Task 1: Understanding Cyber Security Basics & Attack Surface

1. Cyber Security and CIA Triad

Cyber security is the practice of protecting systems, networks, and data from digital attacks. It focuses on three main principles known as the CIA triad: Confidentiality, Integrity, and Availability.

Confidentiality: Ensures that information is accessible only to authorized users. For example, banking apps protect account details using authentication and encryption.

Integrity: Ensures that data remains accurate and is not modified without permission. For example, transaction details in banking systems should not be altered.

Availability: Ensures that systems and services are accessible when required. For example, email and ATM services should be available at all times.

2. Types of Attackers

Script kiddies are beginners who use existing tools without deep knowledge. Insiders are employees or trusted users who misuse their access. Hacktivists attack systems to promote social or political causes. Nation-state attackers are government-backed groups with advanced skills and resources.

3. Attack Surfaces

An attack surface includes all possible entry points an attacker can exploit. Common attack surfaces include web applications, mobile applications, APIs, networks, and cloud infrastructure.

4. OWASP Top 10 Overview

OWASP Top 10 highlights the most critical web application security risks. These include injection attacks, broken authentication, sensitive data exposure, security misconfiguration, and cross-site scripting.

5. Data Flow and Attack Points

A typical data flow follows this path: User to Application to Server to Database. Attacks can occur at each stage, such as phishing at the user level, injection attacks at the server level, and data breaches at the database level.

6. Conclusion

Understanding cyber security basics, attacker types, attack surfaces, and data flow provides a strong foundation for identifying and preventing cyber threats.