Cyber Security Internship - Task-1

Student Name: Akula Danu Teja

University: Aditya University

Task 1: Cyber Security Basics & Attack Surface

1. What is Cyber Security?

Cyber Security is the practice of protecting systems, networks, and data from digital attacks. These attacks aim to access, steal, modify, or destroy sensitive information or disrupt services.

CIA Triad

The core principles of cyber security are called the CIA Triad:

Confidentiality

Ensures data is accessible only to authorized users.
Example:

- **Online banking passwords**
- **WhatsApp end-to-end encryption**

Integrity

Ensures data is accurate and not altered without authorization.
Example:

- **Bank transaction amounts should not change**
- **Exam results stored in databases**

Availability

Ensures systems and data are accessible when needed.
Example:

- **Banking apps working 24/7**
- **Email servers not going down due to attacks**

2. Types of Cyber Attackers

Script Kiddies

- **Beginners using ready-made tools**
- **Motivation: Fun or curiosity**

Insiders

- **Employees or trusted users**
- **Motivation: Revenge, money, negligence**

Hacktivists

- **Politically or socially motivated**
- **Example: Website defacement for protest**

Nation-State Actors

- **Government-backed hackers**
- **Motivation: Espionage, cyber warfare**

3. Attack Surface

An attack surface is all the points where an attacker can try to enter a system.

Common Attack Surfaces

- **Web applications**
- **Mobile applications**
- **APIs**
- **Networks (Wi-Fi, routers)**
- **Cloud infrastructure**
- **Databases**

4. OWASP Top 10 (Why It Is Important)

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

Some key vulnerabilities:

1. **Broken Access Control**
2. **Cryptographic Failures**
3. **Injection (SQL Injection)**
4. **Insecure Design**
5. **Security Misconfiguration**
6. **Vulnerable Components**
7. **Authentication Failures**
8. **Software Integrity Failures**
9. **Logging & Monitoring Failures**
10. **Server-Side Request Forgery (SSRF)**

👉 **Importance:**

- **Used by companies worldwide**
- **Helps developers and security teams prevent common attacks**

5. Daily Applications & Their Attack Surfaces

Email

- **Phishing links**
- **Malware attachments**
- **Credential theft**

WhatsApp

- **Malicious links**
- **Social engineering**
- **Account takeover**

Banking Apps

- **Weak authentication**
- **Insecure APIs**
- **Man-in-the-middle attacks**

6. Data Flow in Applications

User → Application → Server → Database

Possible Attack Points

- **User input (Injection attacks)**
- **Application logic flaws**
- **Server misconfiguration**
- **Database access leaks**

7. Vulnerability vs Threat vs Risk

- **Vulnerability: Weakness in a system**
- **Threat: Potential attacker or event**
- **Risk: Impact of a threat exploiting a vulnerability**

8. Summary

Cyber security focuses on protecting data using confidentiality, integrity, and availability. Attackers use various techniques to exploit attack surfaces. Understanding OWASP Top 10 and common attack vectors helps reduce security risks and build safer systems.