PAGE No.
DATE / /

Module 1 - Introduction

* Information security.

→ Infosec (Information security) is the set of strategies for managing processes, practices, policies and tools to protect information, assets from unauthorised access, use, disclosure disruption etc.

* Goals of Information security.

→ The CIA triad is widely recognized model that represents the core principles or fundamentals objectives of information security.

(C) Confidentiality

→ Refers to protection of sensitive information from unauthorized access, disclosure or exposure to individuals or entities who dont have neccessary permissions

→ Often achieved through various security measures, such as access controls, encryption and authentication mechanism.

PAGE No.
DATE / /

② Integrity

→ Integrity is the principle that emphasizes the accuracy, reliability and trustworthiness of data and information.

→ It involves ensuring that data remains unaltered and consistent throughout its life-cycle.

→ Goal is to prevent unwanted tampering and corruption of data.

③ Availability

→ Focuses on ensuring that authorised users have timely and reliable access to information and resources when needed.

→ Emphasizes on minimizing downtimes, disruptions and outages that could prevent users from accessing critical services or data.

× ×

PAGE No.
DATE / /

* Threats, Vulnerabilities and Attacks.

* Vulnerabilities -

→ A vulnerability is a flaw or a weakness in a system's design, implementation or operation and management

→ Mostly caused due to poor design, configuration mistakes or inappropriate and insecure coding techniques.

→ Eg - Using non-validated input, Not encryptin text.

* Threat

→ A threat to a computing system is a set of circumstances that has potential to cause loss or harm by breaching security. A possible danger that exploits a vulnerability.

→ Can be deliberate or accidental, can be blocked by control of vulnerability.

Eg- ① Interception - Unauthorised party gaining access to asset.

② Interuption (when an asset is unavailable, lost or damaged)

* Attacks

→ An attack is an assault on system security that derives from an intelligent threat i.e. a deliberate attempt to evade security services.

→ Eg - Trojan, DDOS.

---

* Types of vulnerabilities

→ There are 3 types of vulnerabilities

① Hardware vulnerabilities

→ These are attacks on computer systems and networks based on hardware design and manufacturing bugs

PAGE No.
DATE / /

Some examples where this exists

① Computer with conventional BIOS
② Old Routers
③ SSD Failing to Encrypt.

② Software Vulnerability.

→ Software flaw arises from misplacement of software architecture. Can also arise from bad coding practices or improper use of Encrytion Algorithms.

Some examples

① Backdoors :- Creating secret entry points to bypass normal means of authentication

② Code Exploits :- Poor coding practices.

③ Information Leaks - Info accessible to every

④

③ Data Vulnerabilities

→ Mainly caused due to unprocessed or unvalidated input in forms.

Examples:

(1) Text Input fields.

(2) Commands and data passed in URL, (GET Request)

(3) Command line input.

---

* Types of threats.

(1) Unstructured Threats :- Consists of mostly inexperienced individuals using available hacking tools like password hackers and shell scripts.

(2) Structured Threat - Consists of individuals with high-level skills actively working to compromise a system of target.

(3) External Threats :- Workers outside of the company which dont have authorised access to computer systems or network.

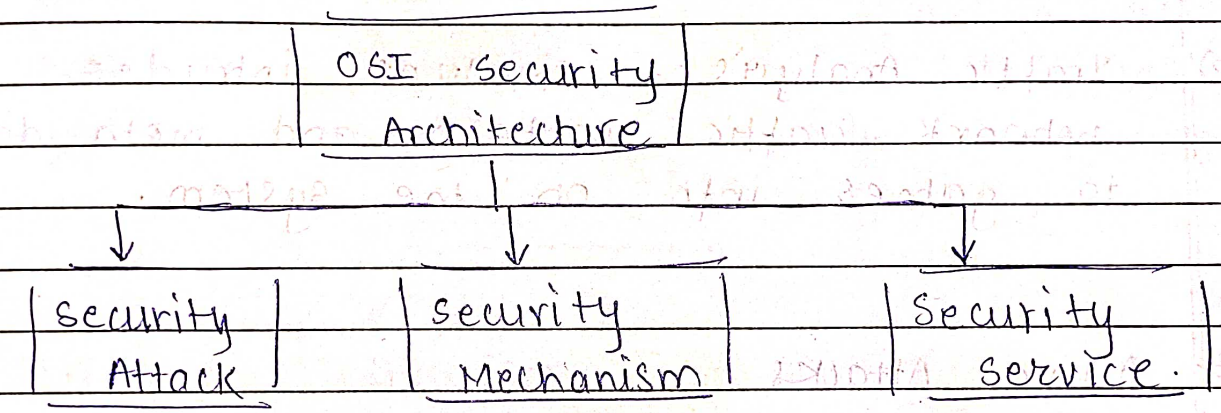
(4) Internal Threats :- Someone who has authorised access to the network.

PAGE No.
DATE / /

* OSI model for security.

→ OSI security model focuses on these concepts

a) Security Attacks
b) Security mechanism
c) Security service.



① Security Attack.

→ An attempt by a person or entity to gain unauthorised access to disrupt or compromise the security of a system.

A) Passive Attack.

Attacks in which the intruder tries to access the message/content/data being shared by the sender and receiver by keeping a close watch on the transmission

→ Both sender and reciever have no clue that the data is shared to the third-party.

a) Eavesdropping :- Involves intruder intercepting and listening in on communication b/w two or more parties without their knowledge or consent.

b) Traffic Analysis :- Involves intruder analysing network traffic pattern and meta-data to gather info on the system.

B- Active Attacks

→ Involves the intruder actively disrupting or altering system, network, or device activity. Active attacks are typically focused on causing more damage or disruption.

→ Messages show deviation from its usual behavior and are not in its usual form.

a) Masquerade :- Attacker pretends to be an authentic sender in order to gain access to the system.

PAGE No.
DATE / /

b) Replay :- Attacker intercepts a transmitted message through a passive channel.

c) Modification of Message - Involves attacker modifying the transmitted message and making the final message received by the receiver look like its not safe.

d) Denial of service (DOS) :- Involves attacker sending a large volume of traffic to the system, rendering it unavailable.

× ×

* Security Mechanism

→ Mechanism that is built to identify any breach of security or attack on the organisation, is called a security mechanism

→ Also responsible for protecting a system, network, or device against unauthorised access, tampering or other security threats

Some examples

① Encipherment (Encryption) :- Involves using algorithms to transform data in which only the person with a decryption key can read it.

b) Digital signature - It's a security mechanism that involves use of cryptographic techniques to create a unique and verifiable identifier.

c) Routing control - Allows selection of specific industry routes for data transmission and enables routing changes

---

* Security services.

→ Refers to different services available for maintaining the security and safety of an organisation.

(1) Authentication - Process of verifying the identity of a user or device.

(2) Access control - Determine who is allowed to access specific resources within a system

(3) Data confidentiality - Protection of information from being accessed by unauthorised users

(4) Data Integrity - Ensures that data has not been tampered with.