# PROJECT REPORT ON

"Introduction to Virtualization with VirtualBox "

**Submitted By:**

Amandeep Singh, UID- 24MCA20044

**Under The Guidance of:**

Mr. Navdeep Singh Sodhi

October, 2024


University Institute of Computing
Chandigarh University,
Mohali, Punjab

# CERTIFICATE

This is to certify that Amandeep Singh (UID-24MCA20044) have successfully completed the project title "Introduction to Virtualization with VirtualBox in Linux" at University Institute of Computing under my supervision and guidance in the fulfilment of requirements of first semester, Master of Computer Application-Specialization in General. Of Chandigarh University, Mohali, Punjab.

| | |
|---|---|
| Dr. Abdullah | Mr. Navdeep Singh Sodhi |
| Head of the Department | Project Guide Supervisor |
| University Institute of Computing | University Institute of Computing |

# ACKNOWLEDGEMENT

We deem it a pleasure to acknowledge our sense of gratitude to our project guide Mr. Navdeep Singh Sodhi under whom we have carried out the project work. His incisive and objective guidance and timely advice encouraged us with constant flow of energy to continue the work.

We wish to reciprocate in full measure the kindness shown by Dr. Abdullah (H.O.D, University Institute of Computing) who inspired us with his valuable suggestions in successfully completing the project work.

We shall remain grateful to Dr. Manisha Malhotra, Additional Director, University Institute of Technology, for providing us a strong academic atmosphere by enforcing strict discipline to do the project work with utmost concentration and dedication.

Finally, we must say that no height is ever achieved without some sacrifices made at some end and it is here where we owe our special debt to our parents and our friends for showing their generous love and care throughout the entire period of time.

Date: 24.10.2024

Place: Chandigarh University, Mohali, Punjab

Amandeep Singh
UID- 24MCA20044

# ABSTRACT

Virtualization is a critical technology in modern computing, enabling multiple operating systems (OS) to run simultaneously on a single hardware platform. This project, "Introduction to Virtualization with VirtualBox in Linux," explores the implementation and significance of virtualization using VirtualBox, an open-source, cross-platform virtualization software developed by Oracle. The focus of this project is on deploying Linux-based systems within VirtualBox to understand how virtualization functions and its applications in both development and testing environments.

The primary objective of this project is to demonstrate the process of setting up and configuring VirtualBox on a host machine, installing a Linux-based guest operating system (Kali Linux), and exploring its capabilities. The project outlines the steps required to create virtual environments, manage resources efficiently, and enable seamless interaction between the host and guest OS. By simulating different environments, developers and system administrators can optimize software performance, test multiple OS configurations, and deploy applications in isolated virtual environments without requiring separate physical machines.

This project underscores the benefits of virtualization, including hardware resource optimization, isolation, and flexibility, which are vital for businesses, developers, and system administrators. VirtualBox offers key features such as snapshot management, shared folders, and seamless mode, making it an ideal tool for creating portable and manageable virtual environments.

The project also highlights the significance of virtualization in areas like cloud computing, development, testing, and network security. By using VirtualBox and Linux together, users can harness the power of both technologies to create secure, scalable, and efficient virtual machines. This abstract provides a foundational overview of the practical aspects of virtualization with VirtualBox, demonstrating its potential for reducing costs, improving system efficiency, and enhancing software development workflows in Linux environments.

# Installation of Parrot

## 1. Introduction

Setting up and running virtual machines (VMs) has become a popular approach for users seeking isolated, secure environments to experiment with new operating systems, perform development work, or engage in tasks that require enhanced privacy and security. Virtual machines offer the flexibility of running different operating systems on a single computer, which enables users to experiment without impacting their primary setup. This guide is intended to provide step-by-step instructions on installing Parrot Linux within VirtualBox, a powerful and open-source virtualization tool.

By the end of this guide, users will have a fully functional Parrot Linux virtual machine, which they can use for tasks such as penetration testing, digital forensics, or privacy-focused browsing. This setup is particularly valuable for individuals in cybersecurity, IT professionals, and anyone interested in exploring security-focused tools within a safe, virtual environment.

