Cyber Security Internship – Task 1

Understanding Cyber Security Basics & Attack Surface

What is Cyber Security?

Cyber security means protecting computers, mobile phones, networks, applications, and data from hackers and cyber attacks. Its main purpose is to keep personal and sensitive information safe while using the internet, online banking, email, social media, and cloud services.

CIA Triad

The CIA Triad is the foundation of cyber security. It focuses on three key principles that protect information systems.

Confidentiality

Confidentiality ensures only authorized users can access sensitive data.

- Bank account details are protected using passwords and OTPs.
- WhatsApp messages are encrypted and private.

Integrity

Integrity ensures data remains accurate and unaltered.

- Online transaction amounts should not change.
- Student marks must not be modified illegally.

Availability

Availability ensures systems and services are accessible when needed.

- Banking applications should work 24/7.
- Websites should remain accessible during peak traffic.

Types of Cyber Attackers

- **Script Kiddies:** Beginners using ready-made hacking tools.
- **Insiders:** Trusted users misusing access.
- **Hacktivists:** Politically or socially motivated attackers.
- **Nation-State Attackers:** Government-backed attackers targeting critical systems.

What is an Attack Surface?

An attack surface includes all points where an attacker can attempt to access or compromise a system. More attack surfaces increase the chances of security breaches.

Common Attack Surfaces

- Web applications such as login pages and forms.
- Mobile applications.
- APIs.
- Networks like Wi-Fi and routers.
- Cloud servers and storage.

OWASP Top 10

OWASP Top 10 lists the most critical web application security risks responsible for many cyber attacks.

- SQL Injection
- Weak authentication and passwords
- Security misconfigurations

Daily Applications and Possible Attacks

- **Email:** Phishing, fake links, malware attachments.
- **WhatsApp:** Fake messages, malicious links, account hijacking.
- **Banking Apps:** Password theft, fake apps, network attacks.

Data Flow in an Application

User → Application → Server → Database

- User enters data into the application.
- Application sends data to the server.
- Server processes the request.
- Database stores or returns the data.

Where Attacks Can Happen

- User side: phishing and fake applications.
- Application side: weak authentication mechanisms.
- Server side: misconfigurations and privilege abuse.
- Database: data theft and unauthorized access.

Vulnerability vs Threat vs Risk

- **Vulnerability:** A weakness in a system.
- **Threat:** An attacker or harmful event.
- **Risk:** Potential damage if an attack succeeds.

Final Summary

Cyber security protects systems and data from cyber attacks. The CIA Triad ensures confidentiality, integrity, and availability of information. Understanding attack surfaces, attackers, and common vulnerabilities helps in preventing security incidents.