## **Operating System Security-:** The process of ensuring OS availability, confidentiality, integrity is known as operating system security. OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions.

Security refers to providing safety for computer system resources like software, CPU, memory, disks, etc. It can protect against all threats, including viruses and unauthorised access.

System security may be threatened through two violations, and these are as follows:

**1. Threat :** A program that has the potential to harm the system seriously.

**2. Attack :** A breach of security that allows unauthorised access to a resource.

There are two types of security breaches that can harm the system:

1. Malicious -:Malicious threats are a type of destructive computer code or web script that is designed to cause system vulnerabilities that lead to back doors and security breaches.
2. Accidental.-: it is easy to handle.

security may be compromised through the breaches. Some of the breaches are as follows:

1. Breach Of Integrity-: This violation has unauthorised data modification.
2. Theft of service -: It involves the unauthorised use of resources.
3. Breach of confidentiality-: It involves the unauthorised reading of data.
4. Breach of availability -:It involves the unauthorised destruction of data.
5. Denial of service -: It includes preventing legitimate use of the system.

The goal of security system-:

1. Integrity
2. Secrecy
3. Availability

## Types of Threats -:

1. Program Threats 2. System Threats

Program Threats-: Program Threats occur when a user program causes these processes to do malicious operations. The common example of a program threat is that when a program is installed on a computer, it could store and transfer user credentials to a hacker. There are various program threats. Some of them are as follows:

1. Virus 2. Trojan Horse 3. Logic Bomb 4. Trap Door

System Threats-: System threats are described as the misuse of system services and network connections to cause user problems. System threats make an environment in which OS resources and user files may be misused. There are various system threats. Some of them are as follows:

1. Port scanning 2. Worm 3. Denial of service

**Threats to operating system-**:

1. Malware
2. Network Intrusion
3. Buffer overflow

There are various ways to ensure operating system security. These are as follows:

1. Authentication

I. Username/Password

Ii. User Attribution (Biometric Verification)

Iii. User card and key

1. One Time Password (OTP)

I. Secret Key

Ii. Random Number

Iii. Network Password

1. Firewalls
2. Physical Security

**Access control -:** Access control is a security mechanism that ensures that only authorised individuals can access specific resources, such as computer systems, data, physical locations, or networks. Access control is important because it helps protect sensitive information and assets from unauthorised access, theft, or damage.

Access control can be implemented using various mechanisms, including passwords, biometric authentication, smart cards, and access control lists (ACLs). Access control can also be applied at different levels, including physical, network, operating system, and application levels.

There are three main types of access control:

1. **Mandatory access control (MAC)**: MAC is a security model that uses labels or tags to enforce access policies. Each user and object in the system is assigned a label that determines the level of access they have. MAC is commonly used in government and military settings.
2. **Discretionary access control (DAC)**: DAC is a security model that allows the owner of a resource to determine who has access to it. Each user is given permission to access the resource by the owner. DAC is commonly used in small to medium-sized organisations.
3. **Role-based access control (RBAC**): RBAC is a security model that assigns users to roles based on their job responsibilities. Each role has a set of permissions that determine what resources the user can access. RBAC is commonly used in large organisations.

**Encryption-:** Encryption is the process of converting plaintext, which is readable and understandable by anyone, into ciphertext, which is incomprehensible and secure. This is done by applying an algorithm, known as a cipher, to the plaintext to transform it into the ciphertext**.**

There are several types of encryption, including:

1. **Symmetric encryption**: In this type of encryption, a single key is used for both encryption and decryption. The same key is shared between the sender and the recipient, and it must be kept secret.
2. **Asymmetric encryption**: This type of encryption uses a pair of keys, a public key and a private key, to encrypt and decrypt messages. The public key is shared with everyone, while the private key is kept secret by the owner.
3. **Hashing**: Hashing is a one-way encryption method that converts plaintext into a fixed-length string of characters. This method is often used to verify the integrity of data, such as passwords or digital signatures.
4. **End-to-end encryption**: This type of encryption ensures that messages are encrypted at the sender's device and can only be decrypted by the recipient's device, meaning that nobody in between can access or read the message.

**System Administration and Maintenance-:** system administration and maintenance refer to the tasks involved in managing and maintaining the health, performance, and security of computer systems and networks. Effective system administration and maintenance are critical to the health and performance of computer systems and networks. By performing regular maintenance and monitoring, system administrators can identify and resolve issues before they become major problems, ensure that systems and data are secure, and minimise downtime due to system failures or disasters.

System administration and maintenance tasks -:

1. Installing and configuring hardware and software
2. System monitoring and performance tuning
3. User management
4. Backup and recovery
5. Security management
6. Upgrades and patch management
7. Disaster recovery planning

**Troubleshooting-:**Troubleshooting is the process of identifying, diagnosing, and resolving problems that arise in computer systems, networks, software, or hardware. It is an essential skill for IT professionals, as it helps to minimise downtime, restore system functionality, and improve system performance.

Troubleshooting did following task-:

1. Identify the Problem
2. Determine the scope of the problem
3. Perform basic troubleshooting
4. Use diagnostic tools
5. Create a plan of action
6. Test the solution

**Assignment**

**Report: Security Mechanisms in Modern Operating Systems-:**

Introduction-: Modern Operating Systems (OS) include several security mechanisms to protect against threats and vulnerabilities. These mechanisms include access control, authentication, encryption, firewalls, and antivirus software. This report discusses these security mechanisms and their importance in protecting computer systems and networks.

Access Control -: Access control is a security mechanism that restricts access to computer systems and data. It ensures that only authorised users have access to sensitive data, applications, and network resources. Access control includes user authentication, which verifies the identity of users before granting access, and authorization, which defines the actions that users are authorised to perform.

Authentication-: Authentication is a security mechanism that verifies the identity of users before granting access. Authentication can be performed using several methods, including passwords, biometrics, and two-factor authentication. Strong authentication is essential to prevent unauthorised access to sensitive data and systems.

Encryption-:Encryption is a security mechanism that protects data by converting it into an unreadable format. Encrypted data can only be accessed using a decryption key, which ensures that only authorised users can access sensitive data. Encryption is used in many modern OS features, including disk encryption, email encryption, and SSL encryption.

Firewalls-: Firewalls are a security mechanism that controls incoming and outgoing network traffic. Firewalls protect against unauthorised access to computer systems by blocking traffic from unauthorised sources and preventing malicious traffic from reaching the network. Firewalls are essential in protecting against network-based attacks and are included in many modern OS.

Antivirus Software-: Antivirus software is a security mechanism that detects and removes malicious software, including viruses, spyware, and malware. Antivirus software is essential in protecting against attacks that attempt to infect computer systems with malicious software.

**Best Practices for System Administration and Maintenance-:**

System administration and maintenance are essential to the health and performance of computer systems and networks. The following are best practices for system administration and maintenance:

1. Perform regular system maintenance, including software updates, patches, and backups.
2. Monitor system performance and resource utilisation to identify and resolve performance issues.
3. Implement strong access control and authentication mechanisms to prevent unauthorised access to sensitive data and systems.
4. Implement firewalls and antivirus software to protect against network-based attacks and malware.
5. Create and test disaster recovery plans to ensure that systems can be restored in the event of a disaster or system failure.

Conclusion

Modern Operating Systems include several security mechanisms to protect against threats and vulnerabilities. These mechanisms include access control, authentication, encryption, firewalls, and antivirus software. Effective system administration and maintenance are essential to the health and performance of computer systems and networks. Best practices for system administration and maintenance include regular maintenance, monitoring, and disaster recovery planning.