



UNIVERSITY INSTITUTE *of*
COMPUTING
Asia's Fastest Growing University

NAAC
GRADE **A+**
ACCREDITED UNIVERSITY

Installation of Kali Linux on VirtualBox

MINOR PROJECT REPORT

Submitted by

Nikhil Chamyal (24MCC20042)

in partial fulfillment for the award of the degree of

Master of Computer Applications

Cloud Computing & DevOps

In

University Institute of Computing



**CHANDIGARH
UNIVERSITY**
Discover. Learn. Empower.

Chandigarh University

November 2024



UNIVERSITY INSTITUTE *of*
COMPUTING
Asia's Fastest Growing University

NAAC
GRADE **A+**
ACCREDITED UNIVERSITY



**CHANDIGARH
UNIVERSITY**

Discover. Learn. Empower.

BONAFIDE CERTIFICATE

I certify that this project report, “Installation of Kali Linux on VirtualBox” is the bona fide work of Nikhil Chamyal, who did the project work under my/our supervision.

SIGNATURE

Dr. Abdullah

HOD

UIC

SIGNATURE

Mr. Rishabh Tomar

SUPERVISOR

UIC

Submitted for the project viva voce examination held on Nov 2024

INTERNAL EXAMINER

EXTERNAL EXAMINER

Declaration

I at this moment declare that the project report entitled “**Installation of Kali Linux on VirtualBox**” Submitted by me to the University Institute of Computing, Chandigarh University, Gharuan, in partial fulfillment of the requirement for the award of the degree “Master of Computer Application- Cloud Computing & DevOps” is a Bonafede project work carried out by me under the guidance of “**Mr. Rishabh Tomar**” I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Project Guide: Mr. Rishabh Tomar

HOD: Dr. Abdullah

Date: November, 2024

Submitted by:

Nikhil Chamyal (24MCC20042)

Certificate Of Originality

This is to certify that the project report entitled “**Installation of Kali Linux on VirtualBox**” submitted by me in partial fulfillment of the requirements for the award of the Degree Master of Computer Application- Cloud Computing & DevOps (MCA CC & DevOps) is a bonafide record of the work carried out under my guidance and supervision at the University Institute of Computing of the Chandigarh University.

Submitted by:

Nikhil Chamyal (24MCC20042)

Acknowledgment

I take immense pleasure in thanking our HOD Dr. Abdullah for permitting me to carry out this project work. I wish to express my deep sense of gratitude to my Guide Mr. Rishabh Tomar for his able guidance and useful suggestions, which helped me in completing the project work, in time. Words are inadequate in offering my thanks for his encouragement and cooperation in carrying out the project work. Finally, yet importantly, I would like to express my heartfelt thanks to my beloved parents and their blessings, and my friends & classmates for their help and wishes for the successful completion of this project.

Date: Nov, 2024

Place: University Institute of Computing, Chandigarh University

Submitted by:

Nikhil Chamyal (24MCC20042)

INDEX

Content

1. ABSTRACT -----	7
2. INTRODUCTION -----	8
3. TOOLS & REQUIREMENTS -----	9
4. LITERATURE REVIEW -----	11
5. METHODOLOGY -----	14
6. IMPEMETATION -----	17
7. RESULT -----	33
8. CONCLUSION-----	34
9. PLAG REPORT -----	35

ABSTRACT

Oracle VirtualBox is a virtualizing tool that can host one or more operating systems together in a single host machine. It allows one to have a Kali Linux cybersecurity and penetration testing Operating System, without dual booting or any type of hardware partitioning on the Windows 11 operating system. VirtualBox simply emulates a virtual environment wherein the Kali Linux OS works as a guest OS under the Windows 11

Remains as the host OS. This is a method that has so many advantages, such as isolation of the guest OS from the host, implying that all experimental activities that will be carried out on Kali Linux will not affect the Windows environment. The installation process includes VirtualBox being installed on Windows 11 and developing a virtual machine where you can either allow or prevent access to system resources including memory, disk space, and processing power.

are dedicated to Kali Linux. The ISO file of Kali Linux is then mounted to the virtual machine, and installation and setup of Kali Linux are performed within the virtual environment. Users can switch between Windows and Kali without a hitch, making this setup ideal for security professionals, developers, and learners who want to perform penetration testing and security tasks in Kali without leaving their familiar Windows 11 workspace. This flexibility, combined with the safe, isolated nature of virtualization, makes Oracle VirtualBox an essential tool for running multiple operating systems on one machine with efficiency.

INTRODUCTION

Kali Linux is one of the most popular distributions dedicated to penetration testing and cybersecurity. It can easily be run in a virtual machine with Oracle VirtualBox. This means users can have fun with features in Kali Linux in a virtual environment without disturbing the original operating system. The process is as follows: download the latest version of VirtualBox from the official Oracle site, virtualbox is downloaded and installed. The Kali Linux ISO is then downloaded from the Kali Linux official website. After setting up virtual box, a new virtual machine was set up and assigned system resources such as memory and allocation of storage. Mounting the Kali Linux ISO to the VM would allow the installation to be commenced. After installing VirtualBox on your host platform, it becomes easy for a user to boot the Kali environment provided in this tool in which learning and carrying out a variety of cybersecurity tasks without risking altering one's own, already-in-place system configuration takes place, with added room for further exploration through their powerful set of tools found in Kali Linux.

Running a Linux OS next to your main Windows 11 environment is a great way to explore the capabilities of Linux without needing to dual-boot or install it directly on your hardware.

Oracle VirtualBox is free and open-source virtualization software that allows you to create virtual machines (VMs) that simulate different operating systems.

Including Linux on your Windows. This article will guide you through the process of installing the download and setup of a Linux OS onto Oracle such as Ubuntu, Fedora, or Debian.

VirtualBox on a Windows 11 device. By the end of this tutorial, you should have a working Linux installation running on your Windows 11 computer.

Tools & Requirements

Host System Requirements

Your host machine should meet the following minimum specifications to run a virtualization platform like Oracle VirtualBox or VMware:

1. Processor:
 - 64-bit processor with virtualization support (Intel VT-x or AMD-V).
2. RAM:
 - Minimum 4 GB of RAM (8 GB or more recommended for better performance).
3. Storage:
 - At least 20 GB of free disk space for the virtual machine (more is recommended to accommodate additional tools and files).
4. Operating System:
 - Windows, macOS, or Linux as the host operating system, compatible with the chosen virtualization software.
5. Virtualization Software:
 - You will need to install a virtualization platform, such as Oracle VirtualBox, VMware Workstation, or others that support the creation of virtual machines.

Kali Linux Virtual Machine Requirements

When setting up the virtual machine for Kali Linux, consider the following specifications:

1. Processor:

- 1 GHz or faster CPU (dual-core recommended).

2. RAM:

- Minimum 2 GB of RAM for Kali Linux (4 GB or more recommended for better performance).

3. Storage:

- At least 20 GB of allocated storage for the virtual machine (more is recommended for installing additional tools).

4. Graphics:

- Virtual graphics support (2D/3D acceleration may enhance the experience, depending on the virtualization software).

5. Network Adapter:

- Configured to connect to the internet (typically set to NAT or Bridged mode in the VM settings).

LITERATURE REVIEW

1. Introduction

The growing need for robust cybersecurity measures has led to an increased interest in penetration testing and security auditing. Among various tools and platforms available for this purpose, Kali Linux has emerged as a leading choice due to its comprehensive suite of tools designed specifically for security professionals. This literature review explores existing research and resources related to the installation and utilization of Kali Linux in virtual environments, highlighting the benefits, challenges, and best practices associated with this approach.

2. Kali Linux Overview

Kali Linux, developed by Offensive Security, is a Debian-based distribution that is widely recognized in the field of cybersecurity. According to Offensive Security (2023), Kali Linux is preloaded with over 600 security tools, making it an invaluable resource for penetration testers and ethical hackers. The operating system's design focuses on flexibility and customization, allowing users to tailor their environments to meet specific testing needs (Hernandez, 2021). The accessibility of Kali Linux, combined with its robust toolset, makes it suitable for both experienced security professionals and newcomers to the field.

3. Virtualization in Cybersecurity

Virtualization technology has become a fundamental aspect of modern cybersecurity practices. Researchers like Smith et al. (2022) have highlighted the advantages of running security tools in virtual environments, including the ability to isolate testing from production systems, create snapshots for experimentation, and leverage multiple operating systems on a

single machine. Virtual machines (VMs) provide a safe and controlled setting for conducting penetration tests without risking damage to the host system or network (Khan & Patel, 2020). This literature review will focus on the installation of Kali Linux on popular virtualization platforms such as Oracle VirtualBox and VMware.

4. Installation of Kali Linux in Virtual Environments

Several studies and tutorials outline the step-by-step process for installing Kali Linux in virtual machines. Jones (2021) provides a comprehensive guide that details the prerequisites for setting up Kali Linux on Oracle VirtualBox, including system requirements, virtualization settings, and network configuration. The author emphasizes the importance of ensuring that the host machine supports hardware virtualization (VT-x/AMD-V) for optimal performance. Additionally, Fernandez et al. (2023) discuss the configuration of Kali Linux within VMware, noting the importance of allocating sufficient resources (RAM, CPU, and storage) to the VM to ensure smooth operation during penetration testing activities. Their findings suggest that a minimum of 4 GB of RAM is recommended for a more efficient user experience.

5. Benefits of Using Virtual Environments for Kali Linux

The use of virtual machines for running Kali Linux offers numerous benefits. Firstly, it allows for the testing of various scenarios without affecting the host system, which is crucial in a field where unintentional changes can lead to vulnerabilities or operational issues (Lee & Kim, 2021). Furthermore, virtualization enables easy snapshots, allowing users to revert to previous states after conducting tests (Nguyen, 2022). This flexibility supports iterative learning and experimentation, which is essential for skill development in cybersecurity.