### *Objective*

The main objective of this guide is to help users set up a Parrot Linux virtual machine in VirtualBox. VirtualBox, being free and open-source, is accessible to a wide range of users, making it a versatile choice for virtualization. Parrot Linux, a Debian-based distribution known for its emphasis on security and privacy, provides a suite of tools specifically designed for ethical hacking, forensics, and anonymity.

Using Parrot Linux in a virtualized environment offers several advantages:

- **Security and Isolation**: Running Parrot Linux as a virtual machine creates a contained environment that is isolated from the host system. This isolation provides a layer of security, as any potentially risky activities or malware within the virtual machine do not affect the main operating system.
- **Testing and Experimentation**: Virtualization enables users to explore different software, settings, and system configurations without the fear of damaging or misconfiguring the host OS.
- **Convenience and Flexibility**: VirtualBox allows users to easily pause, save, and revert the virtual machine state. This feature is particularly useful for users performing repeat tasks, as it lets them pick up where they left off without going through an extensive setup each time.

This guide will walk through each step of downloading and installing both VirtualBox and Parrot Linux, ensuring users can set up their virtual environment with confidence and ease. This setup is ideal for users who want to experiment with ethical hacking and digital forensics tools in a low-risk, self-contained system.

### *Background*

Virtualization has become a cornerstone technology in both personal and professional computing environments. Initially developed to maximize resource utilization in large-scale data centers, it has become a widely accessible tool for everyday users. VirtualBox, an open-source virtualization platform, provides users with the capability to run multiple guest operating systems on a single physical machine, known as the host. This flexibility makes it an excellent choice for running operating systems like Parrot.

**What is VirtualBox?**
Oracle VM VirtualBox is a popular open-source virtualization software that enables users to run different operating systems as virtual machines. This flexibility has made VirtualBox one of the most widely used virtualization tools globally, as it supports a variety of guest operating systems, including Linux distributions, Windows, and macOS. VirtualBox is cross-platform, meaning it can be installed on different host operating systems, including Windows, macOS, and Linux. Its accessibility, combined with an extensive set of features like snapshots, shared folders, and network management, makes it a suitable choice for users with varying technical expertise.

**What is Parrot Linux?**
Parrot Linux, sometimes called Parrot OS, is a Debian-based Linux distribution known for its emphasis on security, privacy, and development capabilities. It is widely used by cybersecurity professionals, ethical hackers, and researchers. Parrot Linux comes in different editions, including:

- **Parrot Security**: This edition includes a wide range of tools for penetration testing, digital forensics, and security auditing.
- **Parrot Home**: A lightweight edition aimed at general users who want a privacy-focused OS without the security tools.

Using Parrot Linux in a virtual machine allows users to access and utilize its powerful toolset without making any permanent changes to the host system. This setup is particularly advantageous for those who wish to practice ethical hacking or security analysis without compromising their primary OS.

**Why Use Parrot Linux in VirtualBox?**
There are several benefits to running Parrot Linux in a VirtualBox environment:

- **Enhanced Security**: By isolating Parrot Linux within a virtual machine, users reduce the risk of malicious software or potential exploits affecting their host system. This isolation is essential for security and privacy-focused tasks.
- **Risk-Free Experimentation**: Users can test various tools and configurations in a virtual environment without worrying about causing damage to their main OS. If an experiment fails, they can revert to an earlier snapshot or restart the virtual machine with minimal consequences.
- **Accessibility to Advanced Tools**: Parrot Linux includes pre-installed tools for ethical hacking, security audits, and forensics, allowing users to experiment with these tools without needing to install them manually.
- **Flexibility and Convenience**: VirtualBox's features like snapshots and easy backups give users flexibility. They can save a virtual machine's current state and return to it anytime, which is particularly useful during iterative testing or long-term projects.

In summary, running Parrot Linux in VirtualBox offers a secure, flexible, and cost-effective solution for exploring a security-focused operating system. By following this guide, users will gain a comprehensive understanding of the setup process and the necessary configurations for a smooth and functional Parrot Linux virtual machine experience. The following sections will detail system requirements, installation steps, and configurations, providing a thorough foundation for users to achieve a successful virtual environment setup.

