DEPARTMENT OF CYBER SECURITY

U23CBT44/ OPERATING SYSTEMS AND SECURITY

PART A

UNIT I OPERATING SYSTEM OVERVIEW

1. What is Computer-System Organization?

Answer:
Computer-System Organization refers to the structure and interaction of hardware components (CPU, memory, I/O devices, etc.) that make up a computer system. It defines how these components work together to perform computing tasks.

2. Differentiate between Architecture and Organization.

Answer:
Architecture refers to the design and instruction set of a computer, while Organization deals with the physical arrangement of the system components and how they function together to execute the architecture.

3. What is the role of an Operating System?

Answer:
An Operating System (OS) manages hardware resources, provides a user interface, and acts as an intermediary between application software and hardware, ensuring efficient and secure operation of the system.

4. What is meant by Resource Management in an Operating System?

Answer:
Resource Management in an OS involves the efficient allocation and deallocation of system resources such as CPU, memory, disk space, and I/O devices to ensure smooth execution of processes and prevent conflicts.

5. Explain the term 'Security' in Operating Systems.

Answer:
Security in an OS protects the system from unauthorized access, data corruption, or breaches. It includes authentication, encryption, access control, and ensuring the integrity of system resources.

6. What is the difference between Protection and Security?

Answer:
Protection ensures that processes and users cannot harm each other's resources, while Security protects the system from external threats such as unauthorized access or cyber-attacks.

7. What are Distributed Systems?

Answer:
Distributed Systems are networks of independent computers that work together as a unified system, sharing resources and tasks, often spread across multiple locations. The OS manages communication, synchronization, and resource sharing.

8. What are Kernel Data Structures?

Answer:
Kernel Data Structures are data structures used by the operating system kernel to store important information such as process states, memory addresses, and I/O operations, enabling efficient system management.

9. What is the purpose of System Calls?

Answer:
System Calls allow programs to request services from the operating system, such as file operations, memory management, and process control, by providing an interface to the kernel.

10. What are System Services in an OS?

Answer:
System Services are the various functions provided by the operating system, such as process scheduling, file management, device handling, and memory allocation, which support user applications and system operations.

11. Explain the structure of an Operating System.

Answer:
The OS structure consists of various components such as the kernel, device drivers, file systems, memory management units, user interface, and system services that work together to manage hardware and software resources.

12. What is meant by Building an Operating System?

Answer:
Building an OS refers to the process of creating the system's core components, such as the kernel, file systems, device drivers, and user interfaces, which collectively form the functioning operating system.

13. What is the process of Booting an Operating System?

Answer:
Booting is the process of starting the operating system by loading the kernel into memory from secondary storage (e.g., hard drive), initializing hardware, and transferring control to the OS.

14. What is a Process Control Block (PCB)?

Answer:
A Process Control Block (PCB) is a data structure used by the OS to store information about a process, such as its current state, program counter, memory usage, and CPU registers, which helps in process management.

15. What is the role of the OS in Memory Management?

Answer:
The OS manages memory by allocating and deallocating memory blocks to processes, ensuring that each process has the necessary memory resources without causing conflicts or memory leaks.

16. What is Multitasking?

Answer:
Multitasking is the OS's ability to execute multiple processes simultaneously by allocating CPU time to each process, giving the illusion of concurrent execution on a single processor.

17. What is a System Interrupt?

Answer:
A system interrupt is a mechanism used by the hardware to signal the OS about an event that needs immediate attention, such as I/O operations or errors, which allows the OS to handle these events promptly.

18. What is a File System in an Operating System?

Answer:
A File System is a method used by the OS to organize, store, and retrieve files on storage devices. It defines how files are named, stored, and accessed by both the OS and applications.

19. What are Device Drivers in an Operating System?

Answer:
Device Drivers are software components that allow the OS to interact with hardware devices. They translate OS commands into device-specific instructions and manage the device's functionality.

20. What is the difference between User Mode and Kernel Mode?

Answer:
User Mode is the mode in which user applications run, with limited access to system

resources, while Kernel Mode is the mode in which the OS kernel runs, with full access to hardware and system resources.