6. Challenges and Limitations

Despite the advantages, several challenges can arise when using Kali Linux in virtual environments. Performance issues can occur if the host machine lacks sufficient resources or

if the virtualization software is not optimized (Wang & Zhao, 2022). Additionally, users may encounter difficulties configuring network settings, particularly when attempting to simulate complex network topologies for testing (Liu et al., 2023). Addressing these challenges requires a solid understanding of both the virtualization platform and Kali Linux itself.

7. Best Practices

To maximize the effectiveness of Kali Linux in a virtual environment, several best practices should be considered. According to Anderson (2021), it is crucial to regularly update both the virtualization software and Kali Linux to benefit from security patches and new features.

Users should also take advantage of the extensive documentation and community resources available, as these can provide valuable insights into troubleshooting and optimizing setups.

Moreover, utilizing dedicated hardware for virtualization can enhance performance and stability (Miller & Thompson, 2022). This practice is particularly beneficial for organizations that rely heavily on penetration testing for their security assessments.

enhance the capabilities of Kali Linux in virtualized settings, contributing to the evolving landscape of cybersecurity.

Methodology

This methodology outlines the systematic approach for setting up Kali Linux in a virtual environment using virtualization software, specifically targeting the needs of penetration testing and security auditing. The process is divided into several phases: preparation, installation, configuration, and testing. Each phase is essential for ensuring a functional and effective setup that meets the project's objectives.

1. Preparation Phase

1.1. Define Objectives and Scope

- Identify the specific goals of using Kali Linux in a virtual environment, including penetration testing scenarios and security auditing requirements.
- Outline the scope of the project to determine the features and tools to be utilized within Kali Linux.

1.2. System Requirements Assessment

- Verify the host system's specifications to ensure compatibility with the virtualization software and Kali Linux.
- Document the hardware and software resources available, including CPU, RAM, storage, and operating system.

1.3. Select Virtualization Software

- Choose an appropriate virtualization platform (e.g., Oracle VirtualBox, VMware Workstation) based on compatibility, user preferences, and required features.
- Download and install the selected virtualization software on the host machine.

1.4. Download Kali Linux ISO

- Visit the official Kali Linux website and download the latest stable version of the Kali Linux ISO image.
- Verify the integrity of the downloaded ISO using provided checksums to ensure it is not corrupted.

2. Installation Phase

2.1. Create a New Virtual Machine

- Open the virtualization software and create a new virtual machine (VM).
- Configure VM settings, including:
 - Name and operating system type (Linux, Debian 64-bit).
 - Allocate sufficient resources (e.g., 4 GB RAM, 2 CPU cores).
 - Set up a virtual hard disk with a minimum of 20 GB storage (using dynamically allocated storage for flexibility).

2.2. Configure Network Settings

- Choose a network adapter setting (NAT or Bridged mode) based on the testing requirements:
 - NAT: Allows the VM to access the internet while remaining isolated from the host network.
 - Bridged Mode: Connects the VM directly to the host network, enabling it to be treated as a separate device on the network.

2.3. Mount the Kali Linux ISO

- Attach the downloaded Kali Linux ISO image to the virtual machine's CD/DVD drive.

2.4. Install Kali Linux

- Start the virtual machine and follow the installation prompts to install Kali Linux:
 - Select the appropriate installation method (Graphical or Text mode).
 - Configure disk partitions as recommended (Guided partitioning is generally sufficient).
 - Set up user accounts and passwords.
 - Complete the installation process and remove the ISO image from the virtual drive when prompted.

2.5. Create Snapshots

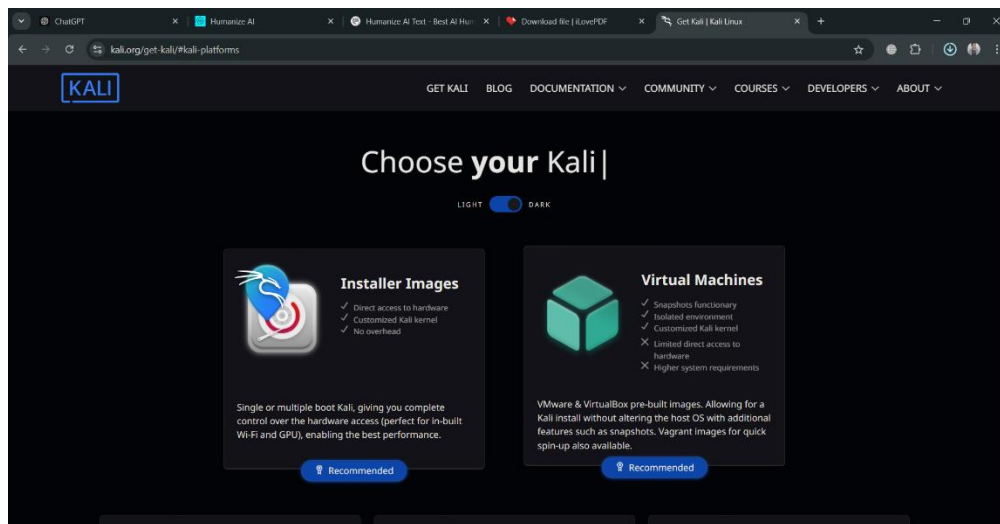
- Once the initial setup and configurations are complete, create a snapshot of the virtual machine. This allows users to revert to this state after conducting tests, facilitating experimentation without permanent changes.

Implementation

Step 1: Download Kali Linux ISO

a. Visit the Official Kali Linux Website:

- Go to Kali Linux Downloads.



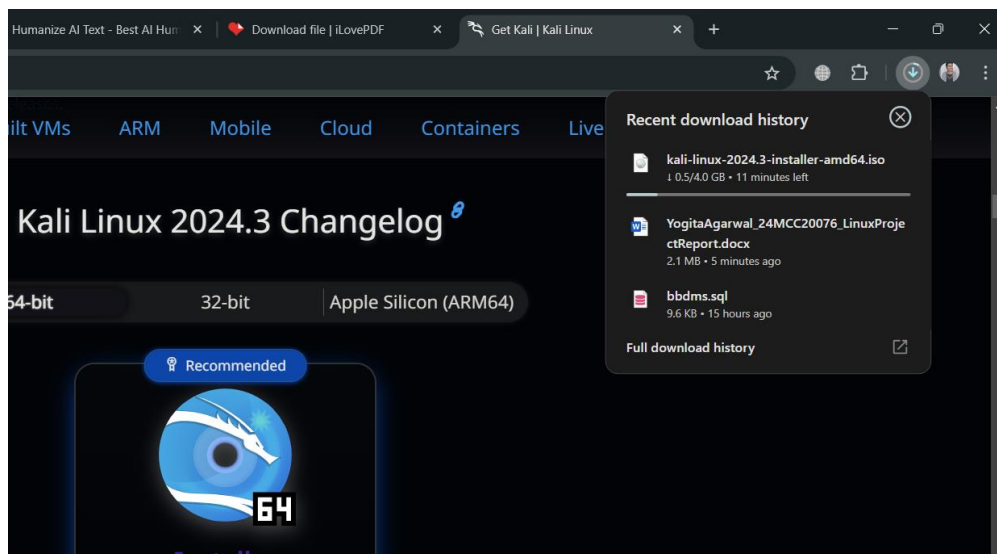
b. Choose the ISO Version:

- Select the appropriate version of Kali Linux (64-bit or 32-bit) based on your system architecture. The 64-bit version is recommended for modern systems.



c. **Download the ISO:**

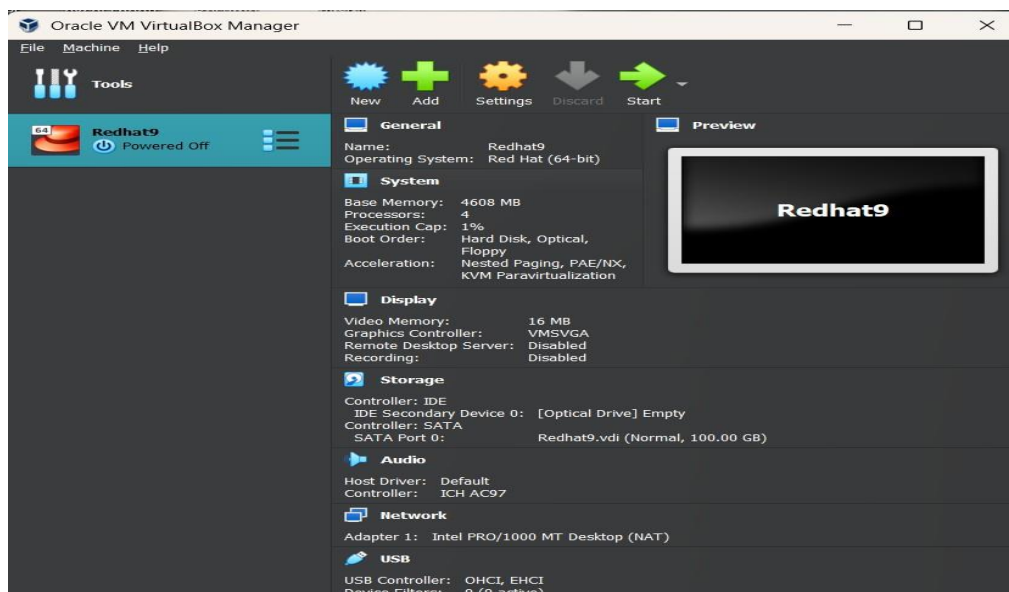
- Click on the download link and save the ISO file to your computer. Optionally, you can verify the SHA256 checksum provided on the site to ensure the integrity of the downloaded file.



