

1.The CIA triad is the foundation of cybersecurity. It has three core goals they are:

CONFIDENTIALITY : The information is only accessible only to authorized people

Eg: only admin can access passwords

INTEGRITY : ensures that data is accurate, complete and not altered without permission.

Hashing(SHA-256)

Eg attacks : MITM attacks

AVAILABILITY: Ensures the systems and data are available when needed.

Eg: an ecommerce site is busy during festival seasons so proper load balancing is needed with scalable server storage.

2.Types of attackers

1. Script Kiddies : they are probably beginners with low level skill sets and understanding about cyber attacks who rely on ready made tools. Eg: running Metasploit without understanding how those tools work.
2. Black hat hackers : skilled people who can write tools for their specific attack surfaces and are anonymous eg: stealing data and selling it in the dark web.
3. Hacktivists : They are groups or individual who use their skills for political or social causes eg:for spreading message or for financial gains

4. Insiders : Employees or Ex-employees of a company who have a grudge against the company or they leak information of the company for money.
5. Nation-State actors : They are government sponsored attackers who work on the motives of a political party or for a country eg:cyber attacks between countries.

3.ATTACK SURFACES:

Attack surfaces are the total number of entry points an attacker can use to compromise a system.

DIGITAL ATTACK SURFACES: Websites,APIs,Login pages,open ports,applications. Each endpoints are an attack system.

Physical Attack Surfaces: Usb Ports,Laptops,servers, Cctv. Eg:A malicious usb inserted into an office system.

4.OWASP Top 10

OWASP Top 10 lists the most critical web application vulnerabilities.

Broken Access Control : Users access admin features without permission.

Cryptographic Failures : Weak encryption or storing passwords in plain text.

SQL Injection : Attacker executes malicious queries.

Insecure Design : Security not considered during planning.

Security Misconfiguration : Default passwords, open admin panels.

Vulnerable Components : Using outdated libraries.

Identification & Authentication Failures : Weak passwords, no rate limiting.

Software or Data Integrity Failures : Focuses on code and data being tampered.

Logging and Alerting Failures : Inadequate logging allows attackers to remain in a system for long periods.

Software supply chain failures : failures in software lifecycle

Mishandling of Exceptional Conditions: If an application fails open during an error it bypass security checks.

OWASP is used by developers, pentesters, auditors Industry standard for secure coding.

5. Mapping daily apps to attack surfaces:

Email : Phishing Emails, malicious attachments.

Attack surface : inbox, spams and links

Whatsapp : APIs, medias, fake accounts sending malicious links and files.

Attack surface: Mobile app, servers, encryption keys.

Online Banking : Login, APIs, Kyc verification, database.

Attack surface: apps, server APIs, cloud.

6.Data flow

User : Enters data to login,messages,payment

Application : mobile/web app sends request

Server : processes the request and validates the input

Database : Stores or retrieves the data

Response : sent back to user.

7.Where attack can happen

User : Phishing emails, credential theft like username and banking details

App : Reverse engineering, tampering

Network : MITM, packet sniffing

Server : SQL injection

Database : Data exfiltration

API : Broken authentication

Attackers always look for the weakest link, not the strongest defense.

8.Summary

Cybersecurity is about protecting data and systems using CIA and other frameworks. Attackers vary from beginners to nation-state actors each with individual goals and motives.

There are multiple attack surfaces such as web apps, APIs, mobile applications, networks and cloud. Daily used apps like Whatsapp and other social medias use these data flow from user to database.

OWASP top 10 are the top ten attacks which helps to identify about the vulnerabilities so developers and security professionals can secure systems effectively.