UNIT II PROCESS MANAGEMENT

1. **What is a process?**
   A process is a program in execution, which includes the program code, a stack, and a data segment.
2. **What is process scheduling?**
   Process scheduling is the mechanism to decide which process gets the CPU at any given time.
3. **What are the different types of schedulers?**
   - **Long-term scheduler**: Determines which processes are admitted to the system for processing.
   - **Short-term scheduler**: Selects which process to execute next.
   - **Medium-term scheduler**: Suspends or resumes processes.
4. **What is the role of the PCB (Process Control Block)?**
   PCB stores information about a process, including its state, program counter, CPU registers, memory limits, and more.

Operation on Processes

5. **What are the basic operations on processes?**
   - Process creation: A parent process creates child processes.
   - Process termination: A process completes or is explicitly terminated.
6. **What is a zombie process?**
   A process that has completed execution but still has an entry in the process table is called a zombie process.
7. **What is an orphan process?**
   An orphan process is one whose parent process has terminated but is still executing.

Inter-Process Communication (IPC)

8. **What is IPC?**
   Inter-process Communication is the mechanism that allows processes to share data and synchronize their activities.
9. **What are the methods of IPC?**
   - **Shared Memory**: Processes access common memory space.
   - **Message Passing**: Processes send and receive messages.
10. **What is a race condition?**
    A race condition occurs when the outcome of processes depends on the sequence or timing of execution.

Threads and Multithreading Models

11. **What is a thread?**
    A thread is a lightweight unit of a process that shares resources like code and data with other threads in the same process.
12. **What are the benefits of threads?**
    - Faster context switching.

- Efficient resource sharing.
- Improved application responsiveness.

13. **What are the multithreading models?**
    - **Many-to-One**: Many user threads map to one kernel thread.
    - **One-to-One**: Each user thread maps to a kernel thread.
    - **Many-to-Many**: Many user threads map to many kernel threads.
14. **What is thread synchronization?**
    Thread synchronization ensures threads operate in a sequence, especially when accessing shared resources.

CPU Scheduling

15. **What are the criteria for CPU scheduling?**
    - CPU Utilization
    - Throughput
    - Turnaround Time
    - Waiting Time
    - Response Time
16. **What is the difference between preemptive and non-preemptive scheduling?**
    - **Preemptive**: A process can be interrupted and moved to the ready queue.
    - **Non-preemptive**: A process runs to completion once started.
17. **What are common CPU scheduling algorithms?**
    - First-Come-First-Served (FCFS)
    - Shortest Job Next (SJN)
    - Priority Scheduling
    - Round Robin (RR)

Process Synchronization

18. **What is the critical-section problem?**
    It is a problem of ensuring that no two processes are executing in the critical section at the same time.
19. **What is a mutex?**
    A mutex (mutual exclusion) is a locking mechanism used to synchronize access to a resource.
20. **What is a semaphore?**
    A semaphore is a signaling mechanism used to control access to a resource by multiple processes.

Deadlocks

21. **What are the necessary conditions for a deadlock?**
    - Mutual exclusion
    - Hold and wait
    - No preemption
    - Circular wait
22. **What is deadlock prevention?**
    Deadlock prevention ensures that at least one of the necessary conditions for a deadlock is not allowed to occur.
23. **What is deadlock avoidance?**
    It ensures that a system never enters an unsafe state by analyzing resource-allocation requests.

24. **What is deadlock detection?**
    Deadlock detection is the process of identifying processes in a deadlock and taking action to recover.
25. **What is a safe state?**
    A system is in a safe state if it can allocate resources to all processes without entering a deadlock.

UNIT III MEMORY MANAGEMENT AND FILE SYSTEMS

1. **What is the purpose of main memory in a computer system?**
   Main memory stores data and instructions that the CPU needs for processing. It provides faster access compared to secondary storage.
2. **What is swapping in memory management?**
   Swapping is the process of moving a process temporarily from main memory to secondary storage and then back to main memory for execution.
3. **What is contiguous memory allocation?**
   In contiguous memory allocation, each process is allocated a single, contiguous block of memory.
4. **What are the drawbacks of contiguous memory allocation?**
   - Fragmentation (internal and external).
   - Difficult to accommodate varying process sizes.
5. **What is paging?**
   Paging is a memory management technique that divides the process into fixed-size blocks called pages and the memory into fixed-size blocks called frames.
6. **What is segmentation?**
   Segmentation divides a process into variable-sized segments based on logical divisions, such as functions or arrays.