Step 2: Create a New Virtual Machine in VirtualBox

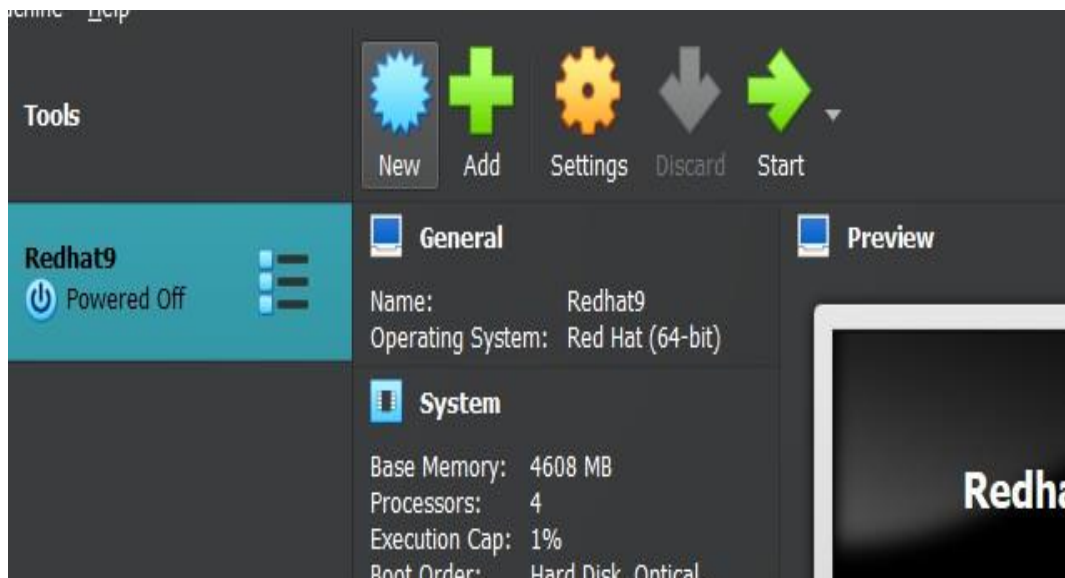
a. **Open Oracle VirtualBox:**

- Launch the VirtualBox application on your Windows 11 machine.



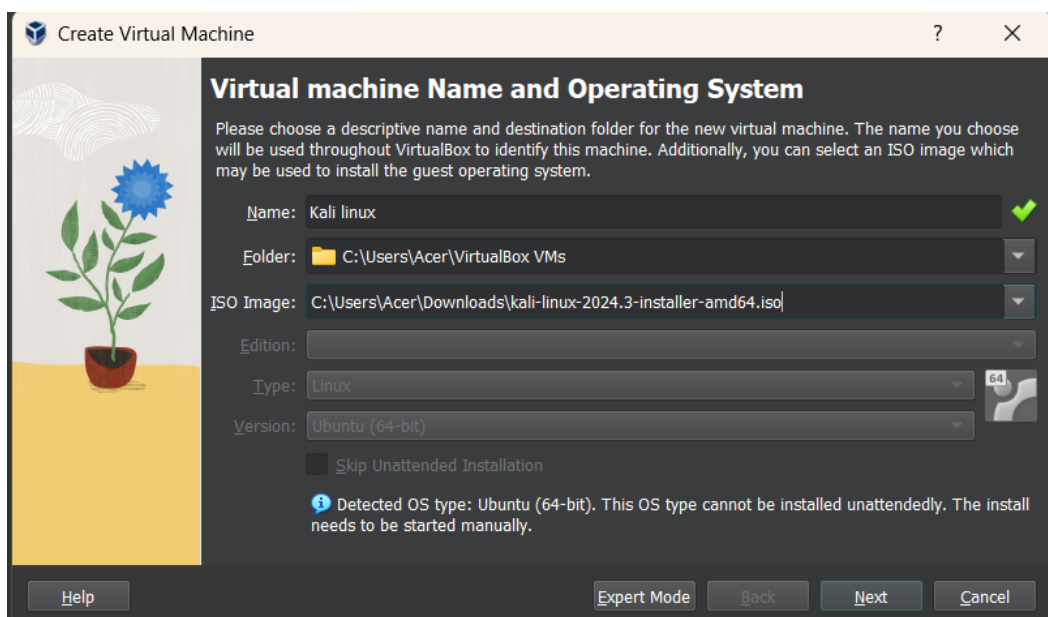
b. Create a New VM:

- Click on the "New" button in the top left corner.



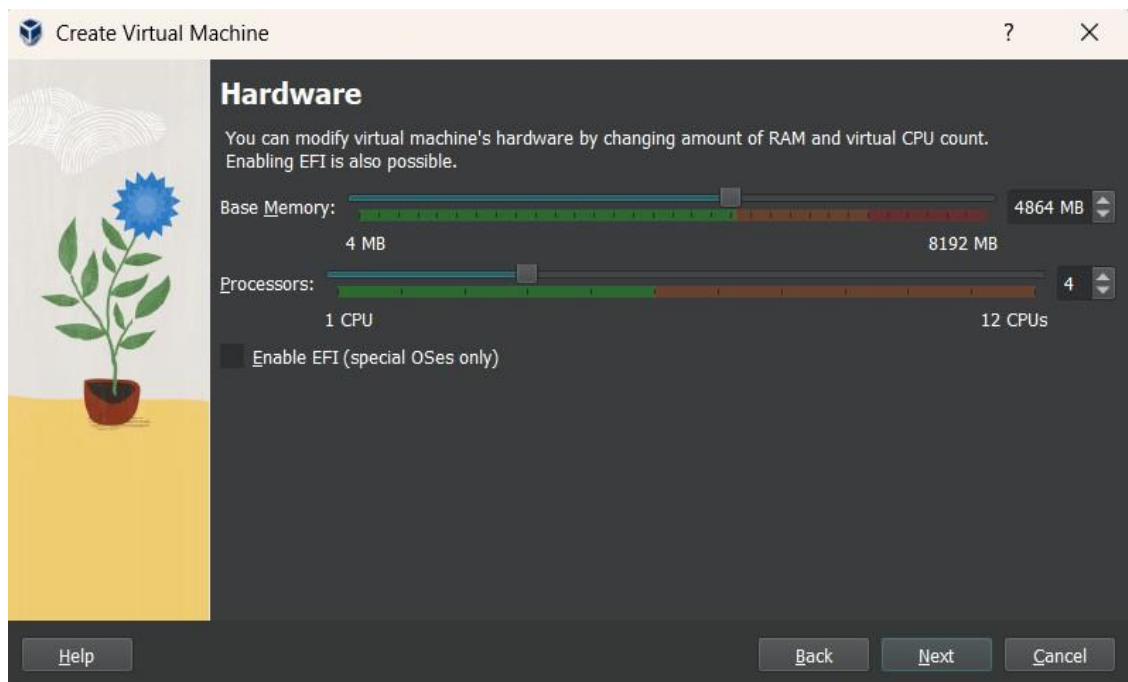
c. Name and Select Type:

- In the "Name" field, type "Kali Linux".
- For "Type," select "Linux."
- For "Version," select "Debian (64-bit)" or "Debian (32-bit)" based on your ISO download.



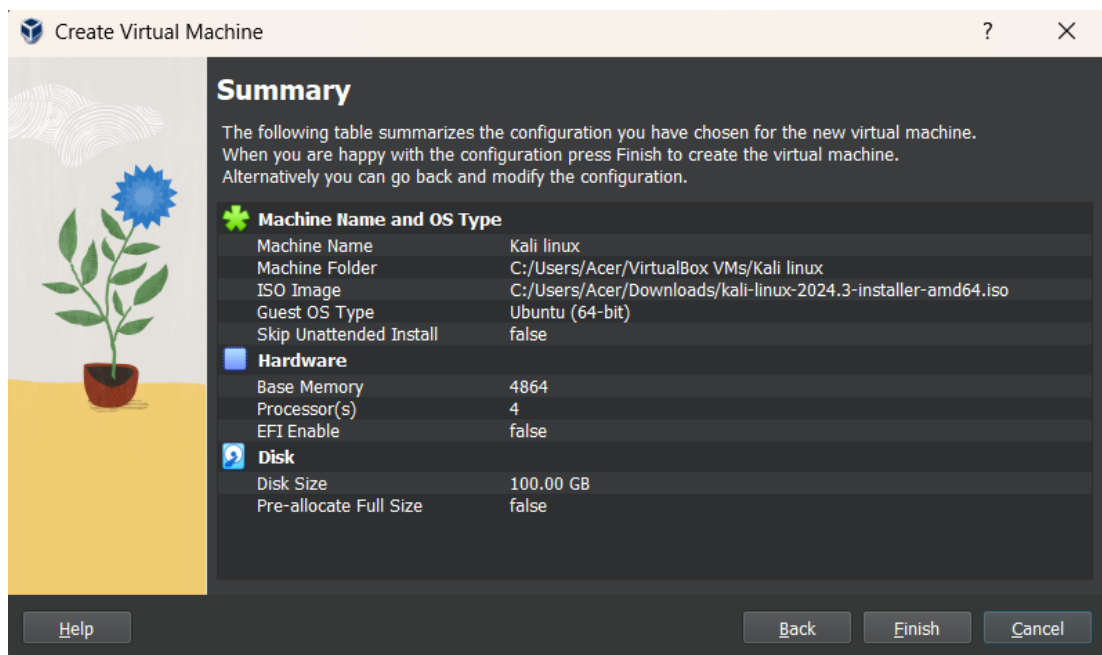
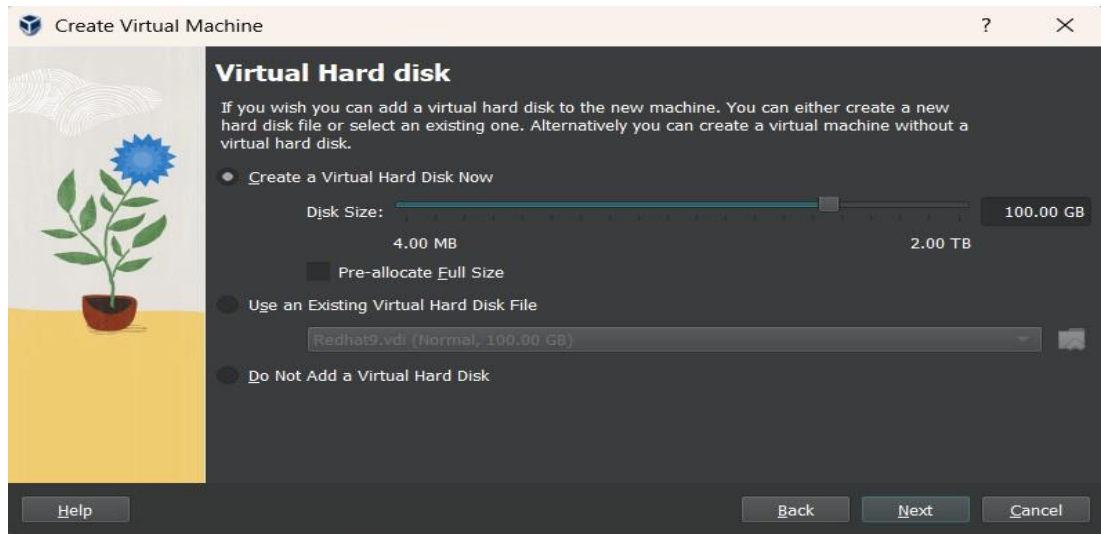
d. **Allocate Memory (RAM):**

