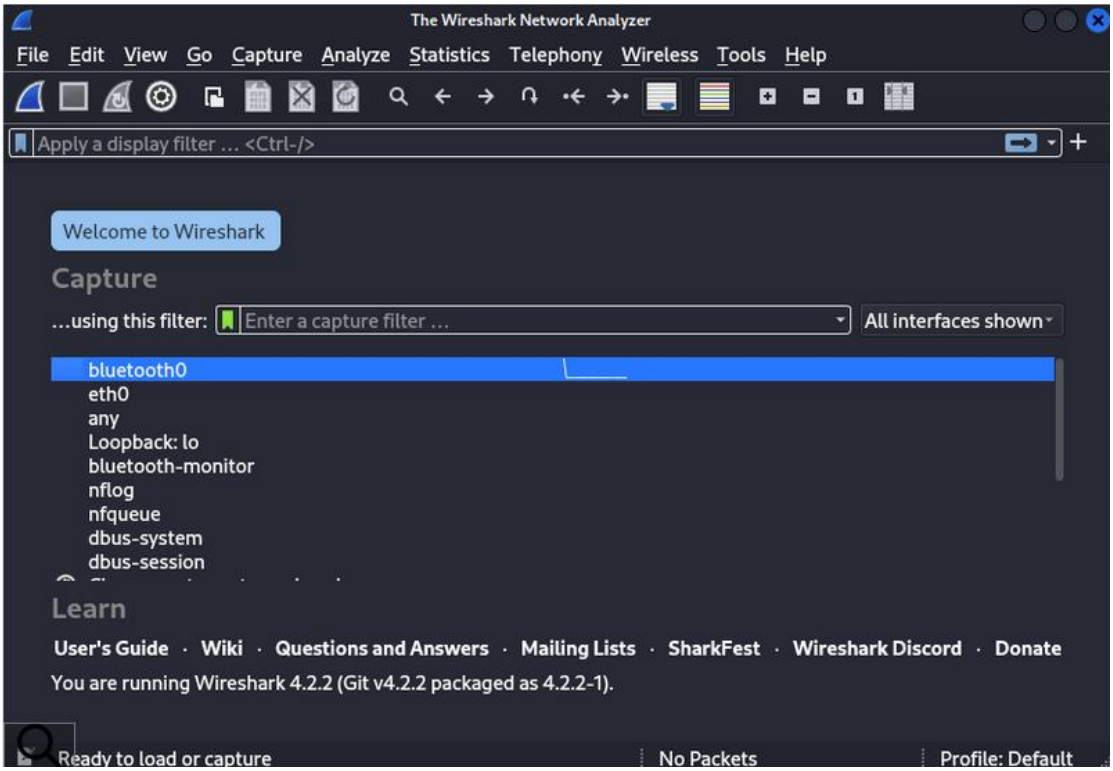
Some of the more popular Kali tools include Metasploit, Nmap, Wireshark, John, and Hydra.

We'll show you how to start Wireshark from the menu and the terminal.

To open Wireshark from the menu, just type "Wireshark" in the search bar and click "Run wireshark."

You can also start it by typing "Wireshark" in the terminal and pressing "Enter."

This will open the Wireshark GUI.



Installing Kali Basic Tools

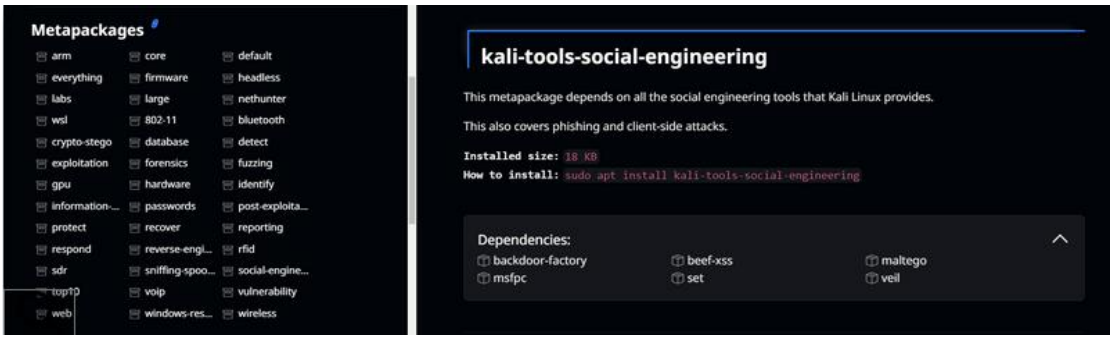
While Kali comes preinstalled with several tools that are sufficient for most situations, you may want to customize your toolset for more specialized purposes.

Metapackages of Kali

Kali provides convenient metapackages that bring together toolkits for different areas, such as wireless network attacks, web application security, reverse engineering, and more.

We will show you how to install additional metapackages.

To see a list of all metapackages and the tools included in each, visit the page Kali-Meta.



If you want to install the social engineering tools, type the following command:

sudo apt install kali-tools-social-engineering

Task 1: Download Kali Linux from the official website and verify the integrity of the ISO file.

Task 2: Install Kali Linux on VirtualBox/VMware and configure essential VM settings (RAM, CPU, Disk Space, Network).

Task 3: Take a screenshot of the installed system and submit it along with a brief installation report.

Note: Take help from the above helping material and follow the steps carefully.