BAHIRDAR UNIVERSITY

BAHIRDAR INSTITUTE OF TECHNOLOGY

FACULTYOFCOMPUTING

OPERATINIG SYSTEM AND SYSTEM PROGRAMMING

INDIVIDUAL ASSIGNMENT

BACKBOX LINUX OS

NAME- Gishenawit Ayenew Hagos

ID-BDU1601617

Submitted to-Wendimu Baye
Submitted Date 16/08/17 EC

Tableofcontents

Installation of Backbox linux Operating System in Virtual Environment Tools

A. Introduction (Background, Motivation)

BackBox Linux is a specialized Ubuntu-based operating system designed for security assessments, penetration testing, and forensic analysis. Built with efficiency, lightweight performance, and simplicity in mind, it provides a robust platform for professionals and students interested in cybersecurity domains. Its tool-rich environment is aligned with open-source values and continues to support industry-standard technologies with long-term reliability.

The prime motive to employ BackBox Linux within a virtual environment, such as VMware Workstation or Oracle VM VirtualBox, originates from the constantly increasing demand to be able to perform ethical hacking and system testing within an isolated and secure test lab.

Virtualization offers a platform for developers and students to execute scripts, call system-level calls (like unlink() for file or symbolic link deletion) and examine system internals without any impact on the host system. This functionality is especially important when learning file manipulation at the system-call level, testing command-line tools, and learning fundamental UNIX concepts such as permissions, symbolic linking, and process control.

Furthermore, working with a virtualized BackBox Linux setup enables students to delve into solid Linux aspects such as shell scripting along with POSIX-standard-compliant functionality while gaining practical exposure to standardized UNIX behavior in a live, hands-on setting.

B.Objectives

The main aims of this project include:

1. To effectively install and configure BackBox Linux on a virtual environment

This project intends to illustrate a full and working installation of BackBox Linux through software such as VMware Workstation or Oracle VM VirtualBox, with compatibility on current virtualization systems.

2. To comprehend the relevance of virtualization in learning operating systems

Virtual machines offer a sandbox environment ideal for testing system-level activities without risking the host machine. Virtualization is emphasized in this project as a valuable

development and teaching aid.

3. **To understand UNIX/Linux system calls and system commands**

One of the main concerns is to comprehend and utilize commands such as unlink(), which makes it possible to delete files or symbolic links from the file system. This directly relates to acquiring knowledge about the functions behind the Linux kernel and file system setup.

4. **To improve technical competence with open-source penetration testing tools.**

BackBox is a collection of cybersecurity utilities. Running and installing it in a VM allows students to get practical experience with professional-level tools in a safe environment.

5. **To adhere to UNIX standardization guidelines for compatibility and portability**

By working within a POSIX-compliant environment like BackBox Linux, the project allows for a better appreciation of how standardization ensures cross-platform compatibility and consistent command behavior.

C. Requirements

i. Hardware Requirements

To run BackBox Linux smoothly in a virtual environment, the host machine should meet the following minimum hardware specifications:

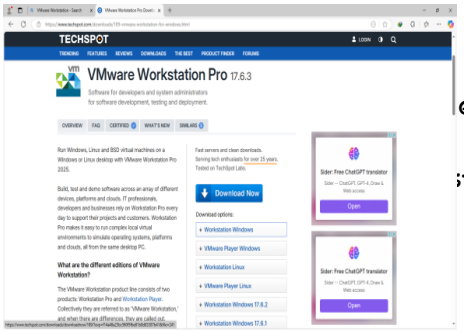
- **Processor:**
  Intel or AMD dual-core processor (64-bit support required)
  Recommended: Quad-core or higher for better virtualization performance
- **Memory (RAM):**
  Minimum: 2 GB
  Recommended: 4 GB or more (especially when running additional tools within BackBox)
- **Hard Disk Space:**
  Minimum: 20 GB of free disk space
  Recommended: 40 GB or more (to accommodate updates, tools, and snapshots)
- **Graphics:**
  Any standard graphics adapter that supports virtualization UI rendering (VMware/VirtualBox)
- **Virtualization Support:**
  Ensure **VT-x** (Intel) or **AMD-V** (AMD) is enabled in BIOS/UEFI for optimal performance

