Elevate-lab-Internship-cyber-security-Task-1-

CIA Triad

- **Confidentiality**

Keeping systems and data from being accessed, seen, read to anyone who is not authorized to do so.

Information is accessible only to the autorized personnel.

ex:- Banking: Using a debit card and PIN to access your account ensures only you see your balance.

Healthcare: Encrypting patient records and requiring staff logins protects sensitive health information (HIPAA).

- **Integrity**

TRUSTWORTHINESS OF DATA OR RESOUCES: Protect the data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.

ex:- Finance: Digital signatures and transaction logs verify that money transfers haven't been altered.

Software Downloads: Verifying a software's hash (digital fingerprint) against the vendor's confirms it's not malicious.

- **Availability**

ACCESSIBLE WHEN REQUIRED BY AUTHORIZED USERS: Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

ex:- ATMs: Public access ensures you can get cash anytime, backed by robust systems.

E-commerce: Redundant servers and load balancing keep sites like Amazon running during high traffic.

Hospitals: 24/7 access to electronic health records (EHRs) is critical for emergency care.

Different type of attacks:-

> - **Black Hat** - Hackers that seek to perform malicious activities.

> - **Gray Hat** - Hackers that perform good or bad activities but do not have the permission of the organization they are hacking against.

> - **White Hat** - Ethical hackers; They use their skills to improve security by exposing vulnerabilities before malicious hackers.

Script Kiddie / Skiddies - Unskilled individual who uses malicious scripts or programs, such as a web shell, developed by others to attack computer systems and networks and deface websites.

State-Sponsored Hacker - Hacker that is hired by a government or entity related.

Hacktivist - Someone who hacks for a cause; political agenda.

Suicide Hackers - Are hackers that are not afraid of going jail or facing any sort of punishment; hack to get the job done.

Type of Attack Surfaces:-

An attack surface is the total number of points in a cloud and/or on-premise infrastructure where an unauthorized user, like a threat actor, can try to enter to cause havoc or extract data. The attack surface definition includes everything from applications, websites, networks, devices and cloud infrastructure and services, and commonly these are manifested as exposed login pages and cloud misconfigurations to employee endpoints and third-party integrations. Basically, it's the available area for potentially initiating a cyberattack.

Common attack surface examples include applications, websites, networks, devices, cloud infrastructure and services, and third-party integrations.

In simple terms, the larger your attack surface, the more chances a threat actor has to find a threat exposure, or weak spot.

Attack surfaces can include:

Digital Attack Surface / Cyber Asset Attack Surface

Physical Attack Surface

Cloud Attack Surface

Social Engineer Attack Surface / Human Attack Surface

In fact, 70% of cyberattacks exploit known vulnerabilities that remain unpatched in an organization's security attack surface. This shows how important it is to understand and manage every potential entry point through attack surface management practices.

OWASP TOP 10:-

A01:2025 - Broken Access Control

A02:2025 - Security Misconfiguration

A03:2025 - Software Supply Chain Failures

A04:2025 - Cryptographic Failures

A05:2025 - Injection

A06:2025 - Insecure Design

A07:2025 - Authentication Failures

A08:2025 - Software or Data Integrity Failures

A09:2025 - Security Logging and Alerting Failures

A10:2025 - Mishandling of Exceptional Conditions

6. Data Flow from User → Application → Server → Database [1]

The data flow in typical daily applications follows a standard client-server architecture. For the specified applications (email, WhatsApp, banking apps), the process is as follows:

- User (Client-side interaction): The user interacts with the application interface on their device (phone, computer) by inputting data such as login credentials, messages, or transaction details. The application captures this input.

- Application (Client-side processing/Network Transmission): The application formats the user input into a request, typically an HTTPS request for secure transmission, and sends it over the network (internet/mobile network). This data is encrypted in transit.

- Server (Server-side processing): The application's backend server receives the request. It processes the data, enforces business logic (e.g., verifying credentials, checking account balances), and determines if interaction with the database is necessary.

- Database (Data storage/retrieval): If required, the server interacts with the database management system (DBMS) to store new data (e.g., a new message) or retrieve existing data (e.g., account balance). The database then sends the requested information back to the server.

- Response (Server → Application → User): The server prepares a response, which is then sent back to the client application over the network (encrypted). The application receives the response and presents the relevant information or confirmation to the user. [3, 4, 5, 6, 7]

7. Identification of Attack Points during Data Flow [8]

Attacks can occur at various points throughout the data flow:

- User/Client Device:

    - Malware: Malicious apps or software on the device can capture input (keylogging) or access data stored insecurely on the device.
    - Phishing/Social Engineering: Attackers trick users into revealing sensitive information through fake login screens or messages.
    - Insecure Data Storage: If sensitive information is stored insecurely on the local device, a breach of the device can expose it.

- During Network Transmission (In Transit):

    - Man-in-the-Middle (MITM) Attacks: On an unsecured Wi-Fi network, an attacker can intercept communication between the application and the server if encryption is inadequate or compromised (e.g., weak TLS enforcement).
    - Eavesdropping: Attackers can "listen in" on network traffic to collect credentials or other confidential information if data is sent over unencrypted channels.

- Server-Side:

    - Weak API Security: APIs without proper authentication or authorization can be exploited to gain unauthorized access or perform fraudulent actions.
    - Insufficient Input Validation: Failing to validate user input can lead to attacks like SQL injection or Cross-Site Scripting (XSS), where malicious code is executed on the server or other users' devices.
    - Improper Session Management: Insecure session tokens allow attackers to hijack user sessions and perform actions on their behalf.

- Database:

    - SQL Injection: Attackers can use the application's input fields to inject malicious SQL commands, potentially leading to data theft, modification, or deletion.
    - Insider Threats: Individuals with legitimate access to the database (e.g., system administrators, contractors) can misuse their privileges to leak or modify data.
    - Insecure Configuration: Unpatched vulnerabilities in the database management system software can be exploited by attackers. [10, 11, 12, 13, 14]

8. Summary of Understanding

Daily-used applications like email, WhatsApp, and banking apps rely on data flowing between the user's device, the application's servers, and its databases. The attack surface encompasses all points where an unauthorized user can try to enter or extract data, including the client application, the network connection, the server infrastructure, and the database. [15, 16, 17, 18]

Vulnerabilities can exist at each stage: users are susceptible to social engineering, network traffic can be intercepted via MITM attacks, application servers are targets for web attacks (like SQL injection or XSS), and databases can be compromised by insider threats or configuration weaknesses. Security measures such as strong encryption (both in transit and at rest), input validation, secure authentication (like MFA), and regular security updates are essential to mitigate these risks. [11, 19, 20, 21, 22]