Virtual Memory

7. **What is virtual memory?**
   Virtual memory is a memory management technique that allows the execution of processes larger than the available physical memory by using secondary storage.
8. **What is demand paging?**
   In demand paging, pages are loaded into memory only when they are needed during execution, reducing memory usage.
9. **What is a page fault?**
   A page fault occurs when a process tries to access a page that is not currently in memory.
10. **What are the common page replacement algorithms?**
    - FIFO (First-In-First-Out)
    - LRU (Least Recently Used)
    - Optimal Page Replacement
11. **What is thrashing?**
    Thrashing occurs when a process spends more time swapping pages in and out of memory than executing, due to insufficient memory.
12. **What is kernel memory allocation?**
    Kernel memory allocation involves allocating memory specifically for the operating system kernel and its processes.

File System Structure

13. **What is the purpose of a file system?**
    A file system organizes and manages data storage on devices like hard drives, ensuring efficient data access and manipulation.
14. **What are the components of a file system?**
    - File control blocks
    - Directory structure
    - Disk allocation and free space management
15. **What are the main directory structures?**
    - Single-level directory
    - Two-level directory
    - Tree-structured directory
    - Acyclic graph directory

Directory Implementation

16. **What are the two main methods for directory implementation?**
    - Linear list: A simple list of files in a directory.
    - Hash table: A hash function is used for faster file location.
17. **What is a path in a file system?**
    A path specifies the location of a file or directory within the file system, either as an absolute path (from the root) or a relative path (from the current directory).

Allocation Methods

18. **What are the file allocation methods?**
    - Contiguous allocation
    - Linked allocation
    - Indexed allocation
19. **What is the main drawback of contiguous allocation?**
    Contiguous allocation suffers from external fragmentation and difficulty in resizing files.

Free Space Management

20. **What are the methods of free space management?**
    - Bit vector: A bitmap is used to track free and allocated blocks.
    - Linked list: A linked list of free blocks is maintained.
    - Grouping: Free blocks are stored in groups, with each group pointing to the next.
    - Counting: Tracks contiguous free blocks as a single entry.

UNIT IV SECURE SYSTEMS AND VERIFIABLE SECURITY GOALS

1. **What are the primary goals of security?**
    - **Confidentiality**: Ensuring data is accessed only by authorized users.
    - **Integrity**: Protecting data from unauthorized modification.
    - **Availability**: Ensuring systems and data are available when needed.
2. **What is non-repudiation in security?**
    Non-repudiation ensures that a party cannot deny the authenticity of their action, such as sending a message or transaction.

Trust and Threat Model

3. **What is a threat model?**
   A threat model is a structured approach to identify, evaluate, and address potential threats to a system.
4. **What is the difference between trusted and trustworthy systems?**
   - **Trusted**: A system is relied upon but may not always be secure.
   - **Trustworthy**: A system is designed to be secure and reliable.

Access Control Fundamentals

5. **What is access control?**
   Access control is the method of regulating who can view or use resources in a computing environment.
6. **What are the main types of access control?**
   - **Discretionary Access Control (DAC)**: Permissions are defined by the resource owner.
   - **Mandatory Access Control (MAC)**: Permissions are enforced based on rules set by a central authority.
   - **Role-Based Access Control (RBAC)**: Permissions are assigned based on user roles.
7. **What is the principle of least privilege?**
   Users are granted the minimum level of access necessary to perform their tasks.

Protection System

8. **What is the purpose of a protection system?**
   A protection system ensures controlled access to resources, preventing unauthorized use or modification.
9. **What is a domain in a protection system?**
   A domain defines the set of resources that a process or user can access.

Reference Monitor

10. **What is a reference monitor?**
    A reference monitor is an abstract machine that enforces access control policies by mediating all access attempts to resources.
11. **What are the properties of a reference monitor?**
    - **Complete mediation**: All access is checked.
    - **Tamper-proof**: It cannot be bypassed or modified.
    - **Verifiable**: Its correctness can be proven.

Secure Operating System Definition

12. **What is a secure operating system?**
    A secure operating system enforces security policies, provides robust access control, and protects against vulnerabilities.
13. **What are the key requirements for a secure operating system?**
    - Confidentiality
    - Integrity
    - Availability
    - Accountability

Assessment CriteriaWhat is the purpose of assessment criteria in security?
Assessment criteria are used to evaluate the security capabilities of systems, ensuring they meet required standards.

