CYBER SECURITY INTERNSHIP REPORT

Task 1: Understanding Cyber Security Basics & Attack Surface

1. Introduction

Cyber security refers to the practice of protecting systems, networks, applications, and data from digital attacks. These attacks aim to access, alter, or destroy sensitive information, disrupt services, or extort money. In today's digital world, cyber security is critical for applications such as banking systems, social media platforms, and cloud services.

2. CIA Triad

1. **Confidentiality:** Ensures that sensitive information is accessible only to authorized users. Example: Bank account details protected using passwords and encryption.
2. **Integrity:** Ensures that data is accurate and not altered by unauthorized users. Example: Transaction data in banking systems remains unchanged.
3. **Availability:** Ensures that systems and data are available when required. Example: Online banking services available 24/7.

3. Types of Attackers

1. **Script Kiddies:** Beginners using ready-made tools to perform attacks.
2. **Insiders:** Employees or authorized users misusing access.
3. **Hacktivists:** Attackers motivated by political or social causes.
4. **Nation-State Actors:** Government-backed attackers targeting critical infrastructure.

4. Common Attack Surfaces

1. Web Applications – SQL Injection, XSS, CSRF
2. Mobile Applications – Insecure storage, weak authentication
3. APIs – Broken authentication, data exposure
4. Networks – Man-in-the-middle attacks, DDoS
5. Cloud Infrastructure – Misconfigured storage, identity issues

5. OWASP Top 10 Overview

OWASP Top 10 represents the most critical security risks to web applications. Examples include Injection attacks, Broken Authentication, Security Misconfiguration, and Sensitive Data Exposure. These vulnerabilities are dangerous because they allow attackers to gain unauthorized access or control of applications.

6. Mapping Daily-Use Applications to Attack Surfaces

1. Email – Phishing, malware attachments
2. WhatsApp – Account takeover, social engineering
3. Banking Apps – Credential theft, man-in-the-middle attacks

7. Data Flow in Applications

Typical data flow: User → Application → Server → Database. User inputs data, the application processes it, the server handles logic, and the database stores information.

8. Possible Attack Points

1. User Level – Phishing, weak passwords
2. Application Level – Input validation flaws
3. Server Level – Misconfigurations
4. Database Level – SQL injection, unauthorized access

9. Conclusion

This task provided a strong foundation in cyber security concepts, attacker types, attack surfaces, and data flow understanding. Learning these basics helps in identifying potential threats and building secure systems.