



BAHIR DAR INSTITUTE OF TECHNOLOGY

FACULTY OF COMPUTING

DEPARTMENT OF INFORMATION SYSTEM

Operating System(OS)

PREPARED BY: TESHOME BIZUAYEHU

ID NUMBER: 1602560

Submitted to: Lec.Alemitu

Submission date: 11/05/2018

BAHIRDAR, ETHIOPIA

1. Installation of Parrot OS Security Edition 2026 in a Virtual Environment

a. Introduction (Background and Motivation)

Virtualization technology allows multiple operating systems to run on a single physical machine by abstracting hardware resources. Tools such as Oracle VM Virtual Box and VMware Workstation are widely used in education, research, and cybersecurity training because they provide isolated and flexible environments.

Parrot Security Edition 2026 is a Linux-based operating system designed for penetration testing, digital forensics, reverse engineering, and privacy protection. Installing Parrot OS in a virtual environment enables safe experimentation with security tools without affecting the host operating system.

The motivation for this project is to gain practical experience in virtualization, understand Linux installation processes, and resolve real-world technical issues encountered during OS deployment.

b. Objectives

The objectives of this project are:

- To install Parrot Security Edition 2026 in a virtual environment
- To configure Oracle VM Virtual Box correctly for Linux installation
- To identify and troubleshoot installation and system-level issues
- To document challenges and solutions in a structured manner
- To understand file system choices and virtualization benefits

c. Requirements

i. *Hardware Requirements*

Component	Minimum Requirement	Used
Processor	Intel CPU with VT-x support	Intel CPU
RAM	2 GB	4 GB
Storage	32 GB free disk space	35 GB
System	64-bit architecture	64-bit

ii. **Software Requirements**

- Host OS: Windows 10 (64-bit)
- Virtualization Tool: Oracle VM VirtualBox (latest version)
- Guest OS ISO: Parrot Security Edition 2026 (64-bit)
- BIOS Feature: Intel Virtualization Technology (VT-x) enabled