ii. Software Requirements

- **Host Operating System:**

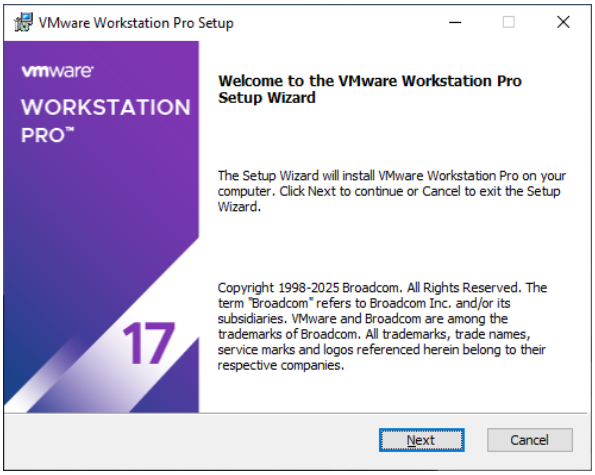
Windows, macOS, or any Linux distribution that supports VirtualBox or VMware

- **Virtualization Software (Choose one):**
  - **Oracle VM VirtualBox** (Free and open-source)
  - **VMware Workstation Player** (Free for personal use)
  - Any other virtualization tool with ISO boot support
- **BackBox Linux ISO:**
  - Official ISO image of the latest supported version
  - Can be downloaded from: https://www.backbox.org/download
- **(Optional) Guest Additions / VMware Tools:**
  For enhanced VM integration features such as drag-and-drop, clipboard sharing, and screen resizing.

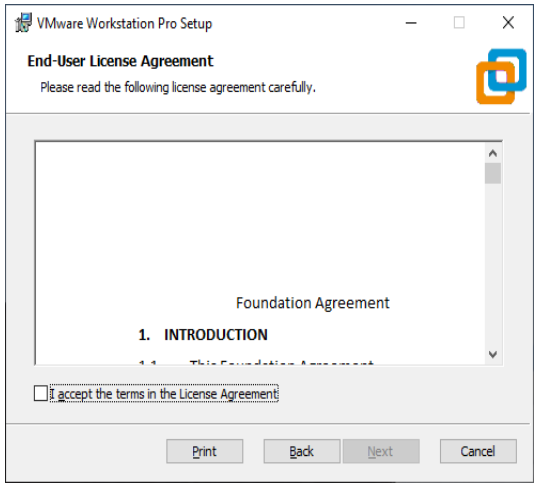


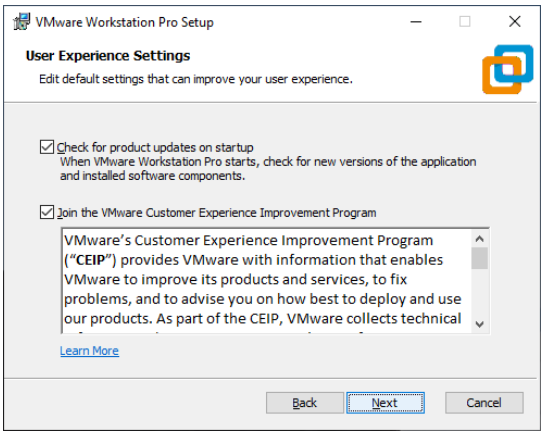
ed VMware virtual environment .so the first step is

