TASK 1 : Understanding Cyber Security Basics & Attack Surfaces

1: What is Cyber Security?

Cyber Security means:

> Protecting computers, apps, websites, and data from hackers and misuse.

Example:

- Bank app → protecting money
- WhatsApp → protecting chats
- Gmail → protecting emails

CIA Triad

CIA = **Confidentiality, Integrity, Availability**

I.Confidentiality (Privacy)

Only the **right person** should see the data

Example:

- Your WhatsApp chats
- Your ATM PIN

If hacker reads it → confidentiality broken

II.Integrity (No change)

Data should **not be altered**

Example:

- Bank balance = ₹10,000
  If hacker changes it to ₹1,00,000 → integrity broken

III.Availability (Always accessible)

Data/app should be available when needed

Example:

- Banking app down during payment
- Website not opening

If server crashes or DDoS attack → availability broken

2: Types of Hackers (Attackers)

Write **simple points**, like this:

I.Script Kiddies

- Beginners
- Use ready-made tools
- No deep knowledge

Example: Download hacking tools from YouTube

II. Insiders

- Employees or trusted people
- Misuse access

Example: Company employee stealing data

III. Hacktivists

- Hack for political/social reasons

Example: Defacing a government website

IV.Nation-State Hackers

- Government-sponsored hackers
- Very powerful

Example: Cyber attacks between countries

3: What is an Attack Surface?

Attack Surface = All possible entry points for hackers

imagine like:

> “From where can a hacker attack?”

Examples:

- Login page
- Mobile app
- Wi-Fi network
- Cloud server

Common Attack Surfaces

I.Web Applications

- Websites and web portals
- Login pages, forms, dashboards

Example: Banking website, shopping website

II. Mobile Applications

- Apps installed on smartphones

Example: WhatsApp, Paytm, Instagram

III. APIs

- Used for communication between apps and servers

Example: Payment API, login API

IV. Network

- Internet connections and internal networks

Example: Wi-Fi, routers, firewalls

V. Cloud Infrastructure

- Online servers and storage

Example: AWS, Google Cloud, Azure

4: OWASP Top 10

OWASP stands for
Open Web Application Security Project

OWASP is a **non-profit organization** that helps people learn how to make **web applications secure**.

Why is OWASP important?

- It provides **free security guidelines**
- It helps developers and security teams
- It identifies **common security risks** in websites

What is OWASP Top 10?

OWASP Top 10 is a list of the **10 most common and dangerous web application security vulnerabilities**.

Examples:

- SQL Injection
- Broken Authentication
- Cross-Site Scripting XSS (similar to sql injection)

5: Map Daily Apps to Attack Surface

App	Possible Attack Surface
WhatsApp	Mobile app, server, network
Gmail	Web app, API, cloud
Banking App	Mobile app, database

6: Data Flow

`User → Application → Server → Database`

Explain:

- User enters data
- App sends it to server
- Server stores it in database

7: Where Attacks Can Happen During the Flow?

- During login (password attack)
- While data is sent (man-in-the-middle)
- Database hacking
- Server misconfiguration

8 : Summary

CIA Triad

CIA triad is the basic rule of cyber security.

- **Confidentiality:** Only the right person can see the data.
- **Integrity:** Data should not be changed.
- **Availability:** Data should be available when needed.

Attack Types

Attack types are different ways hackers attack systems.

- **Phishing:** Fooling users to get passwords.
- **Malware:** Harmful software.
- **SQL Injection:** Attacking databases.
- **XSS:** Injecting script into websites.

Attack Surfaces

Attack surface means the places where hackers can attack.
Major attack surfaces are:

- Web applications
- Mobile applications
- APIs
- Network
- Cloud