d. Installation Steps

Step 1: Install Oracle VM VirtualBox

Download VirtualBox from the official Oracle website

Install using default settings

Restart the system if required

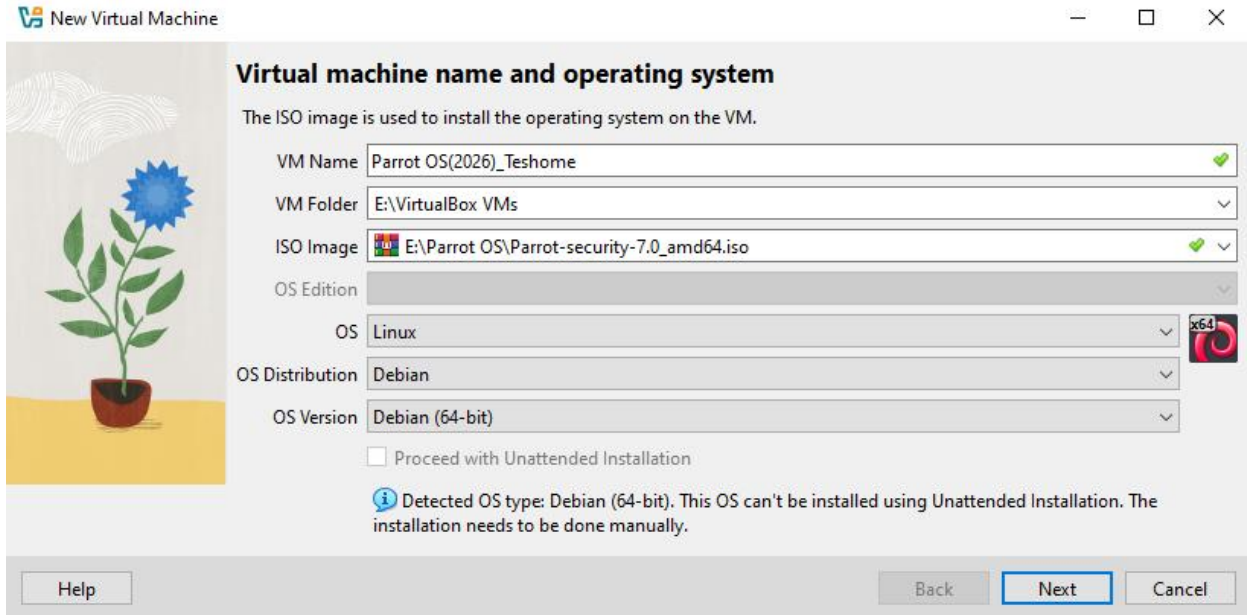
Step 2: Create a New Virtual Machine

Open VirtualBox → Click New

Name: Parrot OS(2026)_Teshome

Type: Linux

Version: Debian (64-bit)



Virtual machine name and operating system

The ISO image is used to install the operating system on the VM.

VM Name: Parrot OS(2026)_Teshome

VM Folder: E:\VirtualBox VMs

ISO Image: E:\Parrot OS\Parrot-security-7.0_amd64.iso

OS Edition:

OS: Linux

OS Distribution: Debian

OS Version: Debian (64-bit)

☐ Proceed with Unattended Installation

Detected OS type: Debian (64-bit). This OS can't be installed using Unattended Installation. The installation needs to be done manually.

Buttons: Help, Back, Next, Cancel

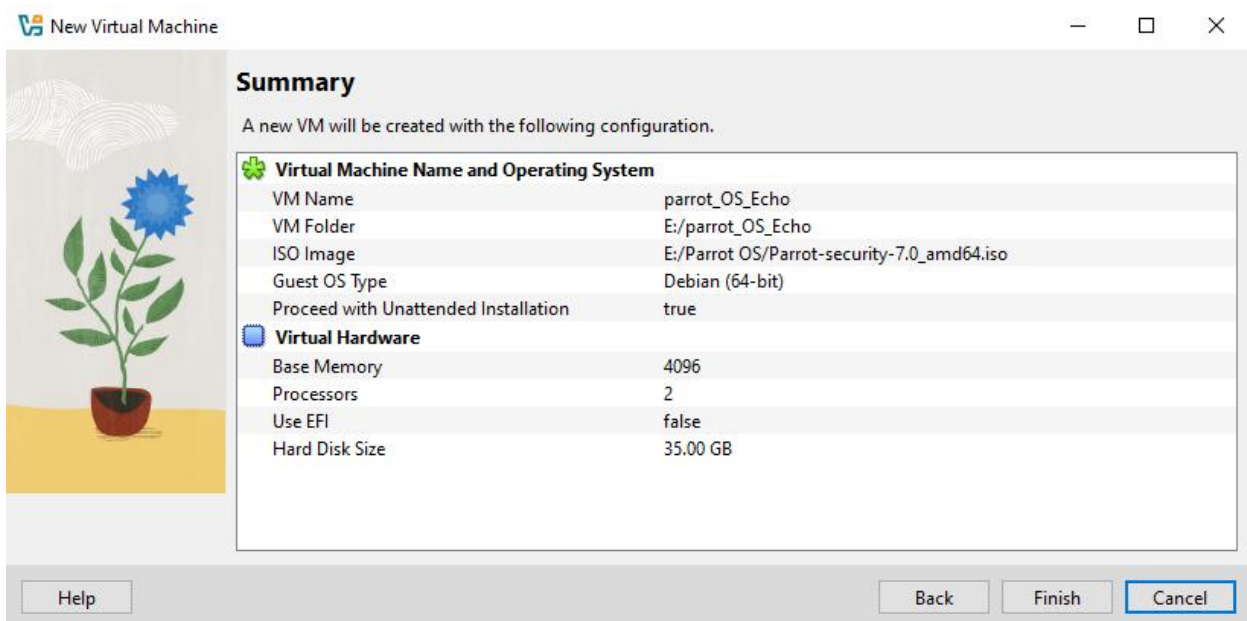
Step 3: Allocate Resources

RAM: 4096 MB

CPU: 2 cores

Virtual Disk: VDI, dynamically allocated

Disk Size: 35 GB



Summary

A new VM will be created with the following configuration.

