An

Analysis Report on

Linux and Windows 7 Operating System

Assignment -1

By

Name of the Student: Lalit Singh

University Student id: 23711218

Subject: Advanced Operating System

(TMC 104)

Course : MCA

Submitted to: Mr. Praveen Joshi

Designation

Deptt. of CS&A

DEPARTMENT OF SCHOOL OF COMPUTING

GRAPHIC ERA HILL UNIVERSITY BHIMTAL CAMPUS

SAT TAL ROAD, BHOWALI, BHIMTAL

DISTRICT- NAINITAL-263156

2023 - 2025

Que 1. Write an Analysis Report on Linux and Windows 7 Operating System .

Consider following points:

I. Architecture

II. Process Management

III. Memory Management

IV. Security Features

Analysis Report on Linux And Windows 7

Introduction:

Windows 7:

Windows 7 is a major release of the Windows NT operating system developed by Microsoft. It was released to manufacturing on July 22, 2009, and became generally available on October 22, 2009. It is the successor to Windows Vista, released nearly three years earlier.

Windows 7 is a refinement of Windows Vista, with a focus on improving performance, usability, and security. It includes a number of new features, such as a redesigned taskbar, a new file system called ReFS, and improved support for multitouch devices.

Windows 7 was a commercial success, with over 900 million licenses sold worldwide. It was the last version of Windows to be released in a traditional boxed format. Microsoft ended support for Windows 7 on January 14, 2020.

Here are some of the key features of Windows 7:

- **Aero user interface:** Windows 7 uses the Aero user interface, which is a graphical user interface (GUI) that uses transparency and other effects to make the operating system look more visually appealing.
- **Improved performance**: Windows 7 is designed to be more efficient than Windows Vista, so it should run faster and smoother on older computers.
- **Improved security**: Windows 7 includes a number of new security features, such as improved firewall protection and a new security center.
- **Multitouch support:** Windows 7 supports multitouch devices, such as touchscreen laptops and tablets.
- **New features**: Windows 7 includes a number of new features, such as a redesigned taskbar, a new file system called ReFS, and improved support for home networking.

Architecture:

The architecture of Windows 7 is a layered architecture, with the following layers:

a) **Hardware Abstraction Layer (HAL**): The HAL provides an interface between the operating system and the hardware. It abstracts the hardware so that the operating system does not need to know about the specific details of the hardware.

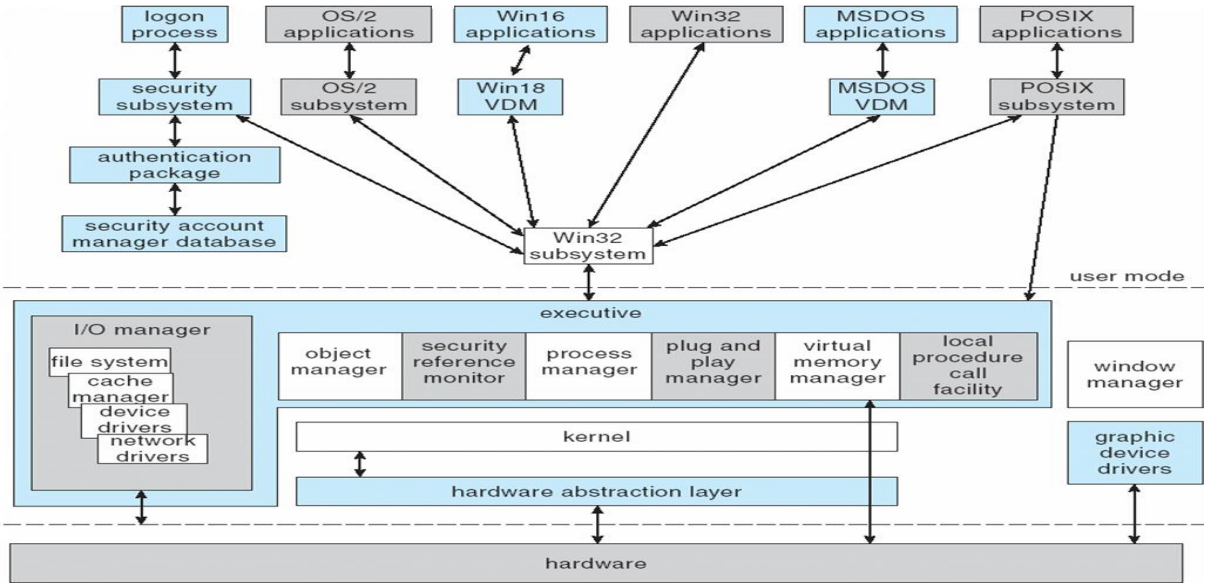
b) **Kernel:** The kernel is the core of the operating system. It manages the hardware, processes, and memory.

c) **Executive:** The executive is a set of services that provide basic operating system functions, such as process management, memory management, and device management.

d) **User Mode Subsystems:** The user mode subsystems provide services to applications, such as the file system, the windowing system, and the printer spooler.

e) **Applications:** Applications are the programs that users run. They run in user mode and interact with the operating system through the user mode subsystems.

