**Know about security attacks on computer**

We live in an age where most of the information is stored in computers, such as music, movies along with that a lot of sensitive information such as bank account details, employee data are also stored. The success of computers for business processes is largely due to the use of internet and intranet. Intranet caters to the organization for its internal communications, while internet can be accessed by anyone. Now this makes business processes very quick and easy (by reducing the distance between the head offices and its branches), but along with that it also brings about security threats on websites and to the individuals that are communicating with each other(through internet or intranet) that may contain sensitive information. So, in order to save your information from attacks it is important to study possible security attacks that can occur on your system.

Before proceeding, let us look at the definition of threat and attack:

**Threat**: A potential violation of security, which may exist due to loop holes in system or when there is a circumstance, action or event that could breach security and cause harm.

**Attack**: An assault on system through an intelligent act that is deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Attacks can be broadly classified as:

1. **Passive Attacks**
2. **Active Attacks**

Let us look at them in detail:

1. Passive Attacks:

A passive attack attempts to learn or make use of information from the system, but does not affect system resources. The goal of opponent is to obtain information that is being transmitted. A telephone conversation, email message, or a transferred file in which contents are hacked is called release of message contents type attack. Now, suppose that the message is masked i.e. the message is encrypted so that even if the message is captured, information cannot be captured. In this case opponent can track pattern of message and could determine the location of the communicating host and could observer the frequency and the length of messages. This can help in guessing the nature of the communication that is taking place. This type of attack is called traffic analysis. Passive attacks are difficult to detect because they do not involve any alteration of data. So, emphasis is on prevention rather than detection

1. Active Attacks

Active attacks involve some modification of data stream or the creation of false stream and can be divided into four categories:

* Masquerade: This is the case where one entity pretends to be different entity (that has more rights to access the services) from the server by way of way of capturing authentication sequences. This may lead to dissemination of some sensitive information to the opponent.
* Replay: This involves passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.
* Modification of message: It means that some portion of legitimate message is altered, delayed or reordered.
* Denial of service: This prevents or inhibits the normal use of the management of communication facilities. It can be done of by disruption of services that are directed at a particular destination. Another form is the disruption of entire network, by disabling the network or by overloading it with messages so as to degrade performance.

**SUMMARY**:

Active attacks present opposite characteristics of the passive attacks. Passive attacks are difficult to detect while measures are available to prevent their success. On the other hand, active attacks are difficult to prevent absolutely. So, measures must be taken to keep them to a minimum which will help in avoiding losses that may result due to such attacks.