TASK - 1
CYBERSECURITY: CIA TRIAD, ATTACK TYPES, AND ATTACK SURFACES

1) What is Cybersecurity?

Cybersecurity is the practice of protecting computers, networks, applications, and data from unauthorized access, attacks, damage, or misuse.
Its main goal is to keep information safe and systems running properly.

Cybersecurity is based on three core principles known as the **CIA Triad:**

- Confidentiality
- Integrity
- Availability

2) CIA Triad

2.1 Confidentiality

Confidentiality means that information should be accessible only to **authorized users**.

Examples:

- In a banking application, only the account holder should see their balance.
- In social media such as WhatsApp, only the sender and receiver should read messages.

If confidentiality is compromised:

- Personal or sensitive data may be leaked.
- Hackers may steal passwords or private information.

2.2 Integrity

Integrity means that data should remain accurate and should not be changed without permission.

Examples:

- Bank transaction records should not be altered.
- Student exam marks should not be modified illegally.

If integrity is compromised:

- Data manipulation or fraud can occur.
- Trust in the system is lost.

2.3 Availability

Availability means that systems and data should be accessible whenever users need them.

Examples:

- ATM services should be available 24/7.
- Email and cloud services should not go down frequently.

If availability is compromised:

- Services may crash or become unavailable.
- Users cannot access important systems.

3) Types of Attackers?

Cybersecurity classifies attackers in two different ways:

3.1Classification by ROLE :

3.1.1 White Hat Hackers

White hat hackers are **ethical hackers** who legally test systems to find security weaknesses.

Motivation:

- Improve security.
- Protect systems.

Example:

- A company hiring a hacker to perform penetration testing.

3.1.2 Black Hat Hackers

Black hat hackers perform **illegal hacking** for personal or financial gain.

Motivation:

- Money.
- Data theft.

- Damage systems.

Example:

- Stealing banking credentials.
- Ransomware attacks.

3.1.3 Grey Hat Hackers

Grey hat hackers fall between white hat and black hat.

Motivation:

- Curiosity.
- Reputation.
- Sometimes helping without permission.

Example:

- Finding a vulnerability and reporting it without approval.

3.2 Classification by SKILL LEVEL & PURPOSE :

3.2.1 Script Kiddies

Script kiddies are beginners who use ready-made hacking tools without deep technical knowledge.

Motivation:

- Fun, curiosity, or experimentation.

Example:

- Using free tools to deface websites or crack passwords.

3.2.2 Insider Attackers

Insiders are employees or trusted users who already have access to the system.

Motivation:

- Revenge, money, or mistakes.

Example:

- An employee leaking company data.

3.2.3 Hacktivists

Hacktivists attack systems for political or social reasons.

Motivation:

- To promote an ideology or protest.

Example:

- Defacing government or organization websites.

3.2.4 Nation-State Attackers

Nation-state attackers are highly skilled hackers supported by governments.

Motivation:

- National security, or cyber warfare.

Example:

- Attacking power grids, defense systems, or large organizations.

4) Attack Surfaces?

An attack surface is any point where an attacker can try to enter or exploit a system.

Common Attack Surfaces:

- Web applications (login pages, forms).
- Mobile applications.
- APIs.
- Networks (Wi-Fi, routers).
- Cloud infrastructure (servers, storage).

A larger attack surface increases the risk of attacks.

5) OWASP Top 10 Vulnerabilities.

OWASP Top 10 lists the most critical web application security risks.

Major OWASP Vulnerabilities:

1. **Broken Access Control**
   Users can access unauthorized data or features.

2. **Cryptographic Failures**
   Sensitive data is not properly encrypted.
3. **Injection Attacks**
   Malicious input is sent to databases or systems.
4. **Insecure Design**
   Security is not considered during application design.
5. **Security Misconfiguration**
   Default settings, open ports, or weak configurations.
6. **Vulnerable and Outdated Components**
   Using old libraries or software.
7. **Authentication Failures**
   Weak passwords or missing multi-factor authentication.
8. **Software and Data Integrity Failures**
   Using untrusted updates or code.
9. **Logging and Monitoring Failures**
   Attacks are not detected in time.
10. **Server-Side Request Forgery (SSRF)**
    The server is tricked into making malicious requests.

6) Daily Applications and Their Attack Surfaces.

Application	Possible Attack Surface
Email	Phishing, weak passwords
WhatsApp	Account takeover, SIM swapping
Banking Apps	Fake apps, insecure APIs
Social Media	Credential stuffing, data leaks

7) Data Flow in Applications.

Typical data flow in an application:

`User → Application → Server → Database.`

Example (Banking App):

1. User enters login details.
2. Application sends data to the server.
3. Server verifies data with the database.
4. Response is sent back to the user.

8. Where Attacks Can Occur in Data Flow

Stage	Possible Attack
User	Phishing, fake applications
Application	Insecure storage
Network	Man-in-the-middle attacks
Server	Injection attacks
Database	Data breaches

9) Summary

Cybersecurity focuses on protecting data, systems, and applications from cyber attacks. The CIA Triad explains the main goals of cybersecurity. Confidentiality ensures that information is accessed only by authorized users, integrity ensures that data is not changed without permission, and availability ensures that systems and services remain accessible when required.

There are different types of attackers with different motivations. Script kiddies use simple tools, insiders misuse trusted access, hacktivists attack for social or political reasons, and nation-state attackers perform advanced cyber attacks. These attackers usually target common systems like web applications, mobile apps, networks, and cloud platforms. Data flows from the user to the application, server, and database, and attacks can occur at any stage. Using strong authentication, regular updates, and proper monitoring helps reduce security risks.