## 2. System Requirements

- **2.1 Host System Requirements**: Describe the hardware and software specifications needed to run VirtualBox and Parrot Linux smoothly.
    - **CPU**: 64-bit processor with virtualization support (Intel VT-x or AMD-V).
    - **RAM**: Minimum 4 GB, recommended 8 GB or higher.
    - **Storage**: At least 20 GB free disk space.
    - **Operating System**: Host OS compatible with VirtualBox (e.g., Windows, macOS, or Linux).
    - **Graphics**: A graphics card that supports OpenGL if GUI performance is important.
- **2.2 Guest Operating System Requirements**: Define the specifications for Parrot Linux as a guest OS within the virtual machine.
    - **RAM**: Minimum 2 GB, recommended 4 GB or more.
    - **Storage**: 20 GB or more for the Parrot Linux virtual disk.
    - **CPU Allocation**: At least 2 cores (adjust based on host capacity).
- **2.3 Additional Software Requirements**: Identify any required software or VirtualBox extensions.
    - **VirtualBox Extension Pack**: This optional extension enables additional features like USB 2.0/3.0 support, disk encryption, and virtual network capabilities.
    - **VirtualBox Guest Additions** (to be installed after setting up Parrot Linux): Provides additional performance improvements and integration features, including clipboard sharing, drag-and-drop, and screen resolution adjustments.

## 3. Downloading and Installing VirtualBox

- **Step 1**: Go to the official VirtualBox website and navigate to the "Downloads" section.
- **Step 2**: Select the appropriate installer for your host operating system (e.g., Windows, macOS, or Linux).
- **Step 3**: Download and run the installer, following the prompts. Accept the default settings unless specific configurations are required.
- **Step 4**: After installation, open VirtualBox and verify that it runs correctly.
- **Optional**: Download and install the VirtualBox Extension Pack for added functionality.
- **Troubleshooting Tip**: Ensure your host system's virtualization support (Intel VT-x or AMD-V) is enabled in the BIOS/UEFI settings if VirtualBox fails to start or run smoothly.

## 4. Downloading Parrot

- **Step 1**: Visit the official Parrot OS website and go to the "Download" section.
- **Step 2**: Choose the appropriate Parrot Linux edition:
    - **Parrot Security**: Includes tools for penetration testing, forensics, and development.
    - **Parrot Home**: Lightweight version without security tools, ideal for general use.
- **Step 3**: Download the ISO file for your chosen version (e.g., 64-bit).
- **Note**: Verify the file integrity using the checksum provided on the website to ensure a secure and uncorrupted download.

## 5. Creating a Parrot Linux Virtual Machine

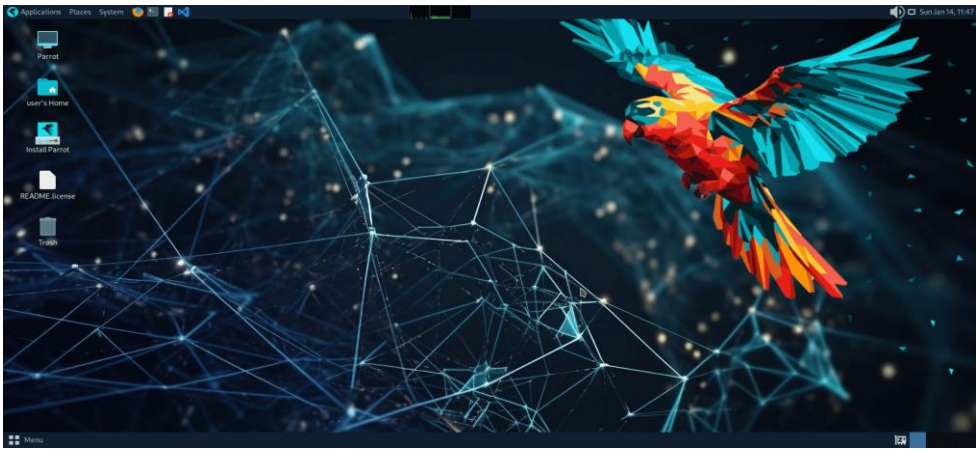
- **Step 1**: Open VirtualBox and click on "New" to create a new virtual machine.
- **Step 2**: Name the VM (e.g., "Parrot Linux") and select the "Linux" type with "Debian (64-bit)" as the version.
- **Step 3**: Allocate memory (RAM) to the VM:

