Cybersecurity Fundamentals – Learning Summary

1. Cybersecurity & CIA Triad

Cybersecurity is the practice of protecting systems, networks, applications, and data from cyber threats. The CIA Triad consists of Confidentiality, Integrity, and Availability, which together ensure data privacy, accuracy, and system accessibility.

1. Confidentiality: Protects data from unauthorized access using encryption and authentication.
2. Integrity: Ensures data is not altered or tampered with.
3. Availability: Ensures systems and services remain accessible when needed.

2. Common Attack Surfaces

Attack surfaces are points where attackers can attempt to gain unauthorized access. Common attack surfaces include web applications, APIs, mobile applications, networks, and cloud infrastructure.

1. Web Applications – vulnerable forms, login pages, cookies.
2. APIs – exposed endpoints, weak authorization.
3. Mobile Applications – insecure storage, permissions.
4. Networks – open ports, public Wi-Fi.
5. Cloud Infrastructure – misconfigured storage and IAM.

3. Daily Used Applications & Attack Surfaces

1. Email: phishing links, malicious attachments.
2. Messaging Apps: malicious links, OTP interception.
3. Banking Apps: login pages, APIs, network communication.

4. Data Flow & Attack Points

Data flows from the user to the application, then to the server, and finally to the database. At each stage, attackers may exploit vulnerabilities.

1. User Level – phishing and social engineering.
2. Application Level – XSS and CSRF.
3. Network Level – Man-in-the-Middle attacks.
4. Server Level – broken access control.
5. Database Level – SQL injection.

5. OWASP Top 10 Overview

The OWASP Top 10 highlights the most critical web application security risks. It includes issues such as broken access control, injection, insecure design, security misconfiguration, and vulnerable components.