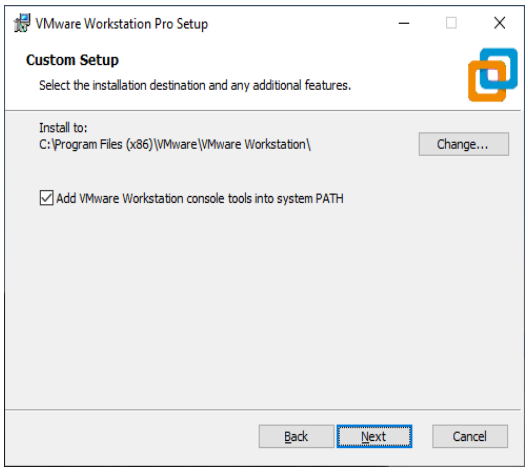
station

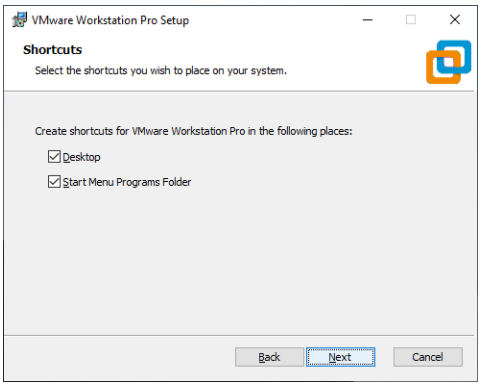


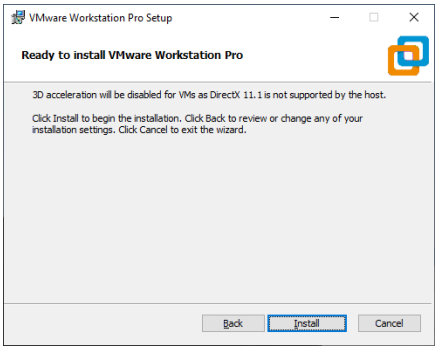
->

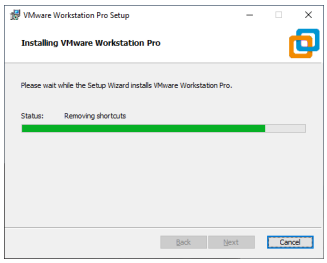


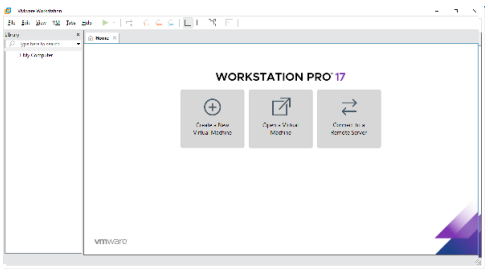

VMware Workstation Pro Setup
User Experience Settings
Edit default settings that can improve your user experience.
Check for product updates on startup
When VMware Workstation Pro starts, check for new versions of the application and installed software components.
Join the VMware Customer Experience Improvement Program
VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical
Learn More
Back
Next
Cancel


VMware Workstation Pro Setup
Custom Setup
Select the installation destination and any additional features.
Install to:
C:\Program Files (x86)\VMware\VMware Workstation\
Change...
Add VMware Workstation console tools into system PATH
Back
Next
Cancel

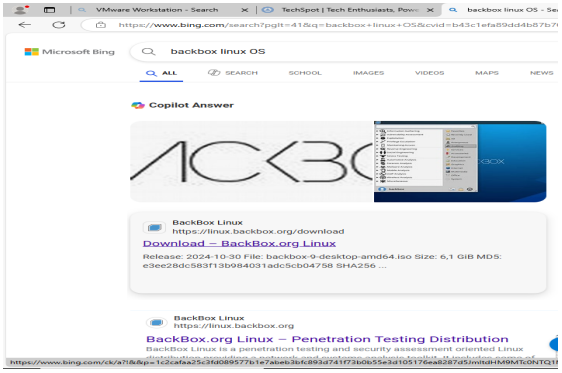

VMware Workstation Pro Setup
Shortcuts
Select the shortcuts you wish to place on your system.
Create shortcuts for VMware Workstation Pro in the following places:
Desktop
Start Menu Programs Folder
Back
Next
Cancel


VMware Workstation Pro Setup
Ready to install VMware Workstation Pro
3D acceleration will be disabled for VMs as DirectX 11.1 is not supported by the host.
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

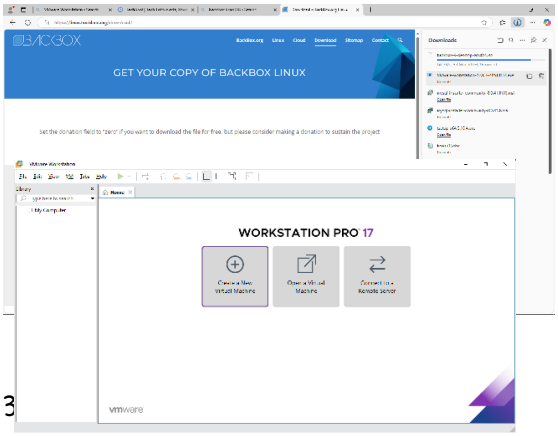

VMware Workstation Pro Setup
Installing VMware Workstation Pro
Please wait while the Setup Wizard installs VMware Workstation Pro.
Status: Removing shortcuts
Back
Next
Cancel