    - **Recommended**: Assign at least 2 GB (2048 MB) for the VM, but 4 GB or more is preferable if the host system has enough RAM.
- **Step 4**: Configure the hard disk:
    - Choose "Create a virtual hard disk now" and select the "VDI (VirtualBox Disk Image)" format.
    - Opt for "Dynamically allocated" for flexible disk space management.
    - Set the disk size to at least 20 GB.
- **Step 5**: Customize additional settings:
    - **Processor**: Allocate 2 cores if possible.
    - **Display**: Increase video memory to at least 128 MB and enable 3D acceleration if required.
- **Step 6**: Insert the Parrot Linux ISO as the startup disk:
    - Go to "Settings" -> "Storage," click on the "Empty" disk icon, then click on the disk icon on the right and select "Choose a disk file" to browse for the downloaded Parrot ISO.

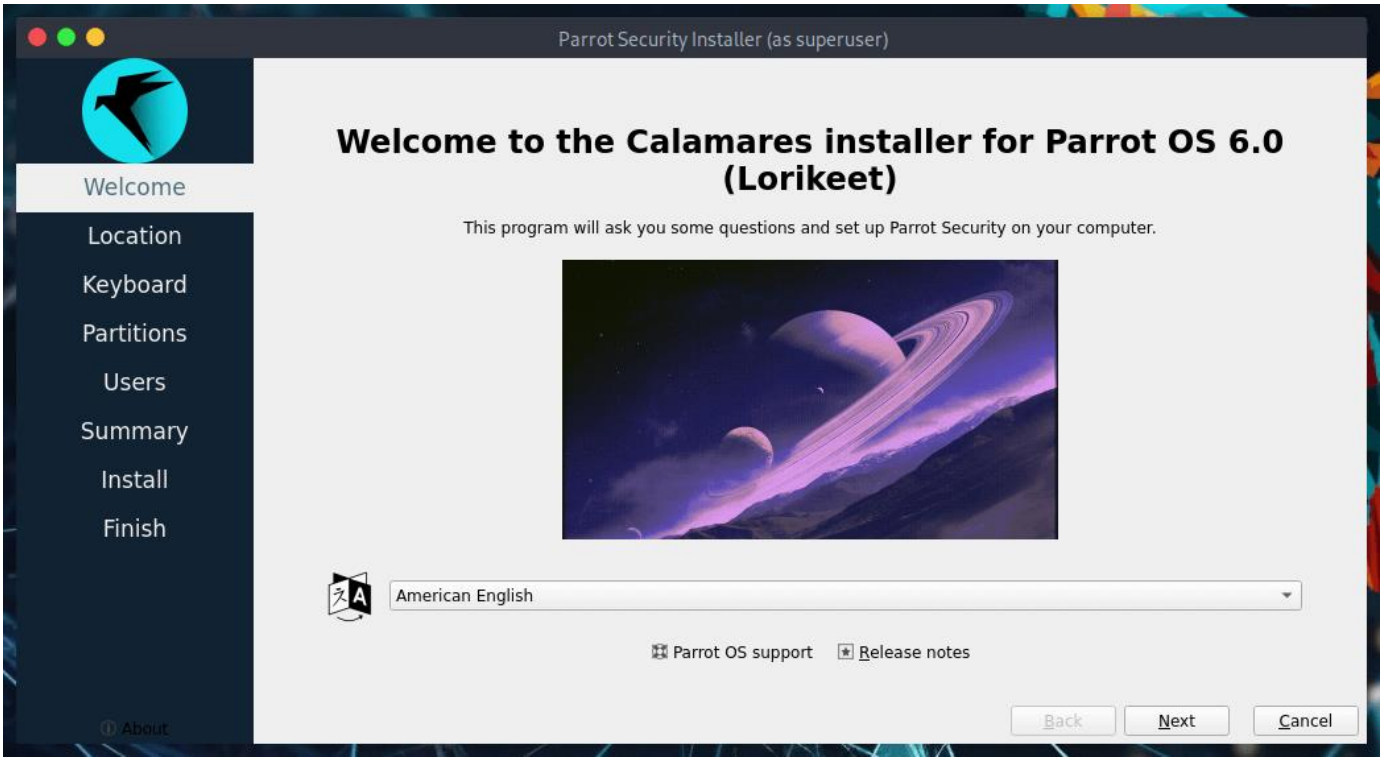
## 6. Installing Parrot Linux

- **Step 1**: Start the VM, which should boot from the Parrot ISO. Select "Install" or "Graphical Install" from the Parrot menu.
- **Step 2**: Follow the installation prompts:
    - **Language and Region Settings**: Select your preferred language, location, and keyboard layout.
    - **Partitioning**: Choose "Guided - use entire disk" if you're setting up a basic installation (no dual-boot required).
    - **Create User and Set Passwords**: Set up a root password and a regular user account with a password.
- **Step 3**: Finalize the installation by confirming settings and allowing the installation process to complete.
- **Step 4**: Remove the ISO image from the virtual disk to avoid booting into the installer again.
    - Go to "Settings" -> "Storage," select the ISO, and choose "Remove Disk from Virtual Drive."
- **Step 5**: Restart the VM to boot into Parrot Linux.