The Windows 7 architecture is designed to be modular and scalable. This means that the operating system can be adapted to different hardware platforms and different needs.



- The HAL is the lowest layer of the architecture. It provides an interface between the operating system and the hardware.
- The kernel is the next layer up. It is responsible for managing the hardware, processes, and memory.
- The executive is the next layer up. It provides basic operating system services, such as process management, memory management, and device management.
- The user mode subsystems are the next layer up. They provide services to applications, such as the file system, the windowing system, and the printer spooler.
- Applications are the programs that users run. They run in user mode and interact with the operating system through the user mode subsystems.

Process Management

Process management is the task of creating, running, and terminating processes in an operating system. The Windows 7 operating system uses a preemptive multitasking scheduler to manage processes. This means that the operating system can preempt a running process to give another process a chance to run.

The Windows 7 process management system also includes a number of other features, such as:

- **Process creation:** The operating system provides a number of APIs that allow applications to create new processes.
- **Process scheduling:** The operating system uses a variety of factors to determine which process to run next, such as the process's priority and its CPU usage.
- **Process synchronization:** The operating system provides a number of mechanisms for processes to synchronize their activities, such as mutexes and semaphores.
- **Process termination:** The operating system provides a mechanism for processes to terminate themselves gracefully.

The Windows 7 process management system is designed to be efficient and fair. The operating system tries to ensure that all processes have a chance to run, even if they are not the highest priority process.

Here are some of the key concepts of process management in Windows 7:

- **Process:** A process is a program that is currently running. Each process has its own address space, which is a region of memory that is used to store the process's code, data, and stack.
- **Thread:** A thread is a lightweight process. Each process can have multiple threads, and each thread can run independently of the other threads in the process.
- **Process state**: The state of a process can be one of the following:
    - Ready: The process is ready to run.
    - Running: The process is currently running.
    - Waiting: The process is waiting for an event to occur, such as the completion of an I/O operation.
    - Terminated: The process has finished running.
- **Process scheduling:** The process scheduler is responsible for determining which process to run next. The scheduler takes into account factors such as the process's priority and its CPU usage.
- **Process synchronization:** Process synchronization is the mechanism that allows processes to share resources and avoid conflicts. The operating system provides a number of synchronization mechanisms, such as mutexes and semaphores.

Memory Management

Memory management is the task of allocating and de-allocating memory to processes in an operating system. The Windows 7 operating system uses a demand paging memory management system. This means that the operating system only loads pages of memory into memory when they are needed. This makes Windows 7 more efficient than operating systems that use a continuous memory management system.

Microsoft Windows has its own virtual address space for each 32-bit process, allowing up to 4 gigabytes of memory to be viewed. Each process has 8-terabyte address space on 64-bit Windows. All threads have access to the visible address space of the process. Threads, on the other hand, do not have access to the memory of another process, which protects one process from being damaged by another.

Architecture for 32-bit Windows: The automatic configuration of the 32-bit Windows Operating System (OS) allocates 4 GB (232) of accessible memory space to the kernel and user programs equally. With 4 GB physical memory available, the kernel will receive 2 GB and the app memory will receive 2 GB. Kernel-mode address space is shared by all processes, but application mode access space is provided for each user process.

Architecture for 64-bit Windows: The automatic configuration of the 64-bit Windows Operating System (OS) allocates up to 16 TB (254) of accessible memory space to the kernel and user programs equally. As 16 TB real memory is available, the kernel will have 8 TB of virtual address (VA) space and user application memory will have 8 TB of VA space. Visible address space in the kernel is allocated for all processes. Each 64-bit functionality gets its place, but each 32-bit system works on a 2 GB (Windows) virtual machine.

Windows 7 also uses a variety of other memory management techniques, such as paging, swapping, and virtual memory.