Virtual Machine Name and Operating System	
VM Name	parrot_OS_Echo
VM Folder	E:/parrot_OS_Echo
ISO Image	E:/Parrot OS/Parrot-security-7.0_amd64.iso
Guest OS Type	Debian (64-bit)
Proceed with Unattended Installation	true
Virtual Hardware	
Base Memory	4096
Processors	2
Use EFI	false
Hard Disk Size	35.00 GB

Buttons: Help, Back, Finish, Cancel

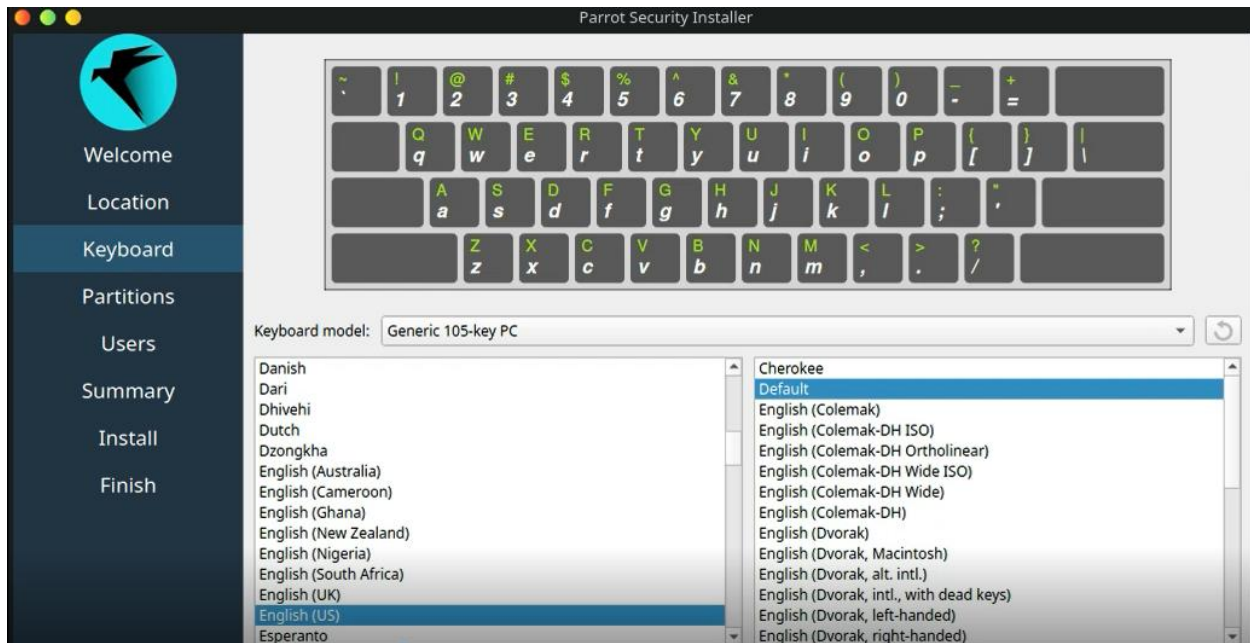
Step 4: Start Installation

Start the VM

Choose Install Parrot OS

Follow Calamares installer steps (language, keyboard, timezone)