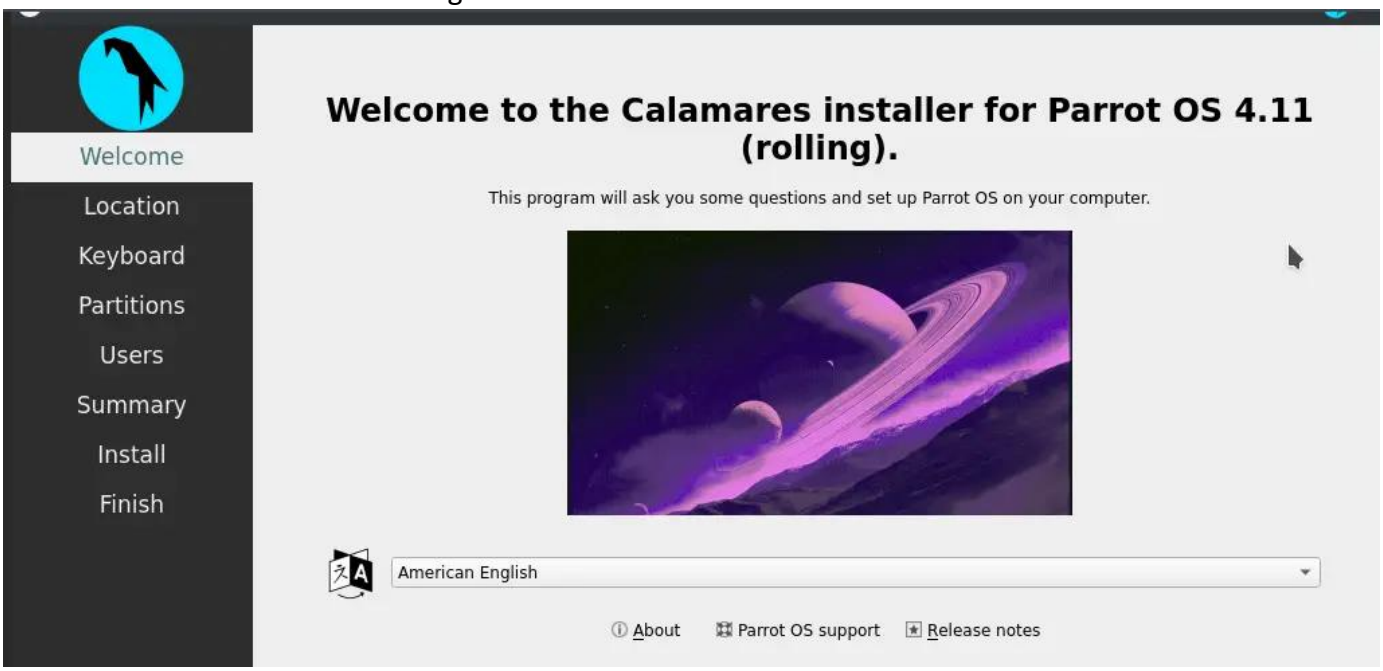
**1 Click on Install Parrot**



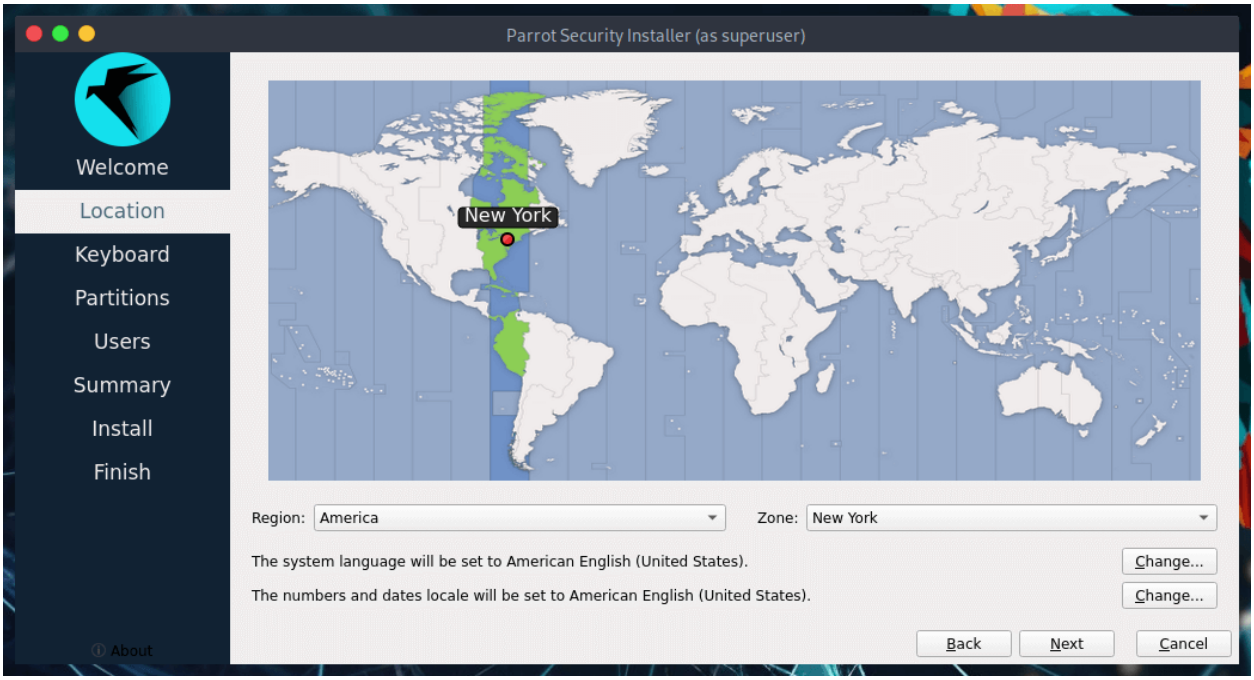

