Purpose of network security

1. Confidentiality – Information needs to be hidden from unauthorized access.

2. Integrity – Protect information Protected from unauthorized change

3. Availability – Information available to an authorized entity when it is needed.

**Types of Security Attacks:**

Security Attack

Threat to Confidentiality Threat to Integrity Threat to Availability

1. Snooping 1. Modification 1. DoS

2. Traffic Analysis 2. Masquerading

3. Replaying

4. Repudiation

What is Snooping?

It refers to unauthorized access. For example – A confidential file is sent by sender, the intruder receives the data and use for her/his own benefit is called Snooping.

**Traffic Analysis**

Example – Someone can find the email address of the sender or the receiver and can collect pairs of requests or responses to help his/her guess the nature of transaction.

**Modification**

**Masquerading**

Example – A user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

**Replaying**

The attacker obtains a copy of a message sent by a user and tries to replay it later.

**Repudiation**

The sender of the message might deny that she has sent the message, the receiver of the message might deny that she/he has received the message.

**Denial of Service**

The attacker can use several strategies or mechanisms. He/she might send so many requests to a server that the server crashes because of heavy message/data load. The attacker might intercept and remove a server’s response to a client, making the client to believe that the server is not responding. The attacker may also intercept requests from the clients, causing the clients to send request many times and overload the system.

**Passive and Active Attack**

Passive – This means that the attack does not modify the data or harm the system. Example – Snooping and Traffic Analysis.

Active – It may change the data or harm the system. Example – Integrity and Availability.