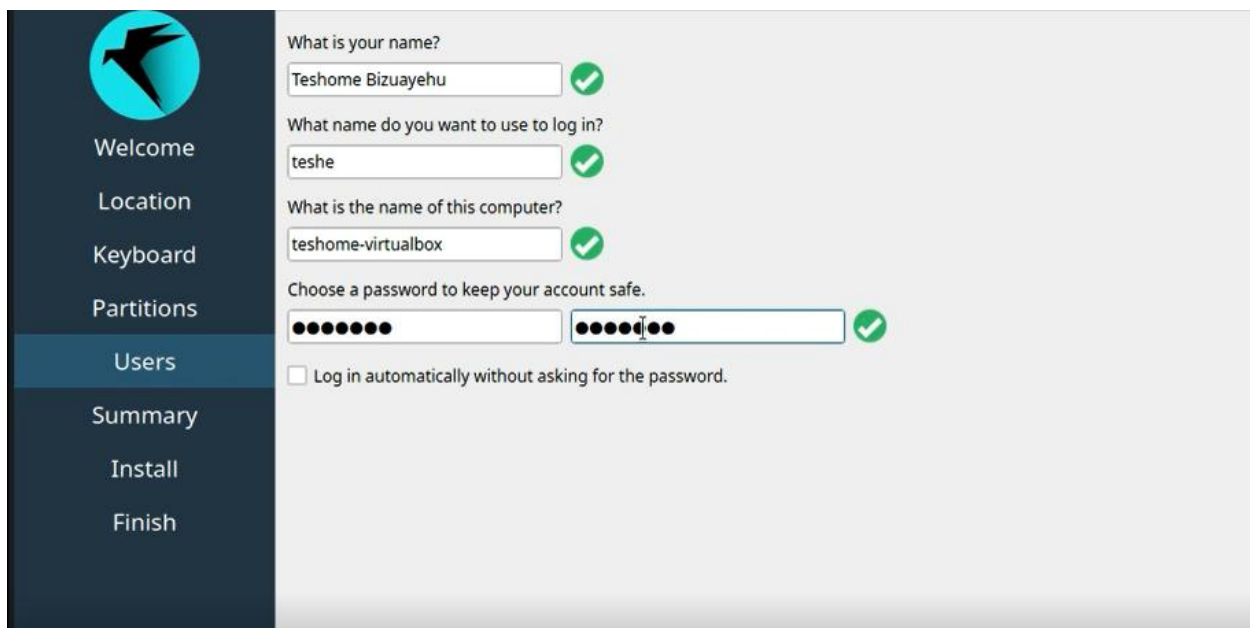




Step 5: User Account Creation

Username and full name were set as required

Password configured securely.