2 The next step is selecting the system's language. Choose your language and click on *Next*.



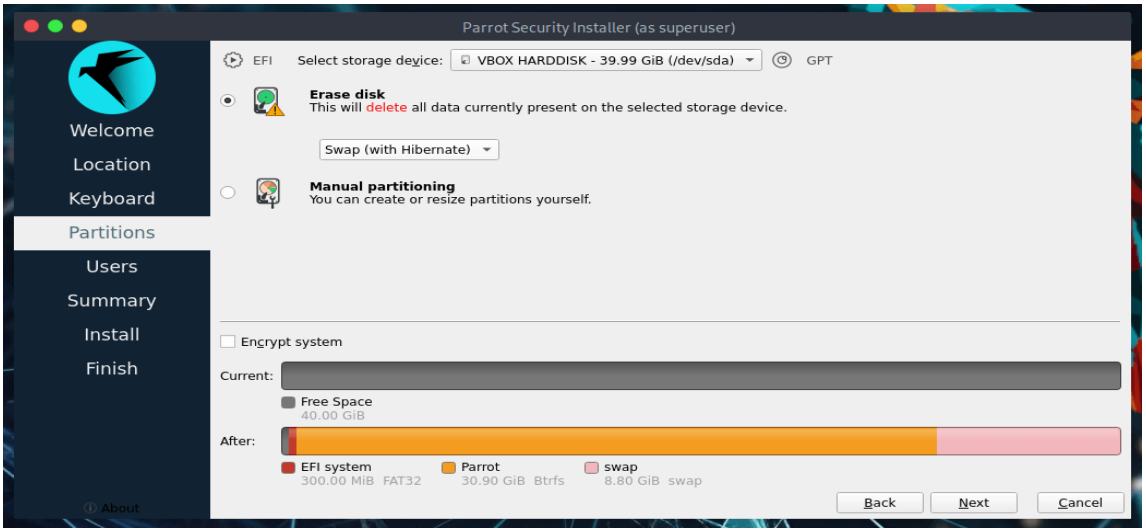

