Cyber Security Internship – Task 1

Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security :

Cyber security is the practice of protecting computer systems, networks, applications, and data from digital attacks. These attacks aim to steal information, disrupt services, or gain unauthorized access to systems.

In today's digital world, cyber security is important for protecting personal data, financial information, and organizational system.

2. CIA Triad :

The CIA Triad forms the foundation of cyber security.

a) Confidentiality

Confidentiality ensures that information is accessible only to authorized users.

Examples:

- Banking apps protect account details using passwords and OTPs
- WhatsApp uses end-to-end encryption to protect messages

If confidentiality is broken, sensitive data may be leaked.

b) Integrity

Integrity ensures that data remains accurate and unaltered.

Examples:

- Online transactions where the amount should not change
- Social media posts should not be modified by others

Loss of integrity can result in fraud or misinformation.

c) Availability

Availability ensures that systems and data are accessible when required.

Examples:

- Banking services available 24/7
- Email servers remaining online

Attacks like DDoS can affect availability.

3. Types of Cyber Attackers :

Script Kiddies

Beginner attackers using ready-made tools without deep knowledge.

Insiders

Employees or trusted users misusing authorized access.

Hacktivists

Attackers motivated by political or social causes.

Cyber Criminals

Financially motivated attackers using phishing and ransomware.

Nation-State Actors

Government-backed hackers targeting critical systems.

4. Attack Surfaces :

An attack surface is any point where an attacker can attempt to access a system.

Common attack surfaces include:

- Web applications
- Mobile applications
- APIs
- Networks
- Cloud infrastructure

Larger attack surfaces increase security risk.

5. OWASP Top 10 Overview

OWASP Top 10 lists the most critical web application security risks.

Some important vulnerabilities:

- Broken Access Control
- Injection
- Security Misconfiguration
- Cryptographic Failures

These vulnerabilities are dangerous because they can lead to data breaches and system compromise.

6. Mapping Daily-Use Applications to Attack Surfaces

Email

- Phishing emails
- Malicious attachments

WhatsApp

- Fake links
- Account hijacking

Banking Apps

- Credential theft
- Man-in-the-middle attacks

7. Data Flow in Applications

A typical application data flow is:

User → Application → Server → Database

8. Possible Attack Points

- User level: phishing, weak passwords
- Application level: injection, XSS

- Server level: misconfiguration
- Database level: unauthorized access

9. Summary

Cyber security focuses on protecting systems using confidentiality, integrity, and availability. Understanding attackers, attack surfaces, and data flow helps in identifying vulnerabilities and preventing cyber attacks. OWASP Top 10 provides guidance on major security risks.