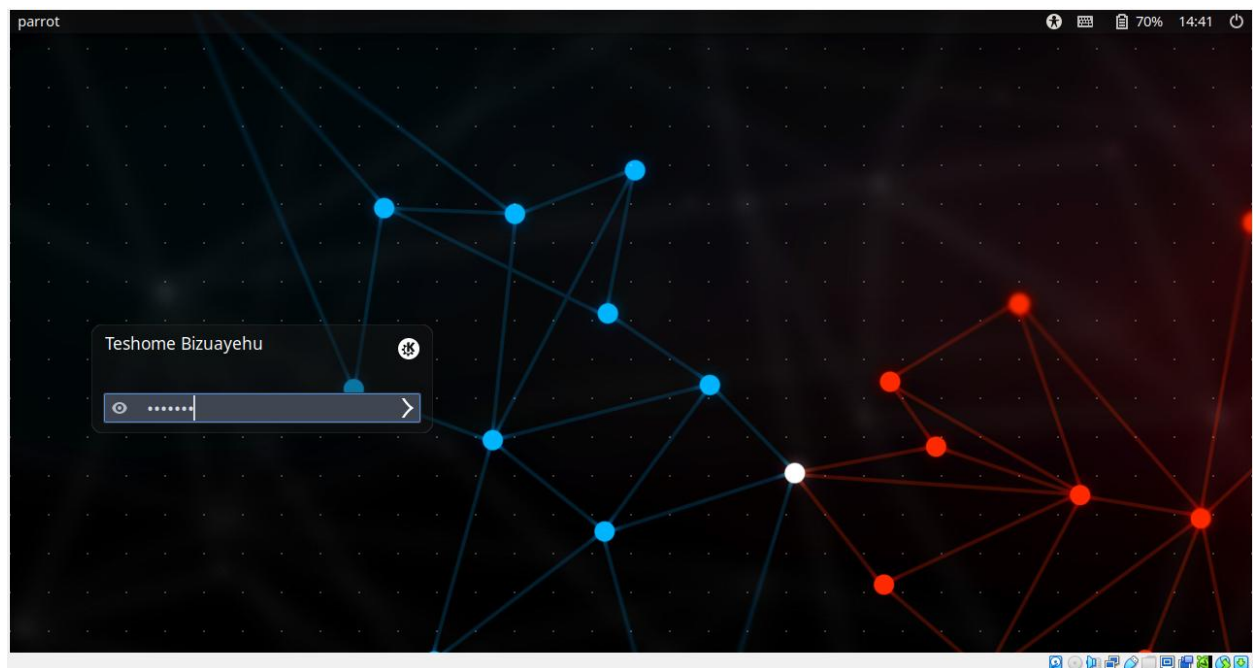
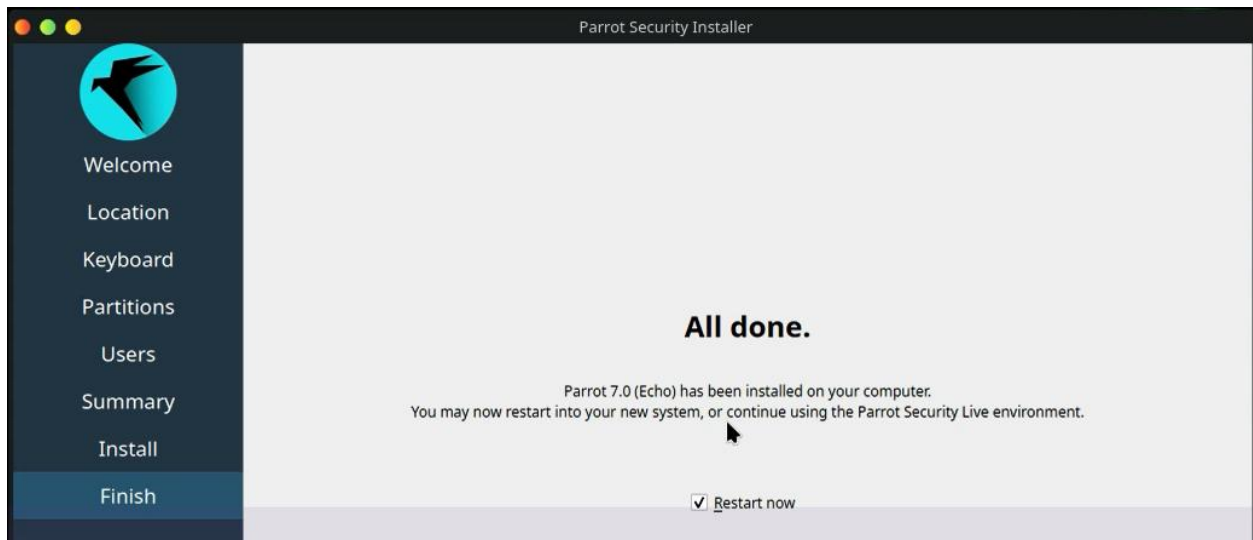


Step 6: Complete Installation

Click Install

Wait for completion

Restart VM and remove ISO



e. Issues (Problems Faced)