WORKSTATION PRO 17
vmware

2 .download backbox linux OS

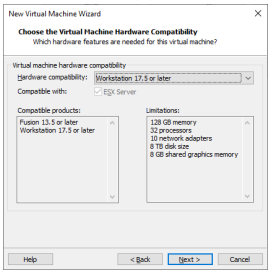


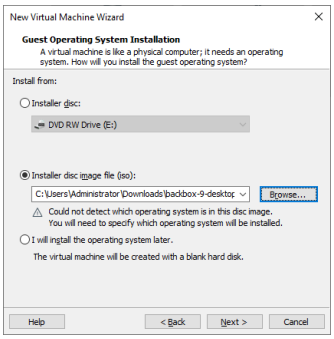
We select backbox.org linux then we download it

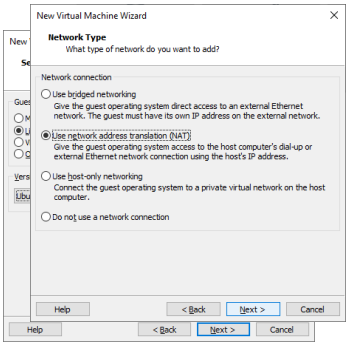


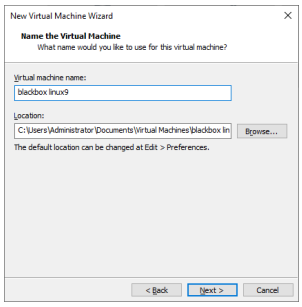
3

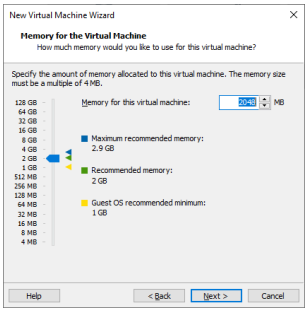
We choose create a new virtual machine then

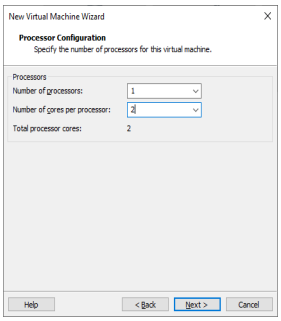


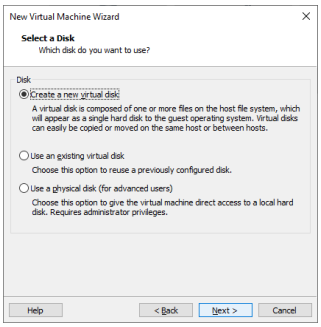




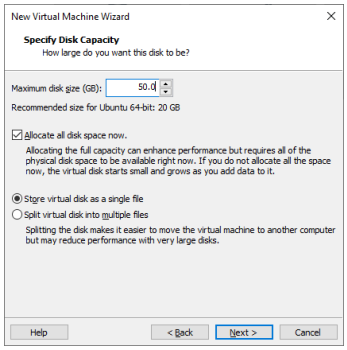


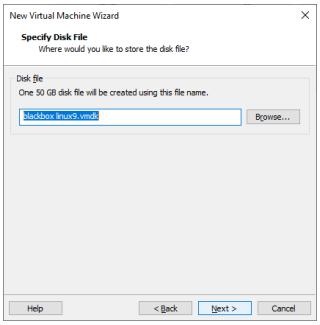




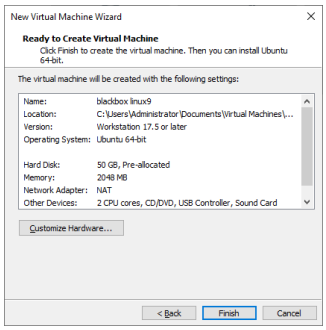

New Virtual Machine Wizard
Select a Disk
Which disk do you want to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.
Help
< Back
Next >
Cancel

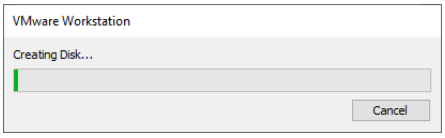
->


New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB): 50.0
Recommended size for Ubuntu 64-bit: 20 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

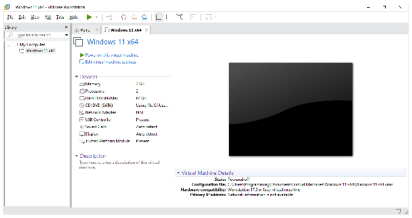

New Virtual Machine Wizard
Specify Disk File
Where would you like to store the disk file?
Disk file
One 50 GB disk file will be created using this file name.
blackbox linux9.vmdk
Browse...
Help
< Back
Next >
Cancel