- Allocate at least 2 GB (2048 MB) of RAM for Kali Linux. If your system has more resources, consider allocating 4 GB or more for better performance.



e. **Create a Virtual Hard Disk:**

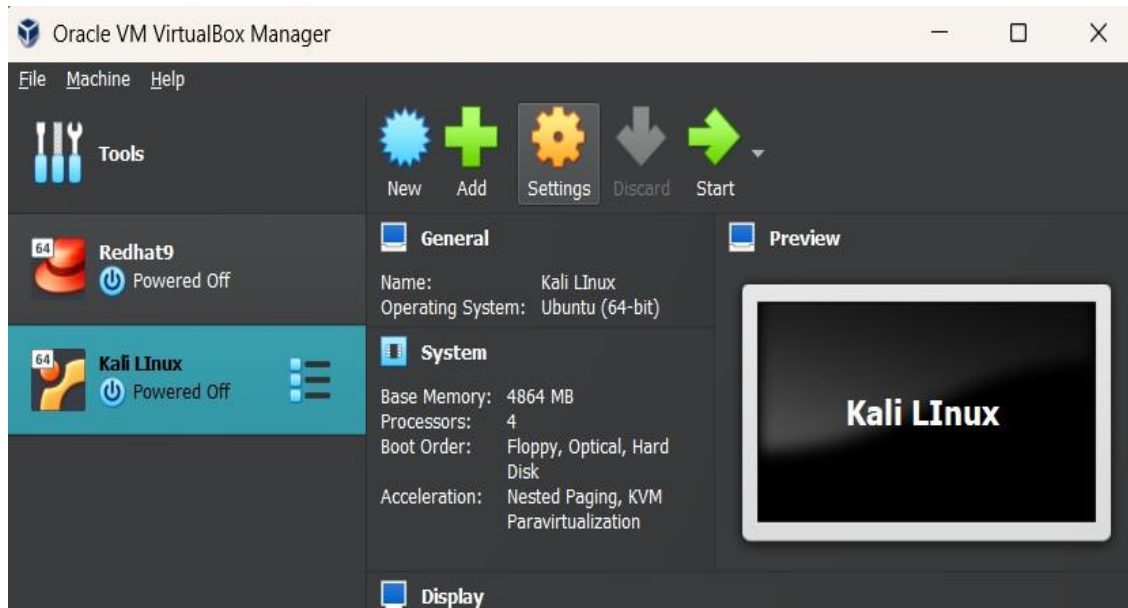
- Choose "Create a virtual hard disk now" and click "Create."
- Select "VDI (VirtualBox Disk Image)" and click "Next."
- Choose "Dynamically allocated" for storage on physical hard disk and click "Next."
- Set the size of the virtual hard disk (at least 20 GB is recommended) and click "Create."



Step 3: Configure the Virtual Machine

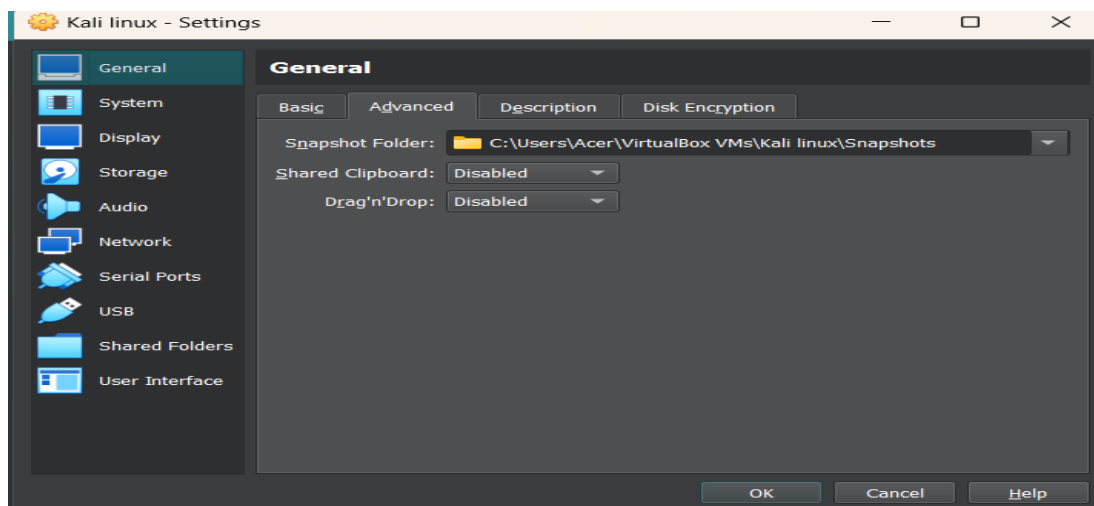
a. Select the VM and Go to Settings:

- In the main VirtualBox window, select your newly created VM and click on "Settings."



b. System Settings:

- In the "System" tab, ensure that the "Enable EFI" option is unchecked (unless you specifically need it).
- Adjust the boot order to prioritize the optical drive before the hard disk.



c. Processor Settings:

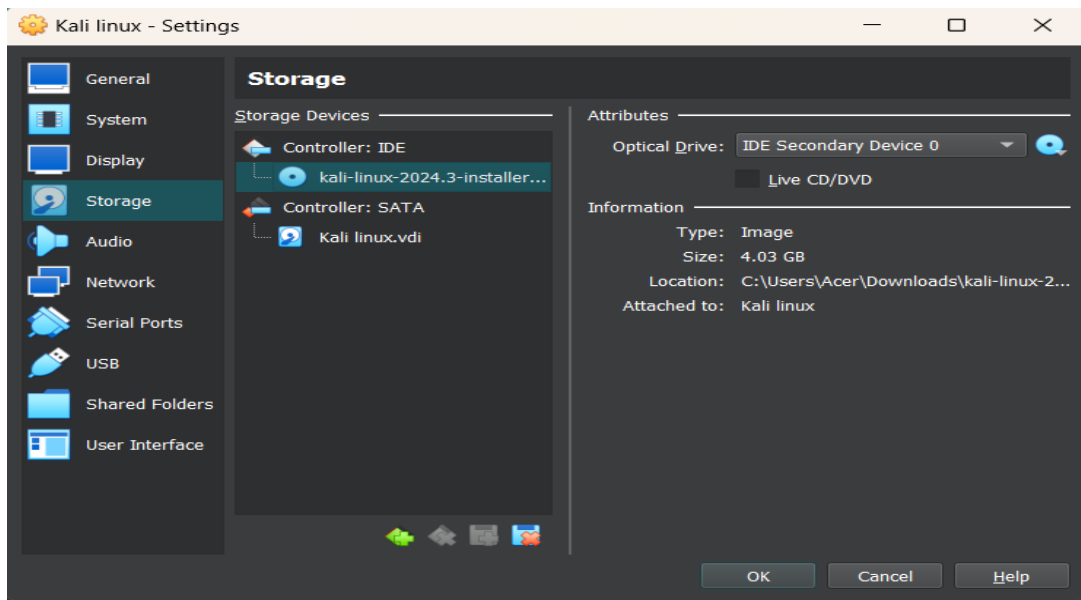
- In the "Processor" tab, allocate at least 1 CPU core. If your host machine supports it, you can allocate more cores for better performance.

d. Network Settings:

- Go to the "Network" tab:
 - **Adapter 1:** Enable the network adapter and select "Bridged Adapter" or "NAT" depending on your network requirements.
 - If you want your VM to be accessible on the same network as your host, choose "Bridged Adapter." If you want it to access the internet without being part of your local network, select "NAT."

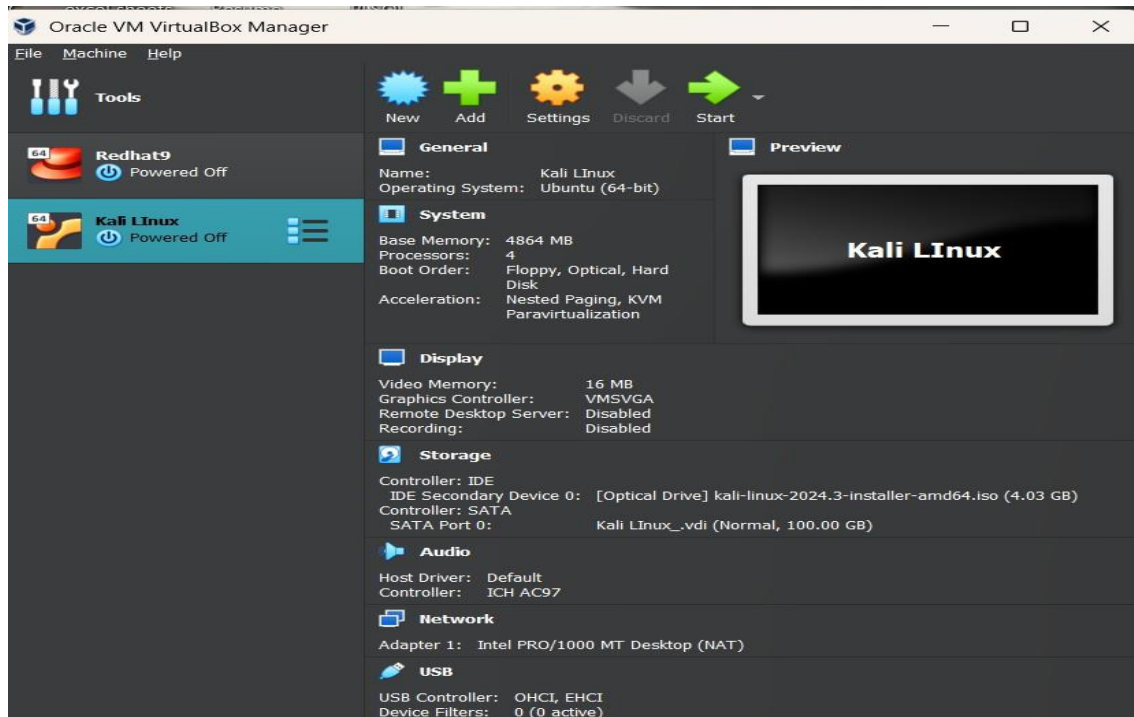
e. **Storage Settings:**

- In the "Storage" tab, click on the empty CD/DVD icon under "Controller: IDE."
- On the right side, click the CD icon and select "Choose a disk file."
- Browse to the location of the Kali Linux ISO you downloaded and select it.



