

Attack :-

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. Security attacks can be classified into passive and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

2) Differentiate b/w Active and passive attack.

Active attack

passive attack

In active attack, modification in information take place. active attack is stronger for

While in passive attack, 1. Modification in the information does not take place.

2. Active attack is danger for integrity as well as availability.
3. In active attack attention is on detection.
4. Due to active attack system is always damaged.
5. In active attack, victim gets informed about the attack.
6. In active attack, system resources can be changed.
7. Active attack influence the services of the system.
8. Active attack is tough to restrict from entering systems or networks.
2. Passive attack is danger for confidentiality.
3. While in passive attack attention is on prevention.
4. While due to passive attack, there is no any harm to the system.
5. In passive attack, victim does not get informed about the attack.
6. In passive attack, system resources are not change.
7. In passive attack, information and messages in the system or network are acquired.
8. Passive attack is easy to prohibited in comparison to active attack.

Ans Internetwork Security :

Internet Security relies on specific resources and standards for protecting data that gets sent through the internet. Internet Security is a branch of computer security specifically related to the internet, often involving browser security but also network security on a more general level, as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the internet.

* The internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing.

* Online viruses, trojans, worms and more.

Many methods are used to protect the transfer of data, including encryption and from-the-ground-up engineering.