->

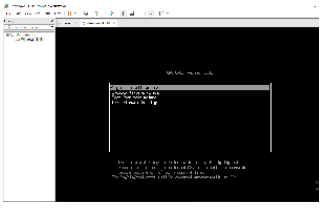

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Ubuntu 64-bit.
The virtual machine will be created with the following settings:
Name: blackbox linux9
Location: C:\Users\Administrator\Documents\Virtual Machines\...
Version: Workstation 17.5 or later
Operating System: Ubuntu 64-bit
Hard Disk: 50 GB, Pre-allocated
Memory: 2048 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Sound Card
Customize Hardware...
< Back
Finish
Cancel


VMware Workstation
Creating Disk...
Cancel

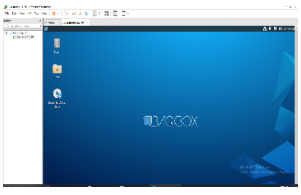
then ->

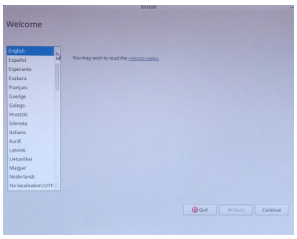


->

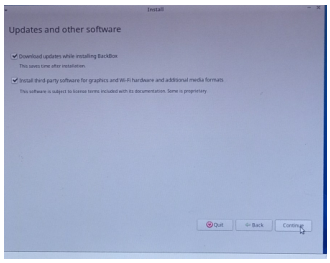


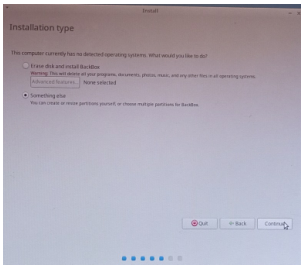
->



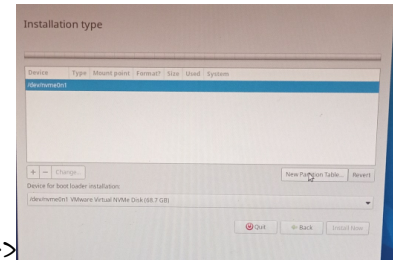

Welcome

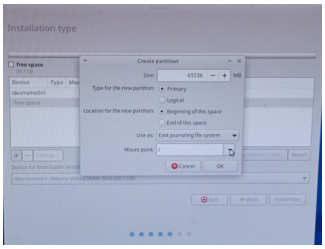
->


Updates and other software

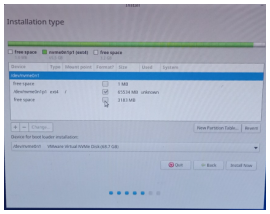

Installation type

->

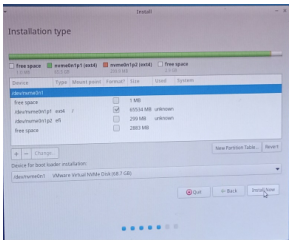

Installation type

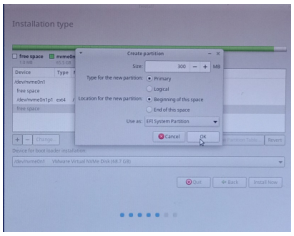

Installation type

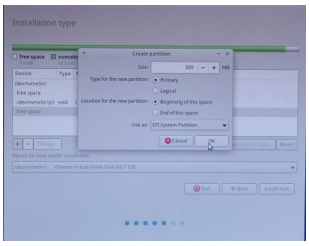
->

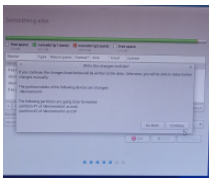

Installation type

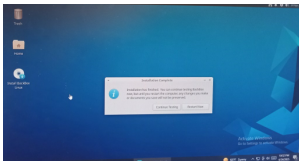
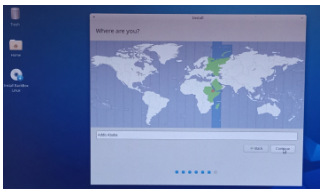
->