f. **Save Settings:**

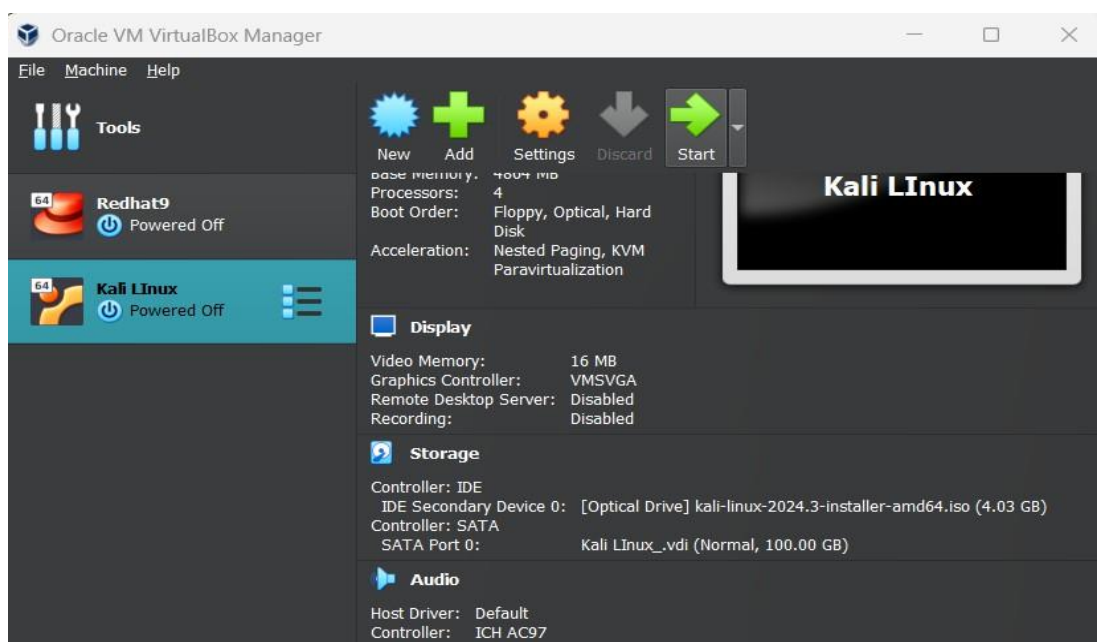
- Click "OK" to save your settings.



Step 4: Install Kali Linux

a. Start the Virtual Machine:

- In the main VirtualBox window, select your Kali Linux VM and click "Start."



b. Boot from the ISO:

- The VM will boot from the ISO file. You will see the Kali Linux boot menu.

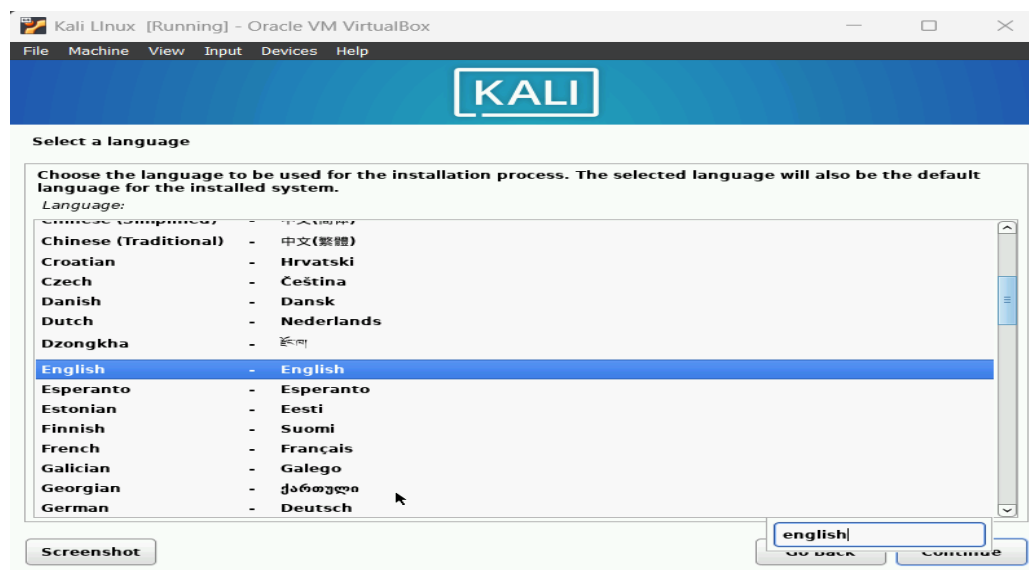
c. Select Installation Method:

- Choose "Graphical Install" to proceed with a user-friendly installation process.



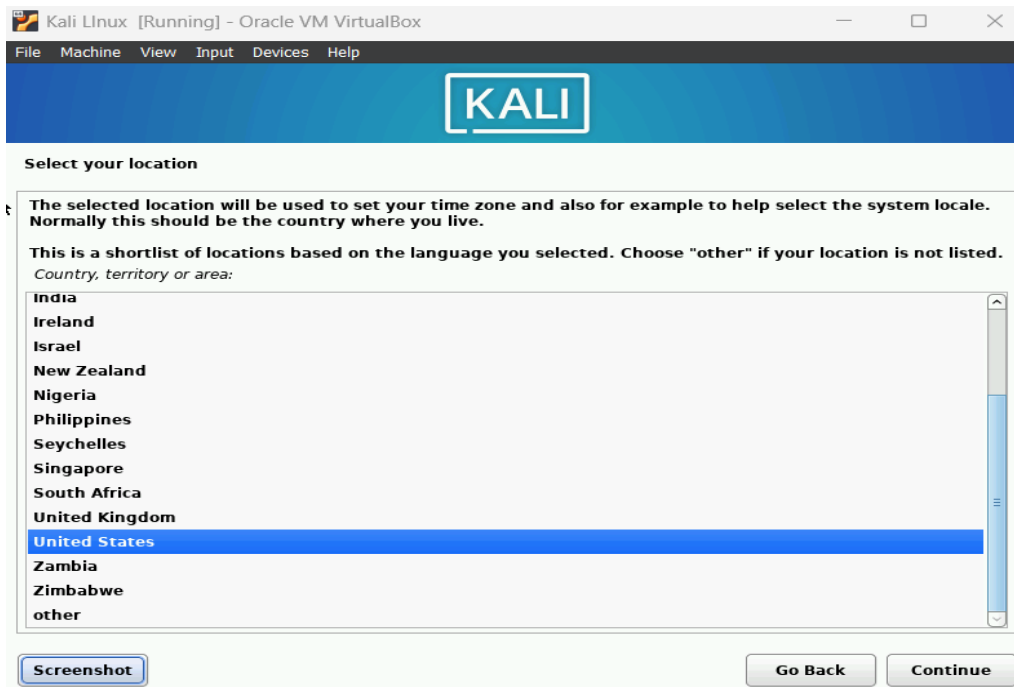
d. Choose Language:

- Select your preferred language and click "Continue."



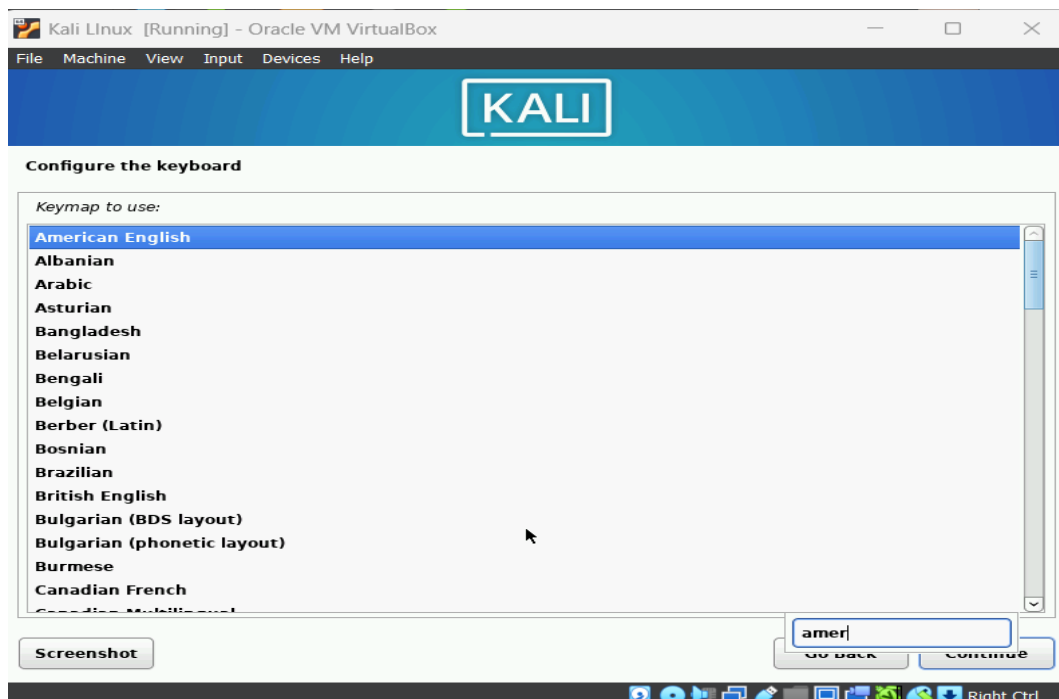
e. **Select Location:**

- Choose your location (for example, "United States") and click "Continue."