3. Download Process Starting



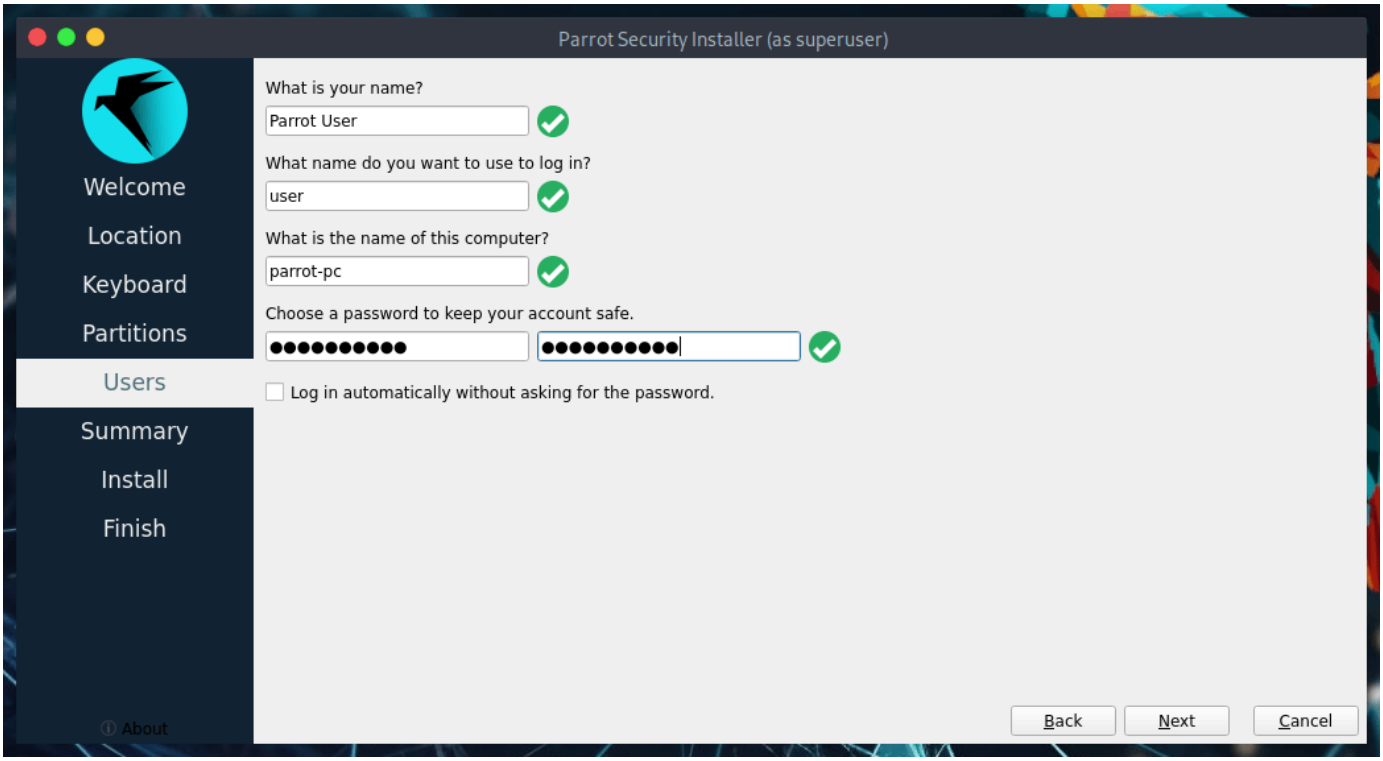

4. select your Region and Zone. Click on *Next*.