- **Memory:** Memory is the most important resource for a computer system. It is used to store data and programs that are currently being used by the computer. Memory is volatile, which means that it loses its contents when the computer is turned off.
- **Page:** A page is a unit of memory that is allocated to a process. The size of a page is typically 4096 bytes. Pages are used to improve the performance of memory management.
- **Paging:** Paging is the process of moving pages of memory between the physical memory and the hard disk. Paging is used to improve the performance of memory management by allowing the operating system to use more memory than is physically available.
- **Swapping:** Swapping is the process of moving an entire process from physical memory to the hard disk. Swapping is used when there is not enough physical memory available to run all of the processes. Swapping is a less efficient technique than paging because it requires the operating system to move the entire process to the hard disk, even if only a small part of the process is not in memory.
- **Virtual memory:** Virtual memory is a technique that allows the operating system to use more memory than is physically available. Virtual memory is implemented by mapping the process's address space to a larger address space on the hard disk. This allows the operating system to allocate pages to processes even if the pages are not currently in physical memory.

Security Features:

- **User Account Control (UAC):** UAC is a security feature that helps to prevent unauthorized users from making changes to your computer. When UAC is enabled, you will be prompted for permission before making changes to system settings or installing new software. This helps to prevent malware from installing itself on your computer without your knowledge.
- **Windows Firewall:** Windows Firewall is a firewall that helps to protect your computer from unauthorized network traffic. The firewall can be configured to block incoming and outgoing traffic, and it can also be used to create exceptions for specific applications. This helps to prevent malware from communicating with its command and control servers.
- **Windows Defender:** Windows Defender is an antivirus and anti-malware program that helps to protect your computer from viruses, spyware, and other malware. Windows Defender is included with Windows 7 and is turned on by default. Windows Defender scans your computer for malware and removes any threats that it finds.
- **Data Execution Prevention (DEP):** DEP is a security feature that helps to prevent malicious code from being executed. DEP is enabled by default on most Windows 7 systems. DEP works by preventing code from being executed in memory that is not designated for code execution. This helps to prevent malware from running on your computer.
- **Secure Boot**: Secure Boot is a security feature that helps to prevent unauthorized software from being loaded when your computer starts up. Secure Boot is enabled by default on most Windows 7 systems. Secure Boot works by verifying the digital signature of the software that is loaded when your computer starts up. This helps to prevent malware from loading when your computer starts up.
- **BitLocker Drive Encryption:** BitLocker Drive Encryption is a security feature that helps to protect your data by encrypting your hard drive. BitLocker can be used to encrypt the entire hard drive or just specific partitions. This helps to prevent unauthorized users from accessing your data.
- **Windows Update:** Windows Update is a service that automatically downloads and installs security updates for Windows 7. Windows Update is turned on by default and is important for keeping your computer secure. Security updates often include patches for vulnerabilities that could be exploited by malware.

Linux:

Linux is a family of open-source Unix-like operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991, by Linus Torvalds. Linux is typically packaged in a Linux distribution. Distributions include the Linux kernel and supporting system software and libraries, many of which are free and open-source software, but they may also include proprietary software. Linux distributions include a variety of desktop environments and can be used for a wide range of purposes, including personal computing, enterprise computing, and embedded systems.

Linux is a popular choice for servers, where it accounts for the majority of web servers and other internet-facing machines. It is also used by many large companies, including Google, Amazon, and Facebook. Linux is also gaining popularity in the desktop market, where it is competing with Windows and macOS.

Here are some of the key features of Linux:

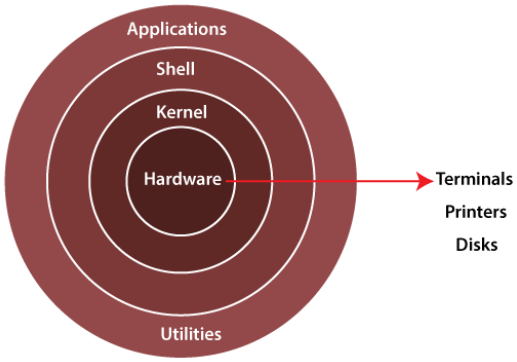
- **Open-source:** Linux is open-source software, which means that the source code is freely available for anyone to use, modify, and redistribute. This makes Linux very flexible and customizable.
- **Stable:** Linux is known for its stability. It is a very reliable operating system that is often used in mission-critical applications.
- **Secure:** Linux is a very secure operating system. It has a number of security features built in, such as kernel hardening and user permissions.
- **Free:** Linux is free to use and distribute. This makes it a very cost-effective option for businesses and individuals.
- **Customizable**: Linux is very customizable. Users can choose from a variety of distributions and desktop environments to meet their specific needs.
- **Portable:** Linux can be installed on a wide variety of hardware platforms. This makes it a very versatile operating system.
- If you are looking for a stable, secure, and customizable operating system, then Linux is a good option for you.