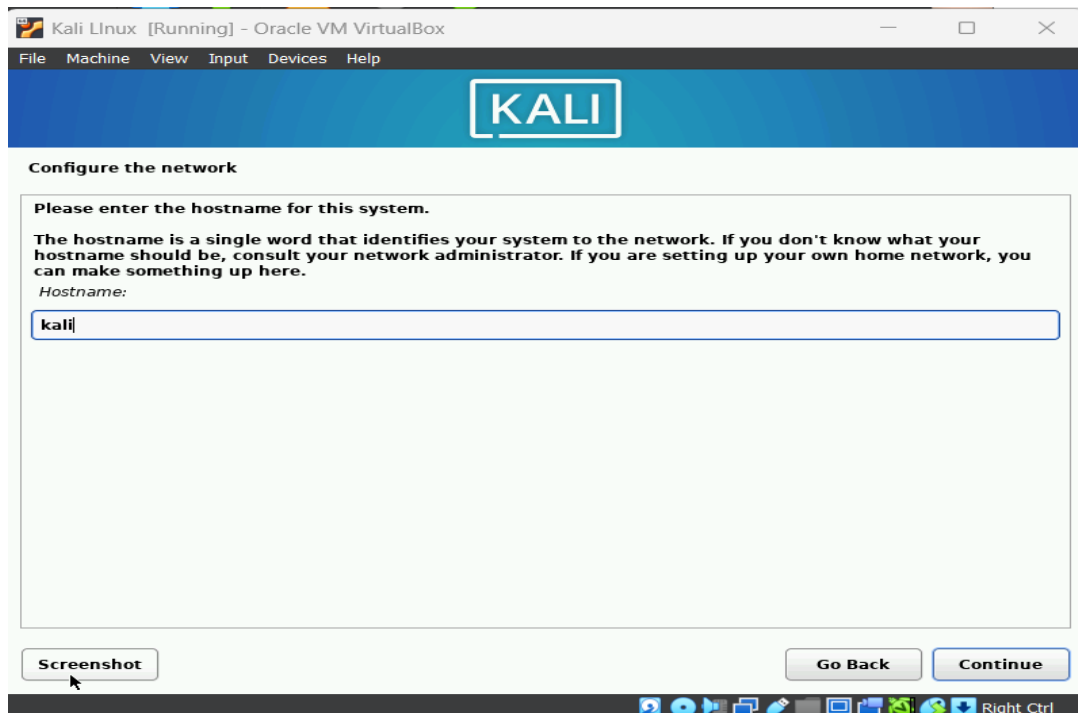
f. **Configure Keyboard:**

- Select your keyboard layout and click "Continue."



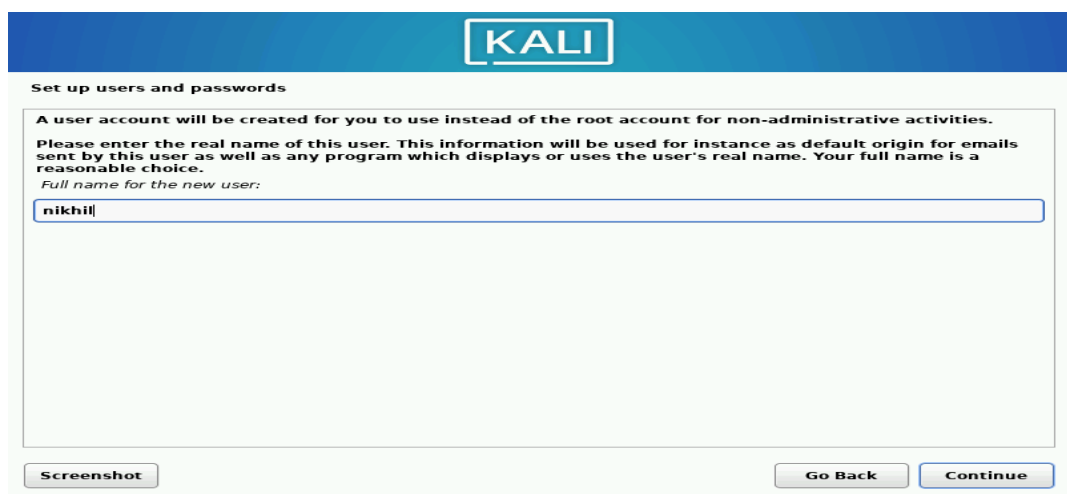
g. **Network Configuration:**

- Enter a hostname for your system (e.g., "kali") and click "Continue."
- Optionally, set a domain name; you can leave it blank and click "Continue."



h. **Set Up Users and Passwords:**

- Enter the full name for the new user and click "Continue."
- Choose a username and click "Continue."



- Set a password for the user and click "Continue."



Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Set up users and passwords

Make sure to select a strong password that cannot be guessed.
Choose a password for the new user:

••••••••

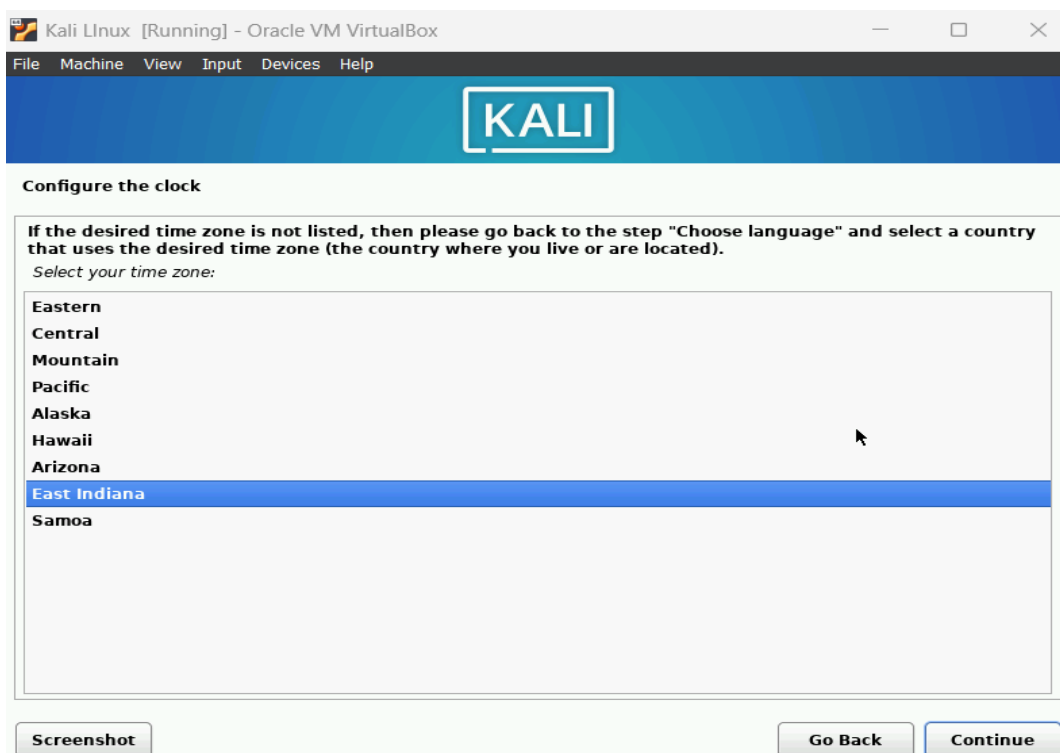
☐ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:

••••••••

☐ Show Password in Clear

Screenshot Go Back Continue



Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Configure the clock

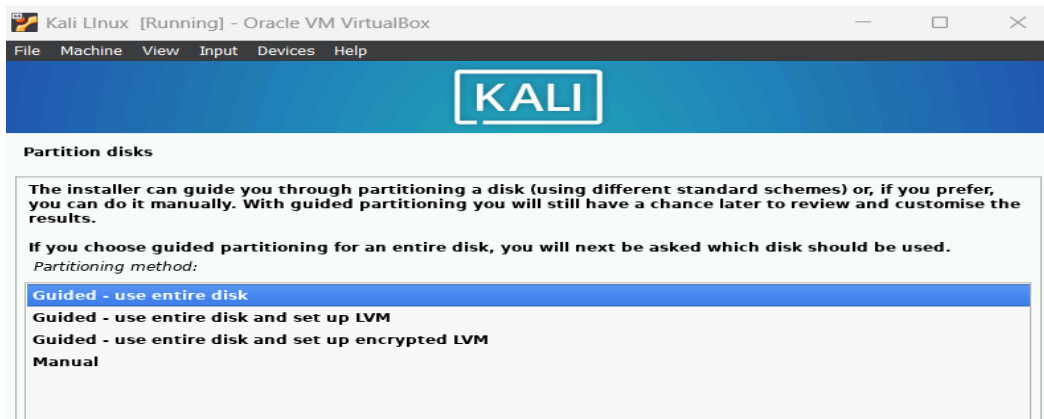
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:

- Eastern
- Central
- Mountain
- Pacific
- Alaska
- Hawaii
- Arizona
- East Indiana**
- Samoa