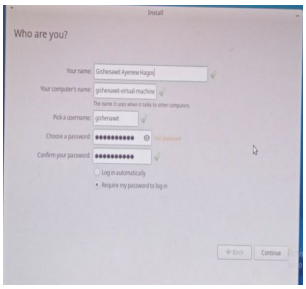

Installation type

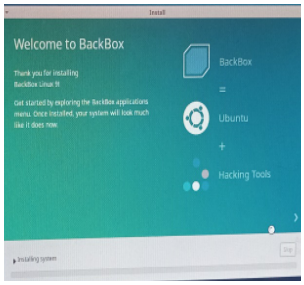

Installation type

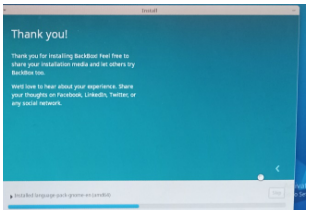


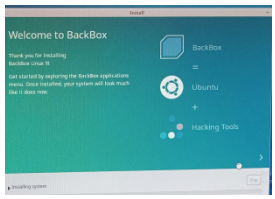
->



->




->




->


E. Issues (Problem Faced)

i. Virtualization Not Enabled

- **Problem:**
  Installation did not proceed, or VM was very slow.
- **Cause:**
  Hardware virtualization (VT-x/AMD-V) was not enabled in BIOS/UEFI.

ii. No Bootable Medium Found

- **Problem:**
  VM could not detect the BackBox Linux ISO file on startup.
- **Cause:**
  ISO was not properly attached to the virtual machine.

iii. Slow Performance

- **Problem:**
  BackBox ran very slowly during installation or use.
- **Cause:**
  Limited RAM/CPU cores assigned to VM.

iv. Screen Resolution Issues

- **Problem:**
  Display stuck at low resolution inside the VM.
- **Cause:**
  Missing Guest Additions/VMware Tools.

v. Network Configuration Errors

- **Problem:**
  No internet connection inside the virtual machine.
- **Cause:**
  Network adapter not set to NAT or Bridged mode.

F. Solution

Below are the solutions applied to resolve the issues encountered during the installation and setup of BackBox Linux in the virtual environment

i. Virtualization Not Enabled

- **Solution:**
  Accessed the BIOS/UEFI settings by pressing the appropriate key during system boot (e.g., F2, DEL, ESC). Enabled the **VT-x (Intel)** or **AMD-V (AMD)** option under "Advanced" or "CPU Configuration." Saved and exited BIOS, then restarted the system.

ii. No Bootable Medium Found

- **Solution:**
  Opened the virtual machine settings, navigated to **Storage**, and made sure the **BackBox Linux ISO file** was properly mounted to the **Optical Drive**. Then restarted the VM and confirmed that the ISO booted correctly.

iii. Slow Performance

- **Solution:**
  Shut down the virtual machine. Allocated more resources in the VM settings:
  - Increased RAM to **4 GB**
  - Assigned **2 CPU cores**
  - Enabled **3D acceleration** for improved graphics performance (if supported) This provided smoother performance during both installation and usage.

iv. Screen Resolution Issues

- **Solution:**
  After installation, installed **Guest Additions** (VirtualBox) or **VMware Tools** (VMware Workstation). These tools improved display resolution, mouse integration, and clipboard sharing.

v. Network Configuration Errors

- **Solution:**
  Adjusted the network settings in VM configuration:
  - Set the network adapter mode to **NAT** to allow internet access through the host system
  - Verified connectivity using `ping google.com` and updated system packages via `sudo apt update`

G. Filesystem Support

BackBox Linux supports various filesystems, with ext4 being the default and most recommended. Here's a summary:

Filesystem	Supported in BackBox Linux?	Purpose & Reason for Use
ext4	✅ Yes (Default)	Most widely used and recommended Linux filesystem. Offers excellent performance, reliability, and journaling support. Ideal for BackBox installations.
Btrfs	✅ Yes	Advanced filesystem with snapshot and self-healing features. Good for experimentation but more complex to manage than ext4.
ZFS	✅ Yes (via manual setup)	High-end, enterprise-grade filesystem. Offers data integrity, compression, and volume management. Requires more resources and is overkill for basic VM setups.
NTFS	✅ Yes (Read/Write support)	Native to Windows. Useful for shared folders between Windows host and Linux VM. Not ideal for root or boot partitions.
FAT32	✅ Yes	Very old but widely compatible. Used for USB drives or EFI boot partitions, not recommended for large files or Linux installs.
exFAT	✅ Yes (after installing exfat-utils)	Suitable for large file support on USB drives. Useful for interoperability with Windows/macOS.
HFS+	🟡 Partially (Read-only or via third-party tools)	macOS filesystem. Not natively used in Linux environments. Limited support.
APFS	❌ No (Very limited support)	Apple's latest filesystem. No reliable read/write support in Linux environments. Not practical for BackBox usage.