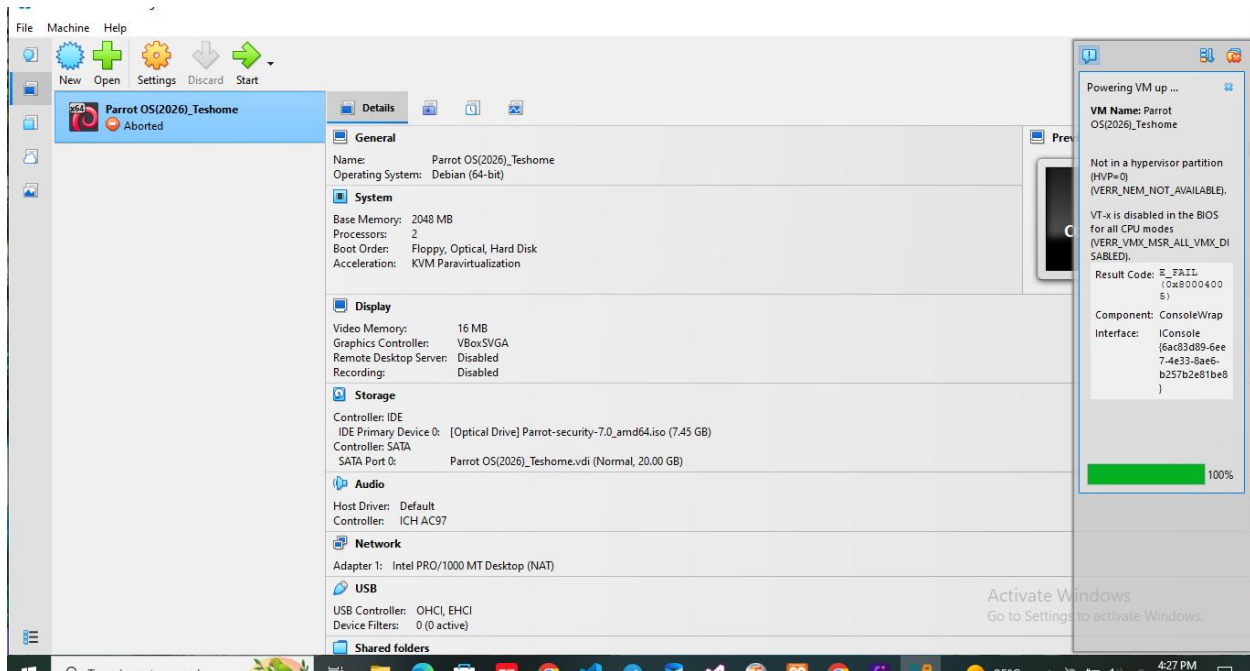
During installation and usage, the following problems were encountered:

Issue 1: Virtual Machine Failed to Start

Error message:

VT-x is disabled in the BIOS

VERR_NEM_NOT_AVAILABLE



Issue 2: Windows Black Screen with Cursor

After forced shutdown during VM failure, Windows booted to a black screen with a movable cursor

Start menu and taskbar were unresponsive

Issue 3: Start Menu and Taskbar Not Working

Start button, Settings, and CMD did not open

Taskbar icons were not responsive

f. Solutions

Solution to Issue 1: Enable Virtualization

- Enabled Intel VT-x in BIOS
- Disabled Hyper-V, Windows Hypervisor Platform, and Core Isolation

- VirtualBox was then able to start the VM successfully

Solution to Issue 2: Restore Windows Desktop

- Opened Task Manager (Ctrl + Alt + Delete)
- Ran explorer.exe
- Desktop restored without data loss

Solution to Issue 3: Repair Windows Shell

- Run sfc /scannow
- Used PowerShell to re-register AppX packages
- Restarted system
- Start menu and taskbar functionality restored

g. Filesystem Support

Selected Filesystem: ***ext4***

Reason for Choosing ext4:

- Default and stable Linux filesystem
- Excellent performance and reliability
- Full compatibility with Parrot OS
- Supports journaling and large files

