SECURING NETWORK

CONFIDENTIALITY

- Confidentiality: Confidentiality refers to the protection of sensitive or confidential information from unauthorized access, use, or disclosure.
- Confidentiality ensures that only authorized individuals or entities have access to sensitive information and that the information is not disclosed to others who do not have the appropriate level of clearance.
- In real life, confidentiality is essential in protecting information such as financial information, personal information, or trade secrets.
- For example, a bank must maintain confidentiality by ensuring that customer account information is protected from unauthorized access, and medical facilities must protect patient information from disclosure to unauthorized persons.

INTEGRITY

- Integrity: Integrity refers to the protection of information from unauthorized alteration or modification. It ensures that data remains intact and accurate, and any modifications to it are authorized and legitimate.
- In real life, integrity is essential in protecting data such as financial records or legal documents.
- For example, a law firm must ensure the integrity of legal documents, so they remain unchanged and accurate, and financial institutions must maintain the integrity of their accounting records to ensure accuracy.

AVAILABILITY

- Availability: Availability refers to the ability to access data and resources when needed. It ensures that information and resources are accessible to authorized individuals or entities when required.
- In real life, availability is critical in maintaining business operations, customer service, and access to critical information.
- For example, a hospital must ensure that patient records are available to authorized personnel when needed, and a retail store must ensure that its systems and resources are available to serve customers.

NETWORK SECURITY ATTACKS

RECONNAISSANCE ATTACKS

- Reconnaissance attacks: Reconnaissance attacks involve the gathering of information about a network or system with the intent of identifying vulnerabilities that can be exploited to gain unauthorized access.
- Examples of reconnaissance attacks include port scanning, network mapping, and vulnerability scanning.

Access attacks

- Access attacks: Access attacks involve attempts to gain unauthorized access to a network or system.
- Examples of access attacks include password cracking, SQL injection, and man-in-the-middle attacks.

SOCIAL ENGINEERING ATTACKS

- Social Engineering attacks: Social engineering attacks involve exploiting human psychology to gain unauthorized access to a network or system.
- Examples of social engineering attacks include phishing, pretexting, and baiting.

DENIAL OF SERVICE ATTACKS

- Denial of Service attacks: Denial of service (DoS) attacks involve overwhelming a network or system with traffic to make it unavailable to users.
- Examples of DoS attacks include ping flooding, SYN flooding, and smurf attacks.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

- Distributed Denial of Service attacks: Distributed denial of service (DDoS) attacks involve using multiple systems to launch a coordinated attack on a network or system.
- Examples of DDoS attacks include botnets, amplification attacks, and reflective attacks.