Recommended filesystem for installation:

 ext4 is the best choice for installing BackBox Linux. It is stable, fast, and fully supported by all Linux distributions.

 For advanced users or research purposes, **Btrfs** or **ZFS** can be explored, especially in security or forensic analysis scenarios due to their snapshot and rollback features.

H. Advantages and Disadvantages

Advantages

1. **Lightweight and Fast**
   BackBox Linux is designed with efficiency in mind. It consumes minimal system resources, which makes it ideal for virtual environments. The lightweight nature allows it to run smoothly even on lower-end hardware when configured properly.

2. **Comprehensive Security Tools**
   BackBox is equipped with a wide range of tools for penetration testing, digital forensics, and vulnerability assessments. This makes it an excellent choice for security professionals and students who want to explore and practice cybersecurity techniques.
3. **Open Source and Free**
   As an open-source Linux distribution, BackBox Linux is completely free to use, modify, and distribute. This makes it accessible for anyone, from students to professionals, without worrying about licensing costs.
4. **Compatibility with Virtualization Platforms**
   BackBox works well on popular virtualization platforms like VMware Workstation and Oracle VirtualBox. It allows users to test various tools and systems without the need for a dedicated physical machine.
5. **Built on Ubuntu**
   Since BackBox Linux is based on Ubuntu, it benefits from Ubuntu's stability, ease of use, and compatibility with a wide range of software packages. Users familiar with Ubuntu will find BackBox easier to adopt.

Disadvantages

1. **Not Fully Compatible with All Hardware**
   Although BackBox Linux supports a wide range of hardware, like any Linux distribution, it may encounter compatibility issues with very new or proprietary hardware (e.g., some wireless network cards or graphics cards). In a virtualized environment, hardware support is typically more limited.
2. **Requires Adequate Resources for Best Performance**
   While BackBox is lightweight, running it in a virtual machine still requires a reasonable amount of RAM and CPU resources for optimal performance, especially when running multiple security tools. Limited resources may hinder the VM's responsiveness.
3. **Learning Curve for New Users**
   For users who are new to Linux, there may be a steeper learning curve compared to using a Windows-based environment. Tasks such as command-line configuration, troubleshooting, and system management can be challenging for beginners.
4. **Limited Support for Non-Technical Use**
   BackBox Linux is primarily designed for penetration testing and security professionals. While it can be used as a general-purpose OS, it's not as polished or user-friendly as distributions like Ubuntu or Fedora for general use cases like office work or multimedia.
5. **Possible Virtualization Overhead**
   Running BackBox Linux in a virtualized environment introduces some overhead. The VM needs to share host resources like CPU, RAM, and disk space, which can degrade performance compared to running directly on physical hardware.

I. Conclusion

In conclusion, installing **BackBox Linux** in a virtualized environment offers a highly effective and accessible platform for those interested in cybersecurity, penetration testing, and digital forensics. With its lightweight nature, robust set of tools, and compatibility with virtualization platforms like VMware Workstation and Oracle VirtualBox, it provides an ideal environment for both learning and

professional exploration of security concepts.

While BackBox Linux is tailored for advanced users in the security field, its Ubuntu foundation ensures that it remains approachable for individuals with basic Linux knowledge. Virtualization adds the additional benefit of testing without the risks of affecting the host machine, making it an excellent choice for experimentation.

However, the installation and use of BackBox in a virtual environment are not without challenges. Users may encounter issues related to hardware compatibility, system performance, and configuration during setup. These challenges can be easily mitigated with proper system resource allocation and by following the correct installation steps.

Ultimately, BackBox Linux, when paired with the flexibility and isolation offered by virtualization, provides a secure, versatile, and powerful platform for anyone looking to enhance their skills in the fields of ethical hacking and system analysis.

J. Future Outlook / Recommendation

The future of **BackBox Linux** and its role in virtualized environments appears promising, especially as the fields of cybersecurity and ethical hacking continue to grow. Here are some key aspects for future development and recommendations for users:

1. Increased Integration with Cloud Platforms

As cloud computing becomes more widespread, there is an increasing demand for virtualized environments that support multi-platform, cloud-based penetration testing tools. Future versions of BackBox Linux may benefit from closer integration with cloud service providers such as AWS, Google Cloud, and Azure, offering more powerful virtual environments for security assessments.