Here are some of the most popular Linux distributions:

- **Ubuntu:** Ubuntu is a popular Linux distribution that is known for its user-friendly interface and wide range of software applications.
- **Fedora:** Fedora is a Linux distribution that is known for its cutting-edge features and development.
- **Debian:** Debian is a Linux distribution that is known for its stability and security.
- **CentOS:** CentOS is a Linux distribution that is based on Red Hat Enterprise Linux and is known for its stability and reliability.
- **openSUSE:** openSUSE is a Linux distribution that is known for its flexibility and customization.

Architecture of Linux system

The Linux operating system's architecture mainly contains some of the components: **the Kernel, System Library, Hardware layer, System,** and **Shell utility**.



1. Kernel:- The kernel is one of the core section of an operating system. It is responsible for each of the major actions of the Linux OS. This operating system contains distinct types of modules and cooperates with underlying hardware directly. The kernel facilitates required abstraction for hiding details of low-level hardware or application programs to the system.

2. System Libraries:- These libraries can be specified as some special functions. These are applied for implementing the operating system's functionality and don't need code access rights of the modules of kernel.

3. System Utility Programs:- It is responsible for doing specialized level and individual activities.

4. Hardware layer:- Linux operating system contains a hardware layer that consists of several peripheral devices like CPU, HDD, and RAM.

5. Shell:- It is an interface among the kernel and user. It can afford the services of kernel. It can take commands through the user and runs the functions of the kernel. The shell is available in distinct types of OSes. These operating systems are categorized into two different types, which are the **graphical shells** and **command-line shells**.

Process Management of Linux system

Linux process management is a crucial aspect of operating systems that involves creating, scheduling, monitoring, and controlling processes. Processes are fundamental units of execution that allow the operating system to run multiple tasks concurrently. Effective process management ensures efficient resource utilization and responsiveness in a multi-user, multitasking environment.

Process: A process can be defined as an independent unit of execution, consisting of an executable program along with its associated data and system resources.

Types of Processes

In Linux, processes can be categorized into two types:

a) Foreground Processes

Foreground processes are the kinds of processes that require input from the user and are characterized by their interactivity. For instance, a foreground process would be like you are running an Office application on the Linux system.

b) Background Processes

On the other hand, background processes are non-interactive operations carried out in the background and do not call for any participation from the user. Antivirus software is an example of a Background Process.

Additionally, processes can be system processes or user processes. System processes are initiated by the kernel, while users initiate User processes.

In Linux, a process can be in one of five states:

a) **Running**:
   The process is currently executing on the CPU.

b) Sleeping:
   The process is waiting for a resource to become available.

c) Stopped:
   The process has been terminated by a user

d) Zombie:
   The process has completed execution but has not yet been cleaned by the system.

e) Orphan:
   The parent process of the current process has been terminated.

Process Management in Linux:

a) **Process Creation**: Processes are created using the fork() system call, which creates a copy of the parent process. The exec() family of functions is then used to load a new program into the child process's memory.

b) **Process Scheduling:** The Linux kernel scheduler assigns CPU time to processes based on priorities, fairness, and scheduling policies. Common scheduling algorithms include the Completely Fair Scheduler (CFS) and the Real-Time Scheduler.

c) **Process Termination:** Processes can be terminated using the exit() system call. When a process terminates, its resources are released, and it transitions to the "zombie" state until its parent process retrieves its exit status.

d) **Process Communication:** Processes can communicate using mechanisms such as pipes, sockets, shared memory, and signals. These mechanisms enable data exchange and coordination between processes.

e) **Process Monitoring and Control: Linux** provides tools like ps, top, and htop to monitor process status and resource usage. Additionally, the systemd init system manages processes during system startup, operation, and shutdown.

<u>Commands for Process Management in Linux</u>

Linux provides several commands for managing processes, which include:

Commands	Description
ps	Displays information about the processes running currently.
top	Provides real-time information about system processes and their resource usage.
kill	Terminates a process by sending a signal to it.

Commands	Description
nice	Adjusts the priority of a process.
renice	Changes the priority of a running process.
ps PID	Shows the state of an exact process.
pidof	Shows the Process ID of a process.
df	Shows Disk Management of your system.
free	Shows the status of your RAM.
bg	For sending a running process to the background.
fg	For running a stopped process in the foreground.