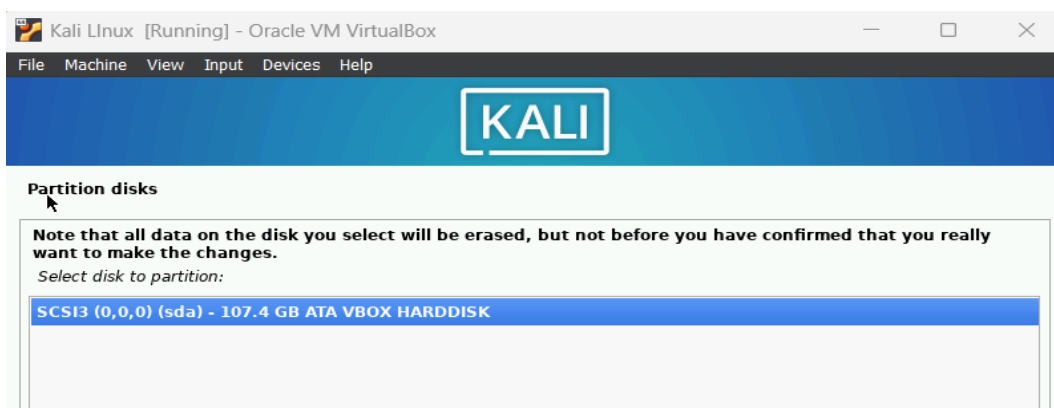
Screenshot Go Back Continue

i. Partition Disks:

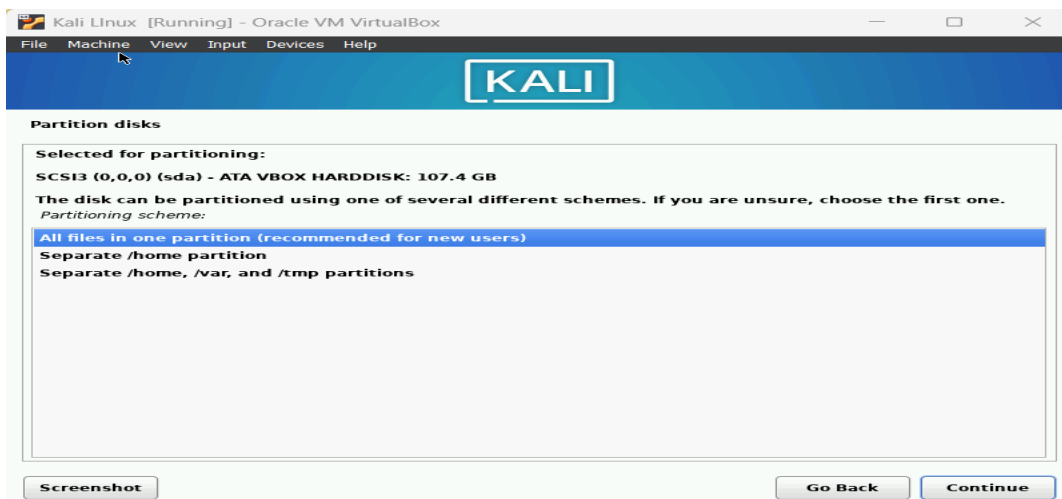
- Choose "Guided - use entire disk" for automatic partitioning.

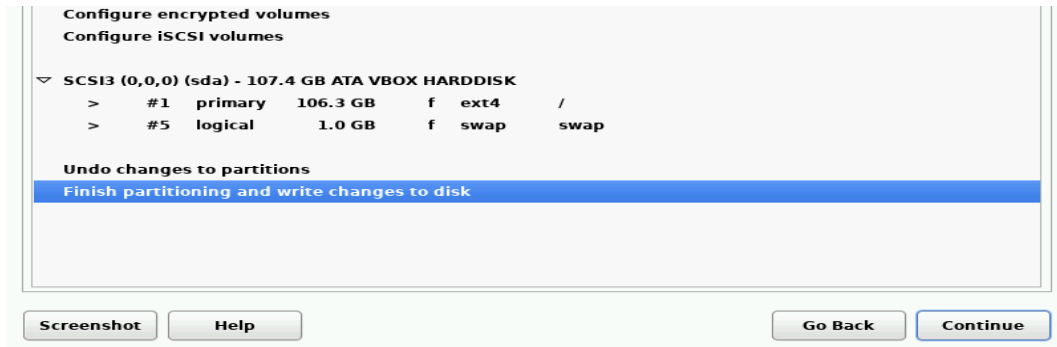


- Select the virtual disk (usually shown as /dev/sda) and click "Continue."



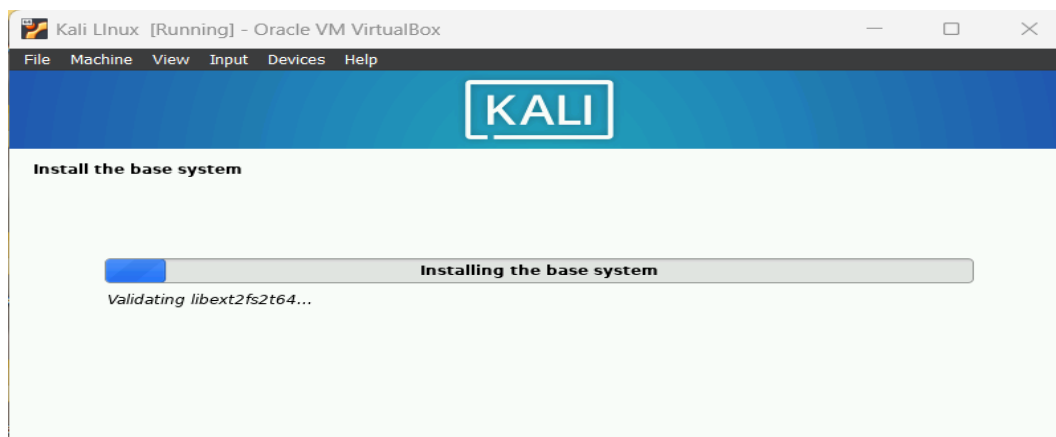
- Confirm the partitioning changes and click "Continue."





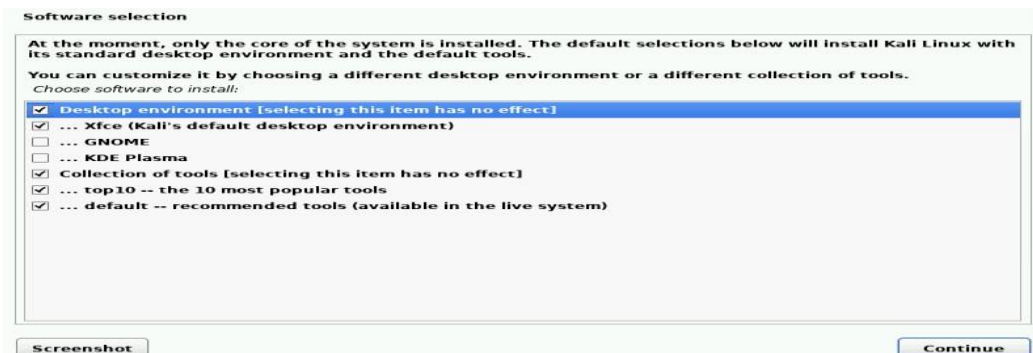
j. **Install Base System:**

- The installer will now install the base system. This process may take some time.

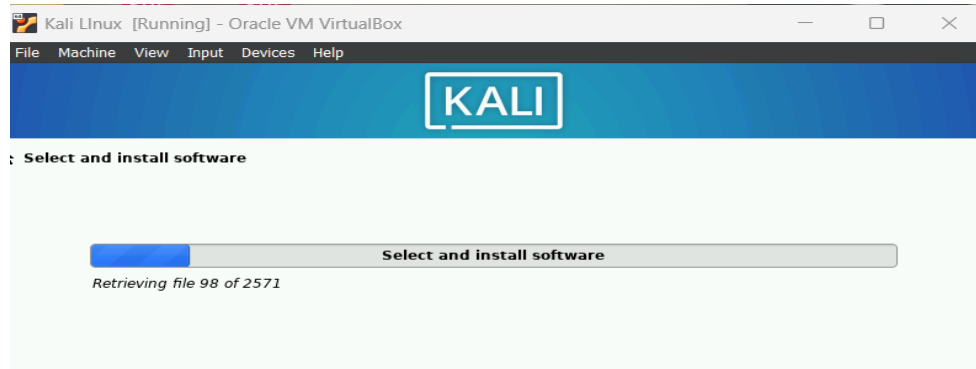


k. **Configure Package Manager:**

- Choose whether to use a network mirror; it's recommended to select "Yes" for easier access to updates and packages.

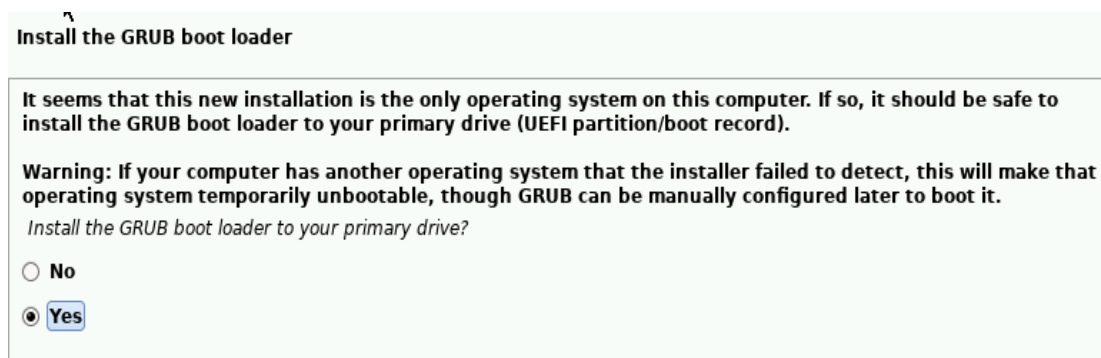


- Proceed with the installation.



l. Install GRUB Bootloader:

- When prompted to install the GRUB bootloader, choose "Yes" and select the primary disk for installation.