**5. disk partitioning**




Click next after creating your partitions and selecting the partition




**5. <u>Result:</u> Installation Successfully.**

## 7. **Conclusion**

This guide has provided a step-by-step walkthrough for setting up Parrot Linux in VirtualBox, allowing users to explore a secure and isolated environment on their host system. By following these instructions, users can install and configure Parrot Linux—a security-focused operating system—within VirtualBox, one of the most accessible and flexible virtualization platforms available today.

Completing this setup offers multiple benefits. First and foremost, it enables users to experiment with Parrot Linux's extensive suite of security tools, all while safeguarding the host operating system from potential risks. The isolation that VirtualBox provides is essential, particularly for users interested in learning or testing security techniques, as it minimizes the possibility of inadvertently affecting the main system. This setup is ideal for cybersecurity professionals, ethical hackers, developers, and privacy enthusiasts who need a reliable environment for safe experimentation.

With Parrot Linux running in a virtual machine, users now have access to a wide range of built-in tools for penetration testing, digital forensics, reverse engineering, and cryptography. The virtualized environment allows users to confidently experiment with these tools, knowing that they can revert to a previous state or restore the VM from a snapshot if needed. This flexibility not only enhances learning opportunities but also encourages exploration without fear of permanent damage to the system.

### Next Steps for Exploration

For users who have successfully set up Parrot Linux in VirtualBox, there are several ways to enhance their knowledge and utilize VirtualBox's and Parrot Linux's full potential:

1. **Explore Additional VirtualBox Features**: VirtualBox offers various advanced settings, such as shared folders, USB passthrough, and network bridging, which can increase interaction between the host and guest systems. Users can try configuring shared folders to transfer files easily or experimenting with different network configurations to simulate various network environments.
2. **Learn to Use VirtualBox Snapshots**: Snapshots allow users to save the current state of the virtual machine and return to it at any point. This feature is incredibly useful when testing security tools or settings, as users can easily revert to a previous configuration if an experiment causes unexpected issues.
3. **Install VirtualBox Guest Additions**: VirtualBox Guest Additions can improve performance and usability by enabling features like full-screen mode, clipboard sharing, and seamless mouse integration. This enhancement makes working with Parrot Linux in a virtual machine smoother and more efficient.
4. **Explore Parrot Linux Security Tools**: Parrot Linux includes a variety of pre-installed tools for security assessments, ethical hacking, and forensics. Beginners can start by exploring familiar tools like Nmap for network scanning or Metasploit for vulnerability testing, while advanced users may dive into reverse engineering or digital forensics.
5. **Practice Setting Up a Virtual Network**: VirtualBox allows users to create multiple VMs and connect them within a virtual network. This setup can be valuable for practicing penetration testing in a controlled, lab-like environment. By adding other virtual machines to this network, users can simulate multi-host environments and learn how to analyze network traffic, discover vulnerabilities, and secure communication between machines.
6. **Experiment with Custom Configurations and Scripts**: Once comfortable with Parrot Linux, users can start experimenting with custom configurations and scripts. For example, setting up automated security checks, custom firewall rules, or logging configurations can offer valuable practice in managing and securing a Linux system.

## Final Thoughts

Setting up Parrot Linux in VirtualBox provides users with a secure, versatile sandbox for exploring cybersecurity and privacy-focused tasks. The virtualization setup outlined in this guide serves as a reliable foundation for learning and experimenting with advanced tools and techniques in a risk-free environment. This experience will be especially beneficial for those pursuing cybersecurity careers, enabling them to hone practical skills without impacting their primary system.

Overall, this setup empowers users to fully leverage the capabilities of Parrot Linux and VirtualBox to deepen their understanding of security practices. As users grow more comfortable, they can continue to expand their virtualized environment, experiment with new tools, and build increasingly complex and secure configurations. Whether for personal interest, professional development, or academic study, this virtual environment offers a safe and practical approach to developing cybersecurity skills.