2. Expanded Toolset and Documentation

To maintain its relevance in the ever-evolving landscape of cybersecurity, BackBox Linux could expand its collection of pre-installed tools, including support for newer technologies like containerization (Docker), blockchain security, and artificial intelligence (AI)-driven penetration testing tools. Improved documentation and tutorials would also help make the OS more accessible to beginners and intermediate users.

3. Enhanced User Experience (UX) and Graphical Interface

While BackBox Linux excels in command-line-based tools, it could benefit from an enhanced graphical user interface (GUI) for a more seamless experience for users transitioning from other

operating systems like Windows or macOS. Simplifying the installation and setup processes, particularly for new users, could help attract a broader user base.

4. Better Hardware Compatibility and Optimization

As technology advances, it's essential for BackBox Linux to continuously improve hardware compatibility, especially with emerging technologies like new wireless chips, GPUs, and processors. As virtual machines become more common, providing optimized settings for VM environments could improve performance and user experience.

5. Increasing Role in Educational Institutions

Given its open-source nature and its focus on cybersecurity, BackBox Linux has the potential to become a staple in educational environments. Schools, universities, and training centers focused on ethical hacking and cybersecurity can adopt BackBox as a key tool in their curricula. Offering certified courses or official training programs could expand its use in academic and professional training sectors.

6. Encouragement of Community Contributions

As an open-source project, BackBox Linux will continue to thrive through community contributions. Encouraging more collaboration from the cybersecurity community will help to maintain and enhance its toolset, security features, and overall functionality. Active community-driven development could result in a more diverse set of tools and improvements in BackBox's capabilities.

What is Virtualization in Modern Operating Systems?

Virtualization is the process of creating a virtual (rather than physical) version of something, such as a virtual machine (VM), storage device, or network resource. In modern operating systems, virtualization refers specifically to the creation and management of virtual machines (VMs) on a physical machine (host). These VMs run their own independent operating systems (guest OS), which can be different from the host OS.

For example, in a virtualized environment, you can run Windows and Linux on the same physical machine, each in its own VM.

Why is Virtualization Used?

1. **Resource Efficiency**
   Virtualization allows multiple operating systems to share the resources of a single

physical machine. This maximizes resource utilization by ensuring that the hardware is used efficiently without requiring dedicated physical machines for each operating system.

2. **Isolation and Security**
   Virtual machines are isolated from each other. If one VM crashes or is compromised, the others are unaffected, which provides an extra layer of security. This isolation is also beneficial for testing and development.
3. **Cost Savings**
   Virtualization reduces the need for physical hardware, which lowers capital expenditure and maintenance costs. Organizations can consolidate multiple servers onto fewer physical machines, reducing space, power, and cooling requirements.
4. **Flexibility and Portability**
   Virtual machines can be easily migrated, cloned, or replicated across different hardware or cloud environments. This flexibility is especially useful in development, testing, and disaster recovery.
5. **Simplified Management**
   Virtualization software provides powerful management tools that allow IT administrators to deploy, monitor, and manage VMs with ease, offering features like snapshots, backups, and automated provisioning.

How Does Virtualization Work in Modern Operating Systems?

1. **Hypervisor (Virtual Machine Monitor)**
   At the core of virtualization is the **hypervisor**, which is responsible for managing the VMs. There are two types of hypervisors:
   - **Type 1 Hypervisor** (bare-metal): Runs directly on the host machine's hardware (e.g., VMware ESXi, Microsoft Hyper-V).
   - **Type 2 Hypervisor** (hosted): Runs on top of the host operating system (e.g., Oracle VirtualBox, VMware Workstation).
2. **Virtual Machines**
   A **virtual machine** is a software-based emulation of a physical computer. Each VM has its own virtual hardware (CPU, memory, storage, network interfaces) provided by the hypervisor, and it runs its own operating system, known as the **guest OS**.
3. **Virtualization Layer**
   The hypervisor creates a virtualization layer that separates the physical hardware from the VMs. This layer allocates resources to the VMs and ensures they can run independently without interfering with one another.
4. **Guest OS**
   Each virtual machine can run a different guest operating system, which is installed on top of the virtualized hardware. The guest OS operates as if it were running on a physical machine, unaware of the virtualization layer beneath it.

In summary, **virtualization** in modern operating systems enables efficient use of hardware, better security, and greater flexibility by allowing multiple isolated environments to run on a single physical machine. It is widely used in data centers, cloud computing, and development/testing environments.

REFERENCE

https://www.techspot.com

https://backbox.org

https://www.ibm.com:WhatIsVirtualization?

https://www.geeksforgeeks.org:Virtualization

THANKYOU!!!