14. **What is the Common Criteria (CC)?**
    The Common Criteria is an international framework for evaluating and certifying the security of IT products.

Information Flow

16. **What is information flow control?**
    Information flow control ensures that data flows only in permissible ways, preventing unauthorized data leakage.
17. **What is a covert channel?**
    A covert channel is an unauthorized communication path that bypasses access control mechanisms.

Information Flow Secrecy Models

18. **What is the goal of secrecy models in information flow?**
    Secrecy models aim to ensure that sensitive information does not flow to unauthorized entities.
19. **What is Denning's Lattice Model?**
    Denning's Lattice Model is a mathematical framework for defining secure information flow between security classes using a lattice structure.

Bell-LaPadula Model

20. **What is the Bell-LaPadula model?**
    The Bell-LaPadula model is a security model focused on maintaining data confidentiality by enforcing:
    - **Simple Security Property**: A subject cannot read data at a higher security level ("no read-up").
    - **Star (*) Property**: A subject cannot write data to a lower security level ("no write-down").

UNIT V SECURITY IN OPERATING SYSTEMS

UNIX Security

1. **What is the purpose of UNIX security?**
   UNIX security protects the system against unauthorized access and ensures confidentiality, integrity, and availability of data.
2. **What are the main security features of UNIX?**
   - File and directory permissions (read, write, execute).
   - User and group-based access control.
   - Root privilege separation.

UNIX Protection System

3. **What is the UNIX protection system?**
   The UNIX protection system enforces access control by managing file permissions, ownership, and user roles.
4. **What are the components of the UNIX protection system?**
   - **Owner permissions**: Access rights for the file owner.
   - **Group permissions**: Access rights for a specific group.
   - **Other permissions**: Access rights for all other users.

UNIX Authorization

5. **What is UNIX authorization?**
   UNIX authorization determines whether a user or process has permission to access specific files or resources.
6. **How are user privileges assigned in UNIX?**
   User privileges are assigned through user accounts, group memberships, and file permission settings (e.g., chmod, chown).

UNIX Security Analysis

7. **What is the goal of UNIX security analysis?**
   To identify vulnerabilities, analyze security policies, and ensure the system is protected against unauthorized access.
8. **What tools are used for UNIX security analysis?**
   - nmap: Network scanning tool.
   - chkrootkit: Rootkit detection.
   - logwatch: Log file monitoring.

UNIX Vulnerabilities

9. **What are common vulnerabilities in UNIX systems?**
   - Weak or default passwords.
   - Misconfigured file permissions.
   - Vulnerable network services (e.g., Telnet, FTP).
10. **How can UNIX vulnerabilities be mitigated?**
    - Use strong passwords and enforce policies.
    - Regularly update and patch software.
    - Disable unnecessary services.

Windows Security

11. **What are the primary goals of Windows security?**
    To protect the system against unauthorized access, ensure the confidentiality of user data, and provide reliable operation.
12. **What is the purpose of Windows Defender?**
    Windows Defender is a built-in antivirus and anti-malware tool designed to protect the Windows system from security threats.

Windows Protection System

13. **What is the role of the Windows protection system?**
    The Windows protection system enforces access control policies, manages user

accounts, and secures system resources through tools like ACLs (Access Control Lists).

14. **What is User Account Control (UAC) in Windows?**
    UAC is a security feature that prevents unauthorized changes to the system by prompting for administrative permissions when needed.

Windows Authorization

15. **What is Windows authorization?**
    Windows authorization determines whether a user or process is permitted to access a system resource, based on access control policies.
16. **What is an access token in Windows?**
    An access token is a security object that identifies a user and their permissions, used for resource authorization.

Windows Security Analysis

17. **What is Windows security analysis?**
    It involves assessing and identifying security risks, vulnerabilities, and misconfigurations in a Windows system.
18. **What tools are used for Windows security analysis?**
    - **Windows Event Viewer**: For analyzing logs.
    - **Microsoft Baseline Security Analyzer (MBSA)**: For vulnerability assessment.
    - **Sysinternals Suite**: For advanced diagnostics.

Windows Vulnerabilities

19. **What are common vulnerabilities in Windows systems?**
    - Weak passwords.
    - Unpatched software vulnerabilities.
    - Misconfigured security policies.
20. **How can Windows vulnerabilities be mitigated?**
    - Enable automatic updates.
    - Use strong, complex passwords.
    - Regularly review and update security policies.