Difference between passive and active security threats.

|  |  |
| --- | --- |
| In an active attack, Modification in information takes place. | While in passive attack, Modification in the information does not take place. |
| Active Attack is a danger to Integrity as well as availability. | Passive Attack is a danger to Confidentiality. |
| In an active attack, attention is on prevention. | While in passive attack attention is on detection. |
| Due to active attacks, the execution system is always damaged. | While due to passive attack, there is no harm to the system. |
| In an active attack, Victim gets informed about the attack. | While in a passive attack, Victim does not get informed about the attack. |
| In an active attack, System resources can be changed. | While in passive attack, System resources are not changing. |
| Active attack influences the services of the system. | While in passive attack, information and messages in the system or network are acquired. |
| In an active attack, information collected through passive attacks are used during executing. | While passive attacks are performed by collecting information such as passwords, and messages by themselves. |
| Active attack is tough to restrict from entering systems or networks. | Passive Attack is easy to prohibited in comparison to active attack. |
| Can be easily detected. | Very difficult to detect. |

List and briefly define:

Categories of security mechanisms.

Security mechanisms are technical tools and techniques that are used to implement security services.

**Encipherment :**  
This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

1. **Access Control :**  
   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
2. **Notarization :**  
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
3. **Data Integrity :**  
   This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
4. **Authentication exchange :**  
   This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
5. **Bit stuffing :**  
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
6. **Digital Signature :**  
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender’s identity is to be notified.

Categories of security services.

**Security Services:**

A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. These services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service. Following are the five categories of these services:

**Authentication:** The assurance that the communicating entity is the one that it claims to be.

* **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.
* **Data-Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.

**Data Confidentiality:** Protects data from unauthorized disclosure.

**Access Control:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

**Data Integrity:** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

**Non-repudiation:** Protects against denial by one of the entities involved in a communication of having participated in all or part of the communication.

* **Proof of Origin:** Proof that the message was sent by the specified party.
* **Proof of Delivery:** Proof that the message was received by the specified party.

Discuss intrusion techniques.

A network intrusion is any unauthorized activity on a computer network.

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered.

IDS is classified into:

1. **Network Intrusion Detection System (NIDS):**  
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.
2. **Host Intrusion Detection System (HIDS):**  
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.
3. **Protocol-based Intrusion Detection System (PIDS):**  
   Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System (APIDS):**  
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.
5. **Hybrid Intrusion Detection System :**  
   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.