Filesystem	Supported	Reason
NTFS	No	Windows-oriented
FAT32	No	File size limitation
exFAT	No	External storage only
ext4	Yes	Native Linux filesystem
Btrfs	Optional	Advanced but complex
ZFS	No	Heavy resource usage
HFS+ / APFS	No	macOS only

h. Advantages and Disadvantages

Advantages

- Safe and isolated environment

- No risk to host OS
- Ideal for cybersecurity testing
- Easy snapshot and rollback support

Disadvantages

- Performance overhead compared to native install
- Requires sufficient RAM and CPU
- Hardware access is limited

i. Conclusion

The installation of Parrot Security Edition 2026 in Oracle VM VirtualBox was successfully completed. Several technical challenges were encountered, including virtualization configuration issues and Windows shell corruption, all of which were resolved through systematic troubleshooting. This project provided valuable hands-on experience with virtualization, Linux installation, and system recovery techniques.

j. Future Outlook / Recommendations

- Increase VM RAM and CPU for advanced penetration testing tools
- Use snapshots before major system changes
- Explore VMware Workstation for performance comparison
- Practice installing additional security distributions such as Kali Linux
- Apply disk resizing techniques to avoid storage issues

2.What, why and how virtualization in modern Operating System.

➤ What is Virtualization?

Virtualization is a computing technology that enables a single physical computer to run multiple independent operating systems simultaneously. This is achieved by creating virtual machines (VMs), where each VM behaves like a separate computer with its own operating

system, applications, memory, and storage. Although these virtual machines share the same physical hardware, they are logically isolated from one another, ensuring stability and security.

Virtualization as a Core OS Concept

In modern operating systems, virtualization is no longer an optional feature but a fundamental capability. Operating systems today are designed to cooperate with hypervisors and hardware-assisted virtualization technologies. This allows systems to efficiently share CPU, memory, disk, and network resources while maintaining isolation between workloads. Virtualization plays a key role in modern computing environments such as cloud platforms, enterprise servers, and cybersecurity labs.

➤ Why Virtualization is Important

One of the primary reasons virtualization is used is efficient resource utilization. Instead of running one operating system per physical machine, virtualization allows multiple systems to share hardware, reducing cost and power consumption. It also enables better scalability, as new virtual machines can be created or removed quickly without purchasing new hardware.

Security and Isolation Benefits

Virtualization provides strong isolation between systems, which improves security. If one virtual machine crashes or becomes compromised, it does not directly affect other virtual machines or the host system. This makes virtualization ideal for malware analysis, penetration testing, software testing, and running untrusted applications in controlled environments.

➤ How Virtualization Works

Virtualization works through a software layer known as a hypervisor. The hypervisor manages and allocates hardware resources such as CPU cycles, RAM, storage, and network access to each virtual machine. There

are two main types of hypervisors: Type 1 (bare-metal), which runs directly on hardware, and Type 2 (hosted), which runs on top of an existing operating system, such as Oracle VM VirtualBox or VMware Workstation.

Role of Hardware Virtualization

Modern CPUs include built-in virtualization support, such as Intel VT-x and AMD-V. These technologies allow the hypervisor to execute virtual machines more efficiently by reducing overhead and improving performance. Hardware virtualization enables faster context switching, better memory management, and stronger isolation between virtual machines.

Virtualization in Everyday Use

Virtualization is widely used in modern computing environments. Cloud services rely heavily on virtualization to provide scalable and on-demand resources. Developers use virtual machines to test applications across different operating systems. Students and researchers use virtualization to learn operating systems, networking, and cybersecurity without risking their primary system.

Challenges of Virtualization

Despite its advantages, virtualization introduces some performance overhead compared to running an operating system directly on hardware. It also requires sufficient system resources, such as RAM and CPU cores. Proper configuration and hardware support are necessary to achieve optimal performance.

Conclusion

Virtualization is a foundational technology in modern operating systems that enables efficient resource usage, system isolation, and flexible computing environments. By combining hypervisors with hardware-assisted virtualization, modern systems can safely and efficiently run multiple operating systems on a single machine, making virtualization essential in today's computing landscape.