1. Cyber Security and CIA Triad

Cyber Security is the practice of protecting systems, networks, and data from digital attacks.

The CIA Triad is the foundation of cyber security:

• Confidentiality – Ensures information is accessible only to authorized users.
 Example: Banking passwords, WhatsApp chats.

• Integrity – Ensures data is not altered by unauthorized users.
 Example: Bank balance accuracy.

• Availability – Ensures systems are accessible when required.
 Example: Online banking services available 24/7.

2. Types of Cyber Attackers

• Script Kiddies – Beginners using ready-made tools

• Insiders – Employees misusing authorized access

• Hacktivists – Socially or politically motivated attackers

• Nation-State Actors – Government-sponsored hackers.

3. Attack Surface

An attack surface refers to all the possible entry points through which an attacker can exploit a system.

Common attack surfaces include:
 • Web applications
 • Mobile applications
 • APIs
 • Networks
 • Cloud infrastructure

4. OWASP Top 10

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

Examples include:
 • SQL Injection
 • Cross-Site Scripting (XSS)
 • Broken Authentication

OWASP Top 10 helps improve application security awareness.

5. Daily Applications and Attack Surface

• Email – Login page, phishing emails, attachments
• WhatsApp – Messages, authentication, backend servers
• Banking App – Login, transactions, database

6. Data Flow in Applications

User →Application → Server → Database

7. Possible Attack Points

• User – Phishing attacks
• Application – Malware
• Network – Man-in-the-middle attacks
• Server – SQL Injection
• Database – Data breach

8. Summary

9. This task helped me understand cyber security basics, attacker types, attack surfaces, and OWASP Top 10 vulnerabilities. It improved my awareness of real-world cyber threats.