Memory Management in Linux:

In Linux, memory management system is designed to efficiently manage memory usage, allowing processes to access and use memory they require while preventing them from accessing memory they do not own.

1. Memory Allocation

Memory allocation is process of assigning memory to a process or program. In Linux, kernel provides two main methods for memory allocation: static and dynamic.

a) Static Memory Allocation

Static memory allocation is done at compile-time, where memory allocation for a program is fixed and cannot be changed during runtime. memory is allocated in program's data section or stack segment. data section contains global variables and static variables, while stack segment contains local variables.

b) Dynamic Memory Allocation

Dynamic memory allocation is done during runtime, where memory allocation for a program can be dynamically adjusted based on program's requirements. kernel provides various system calls such as malloc(), calloc(), and realloc() to dynamically allocate memory. These functions allocate memory from heap segment of program's address space.

2. Virtual Memory

Virtual memory is a memory management technique that allows a program to use more memory than is physically available in system. In Linux, virtual memory is implemented using a combination of hardware and software. hardware component is Memory Management Unit (MMU), which is responsible for translating virtual memory addresses to physical memory addresses. software component is kernel's Virtual Memory Manager (VMM), which manages allocation and deallocation of virtual memory.

3. Memory Mapping

Memory mapping is a technique that allows a process to access a file's contents as if it were part of process's memory. In Linux, memory mapping is implemented using mmap() system call. mmap() system call maps a file into a process's virtual memory address space, allowing process to read and write to file's contents as if it were part of its own memory. Memory mapping is commonly used in applications such as databases and multimedia players, where large files need to be accessed efficiently.

4. Shared Memory
Shared memory is a technique that allows multiple processes to access same portion of memory. In Linux, shared memory is implemented using shmget(), shmat(), and shmdt() system calls. shmget() system call creates a shared memory segment, shmat() attaches shared memory segment to a process's address space, and shmdt() detaches shared memory segment from process's address space. Shared memory is commonly used in inter-process communication, where multiple processes need to share data efficiently.

5. Swapping
Swapping is a technique that allows kernel to move pages of memory from RAM to a swap space on disk when system's memory is low. In Linux, swapping is implemented using a combination of hardware and software. hardware component is disk, which is used as swap space. software component is kernel's Swapping Manager, which manages swapping process. When system's memory is low, Swapping Manager selects pages of memory to swap out to disk, freeing up memory for other processes.

Linux Security Features

Linux is a widely used operating system that is known for its robust security features. While Linux is generally considered to be more secure than other operating systems, it still requires proper configuration and management to ensure maximum security.

1. User Management
User management is an essential part of Linux security. By creating separate user accounts, you can limit access to sensitive files and data. By default, Linux creates a root account during installation. root account has access to all system files and settings and should be used sparingly.

2. Firewall
The firewall is a critical component of Linux security. It allows you to control incoming and outgoing network traffic and block unwanted connections. most popular firewall for Linux is called iptables.

3. SELinux
SELinux is a security module for Linux that provides enhanced security features. It uses a set of policies to enforce mandatory access control (MAC) on system resources. MAC is a security model that enforces restrictions on actions that a user or application can perform on a system.

4. SSH
SSH (Secure Shell) is a protocol used to securely connect to a remote Linux system over network. SSH encrypts all communication between client and server, providing a secure way to access remote systems.

5. Encryption
Encryption is an essential tool for securing data on a Linux system. Encryption allows you to protect sensitive data from unauthorized access, even if an attacker gains access to your system. Linux provides several encryption tools, including LUKS and GnuPG.

LUKS (Linux Unified Key Setup) is a disk encryption standard used by Linux. LUKS allows you to encrypt entire partitions or disks on your system.

Comparison and Analysis:

Architecture: Linux's monolithic design offers better performance optimization, while Windows 7's hybrid model aims for enhanced stability and separation of user and kernel modes.

Process Management: Linux's CFS scheduler provides fairness and efficiency, making it suitable for various workloads. Windows 7's preemptive multitasking and priority-based scheduling prioritize responsiveness.

Memory Management: Both systems use demand paging, but Linux's customizable memory management allows for tailored optimization, while Windows 7 focuses on ease of use.

Security Features: Linux's open-source nature enhances security transparency, while Windows 7 emphasizes user-friendliness through UAC and BitLocker.

Conclusion:

This analysis underscores the distinct features of Linux and Windows 7 operating systems, shedding light on their architectures, process management, memory handling, and security mechanisms. Organizations and users must weigh the trade-offs between performance, stability, security, and user experience to make an informed choice that aligns with their specific requirements.