TASK – 1

Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cyber Security is the protection of computer systems, mobile devices, servers, networks and data from digital attacks. These attacks are performed to steal information, change data, or destroy systems.

2. CIA Triad

Principle	Description	Example
Confidentiality	Data must be accessed only by authorized users	OTP for bank login
Integrity	Data should not be changed illegally	Marks stored in college database
Availability	Data should be accessible whenever needed	ATM services

3. Types of Cyber Attackers

Attacker	Description
Script Kiddies	Beginners using ready-made hacking tools
Insiders	Employees misusing access
Hacktivists	Hackers with social or political motives
Cyber Criminals	Hackers aiming for money
Nation State Attackers	Government-sponsored hackers

4. What is Attack Surface?

Attack Surface is the total number of entry points where attackers can try to enter a system.

Common Attack Surfaces

- Web Applications
- Mobile Applications
- APIs

- Network Devices
- Cloud Infrastructure

5. OWASP Top 10

OWASP Top 10 is a list of most critical web security risks.

Vulnerability	Description
SQL Injection	Database hacking
Broken Authentication	Weak login security
Cross Site Scripting (XSS)	Script injection
Security Misconfiguration	Wrong server settings
Sensitive Data Exposure	Leakage of passwords & data

6. Mapping Daily Applications

In any online system (like Gmail, WhatsApp, Banking Apps), data moves through four main stages:

User → Application → Server → Database

Let us understand each step clearly.

1️⃣ User

The user is the person who enters data into the system.

Examples:

- Entering username & password
- Sending a message on WhatsApp
- Making an online payment

Data at this stage:
Personal details, passwords, OTPs, messages, card numbers.

2️⃣ Application

The application is the software used by the user (mobile app or website).

Functions:

- Takes user input

- Sends it to the server
- Shows response to user

Examples:

- WhatsApp app
- Banking website
- Gmail mobile app

3️⃣ Server

The server is the main system that processes user requests.

Functions:

- Validates login details
- Processes payments
- Controls communication between app and database

4️⃣ Database

The database is where all data is permanently stored.

Stored Data:

- Usernames & passwords
- Bank account data
- Chat messages
- Transaction history

Application	Possible Attacks
Gmail	Phishing
WhatsApp	Malware links
Banking Apps	OTP theft
Instagram	Account hijacking

7. Data Flow

User → Application → Server → Database

Data Flow Stage	Possible Attacks	Explanation
User	Phishing	Fake emails/websites steal login info
Application	Malware	Fake apps install viruses
Server	DDoS Attack	Floods server and makes it unavailable
Database	SQL Injection	Hackers steal or delete data

Real Example (Banking App)

Stage	Example Attack
User	Fake SMS asking for OTP
Application	Fake banking app
Server	Server overload attack
Database	Account balance manipulation

8. Attack Points in Data Flow

Level	Possible Attack
User	Phishing
Application	Malware
Server	DDoS
Database	SQL Injection