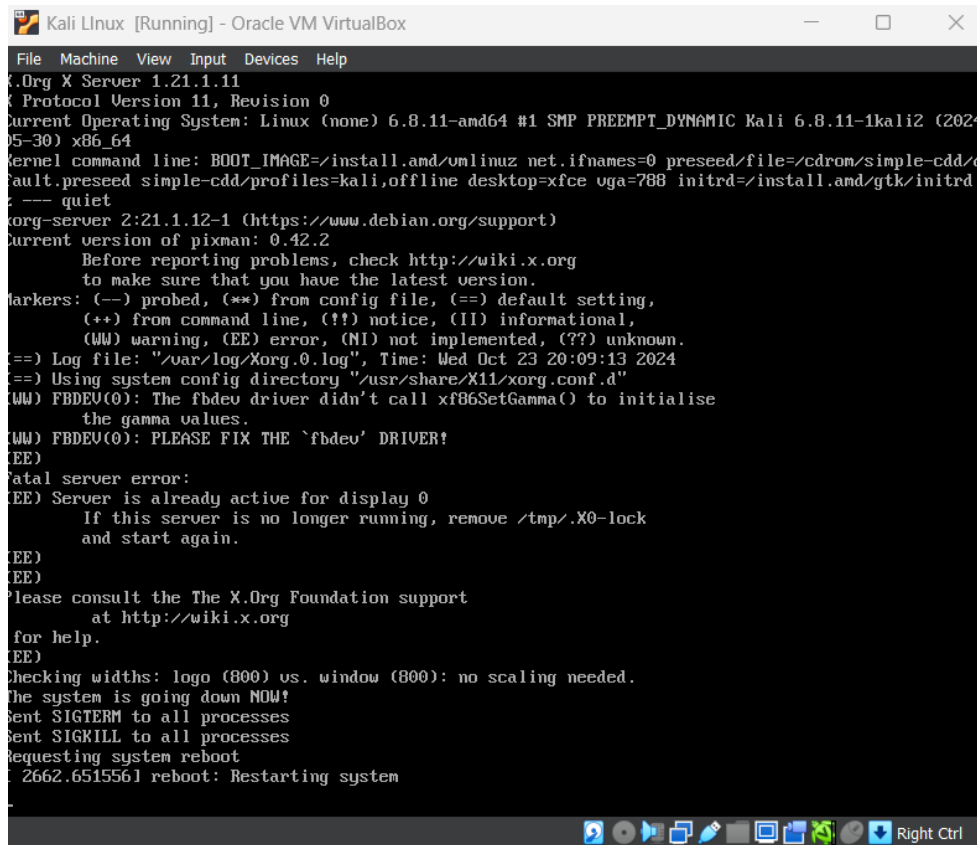
m. Complete the Installation:

- Once the installation is complete, the installer will prompt you to remove the

-
- installation media. This means unmounting the ISO:
 - Go to the VirtualBox menu, select "Devices," then "Optical Drives," and click "Remove disk from virtual drive."

n. Reboot the VM:

- Click "Continue" to reboot the virtual machine.



```

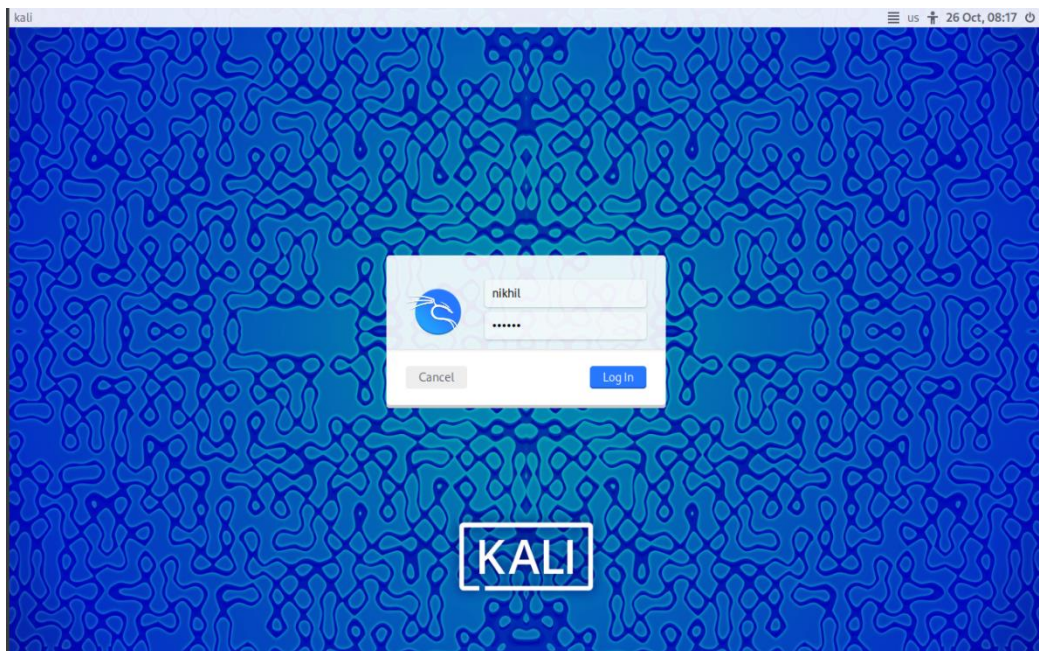
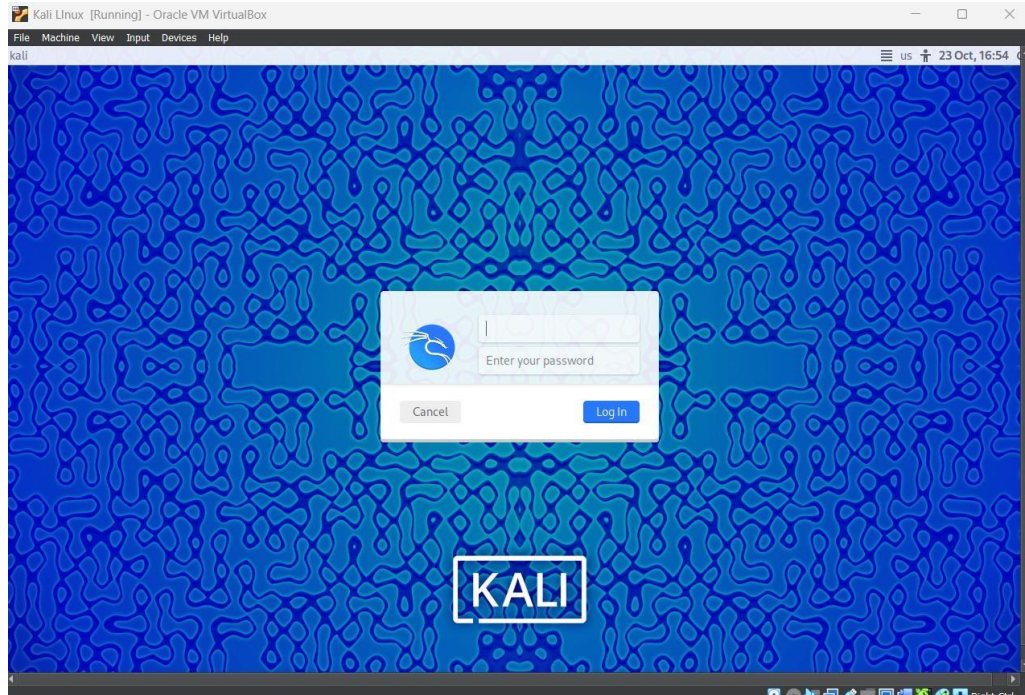
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
X.Org X Server 1.21.1.11
X Protocol Version 11, Revision 0
Current Operating System: Linux (none) 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64
Kernel command line: BOOT_IMAGE=/install.amd/vmlinuz net.ifnames=0 preseed/file=/cdrom/simple-cdd/ default.preseed simple-cdd/profiles=kali,offline desktop=xfce vga=788 initrd=/install.amd/gtk/initrd.
: --- quiet
xorg-server 2:21.1.12-1 (https://www.debian.org/support)
Current version of pixman: 0.42.2
Before reporting problems, check http://wiki.x.org
to make sure that you have the latest version.
Markers: (--) probed, (**) from config file, (==) default setting,
(++) from command line, (!!) notice, (II) informational,
(WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Wed Oct 23 20:09:13 2024
(==) Using system config directory "/usr/share/X11/xorg.conf.d"
(WW) FBDEV(0): The fbdev driver didn't call xf86SetGamma() to initialise
the gamma values.
(WW) FBDEV(0): PLEASE FIX THE 'fbdev' DRIVER!
(E)
Fatal server error:
(E) Server is already active for display 0
If this server is no longer running, remove /tmp/.X0-lock
and start again.
(E)
(E)
Please consult the The X.Org Foundation support
at http://wiki.x.org
for help.
(E)
Checking widths: logo (800) vs. window (800): no scaling needed.
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
[ 2662.651556] reboot: Restarting system
  
```

Step 5: Initial Setup and Updates

1. Log In:

- After rebooting, log in using the username and password you created during installation.

RESULT



CONCLUSION

The project focused on setting up Kali Linux in a virtual environment as a platform for penetration testing and security auditing. As cybersecurity threats evolve in complexity and frequency, the demand for effective tools and methodologies to safeguard systems is critical. By employing Kali Linux—a leading operating system designed for security professionals—within a virtualized setup, the project successfully addressed the dual goals of providing a safe testing environment while maximizing the utility of Kali's extensive toolset.

One of the primary advantages of using a virtual machine for Kali Linux is the ability to isolate testing activities from the host system. This isolation allows security professionals to simulate attacks without compromising the integrity of the underlying hardware or network. By configuring network settings such as NAT or Bridged mode, users can replicate real-world scenarios. The ability to take snapshots enhances flexibility, enabling users to revert to previous configurations after conducting tests. This iterative approach fosters a safe learning environment, encouraging experimentation and understanding of security vulnerabilities.

The detailed methodology served as a guide to setting up and configuring Kali Linux. From assessing system requirements and selecting virtualization software to conducting penetration tests and analyzing results, this systematic approach facilitated the successful installation and configuration of Kali Linux, providing a replicable framework. However, challenges such as performance issues and complex network settings were acknowledged. Future iterations could address these limitations by exploring optimization techniques and advanced configurations. In conclusion, this project successfully established Kali Linux in a virtual environment, providing a valuable resource for penetration testing and security auditing, and underscoring the importance of hands-on experience in cybersecurity education.

Plagiarism Report

