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, and data from unauthorized access, misuse, or cyber attacks. As technology continues to evolve, most daily activities such as online banking, digital payments, communication, and cloud-based storage depend on internet-connected systems. Because sensitive personal and organizational information is continuously shared online, ensuring proper cyber security has become essential for maintaining trust and safety in the digital environment.

2. CIA Triad

The CIA triad represents the core principles of cyber security and consists of Confidentiality, Integrity, and Availability.

Confidentiality ensures that sensitive information is accessible only to authorized individuals. For example, banking credentials, personal emails, and private documents must be protected from unauthorized access. Security measures such as authentication and encryption are commonly used to maintain confidentiality.

Integrity focuses on ensuring that data remains accurate and unchanged during storage or transmission. Any unauthorized modification of information, such as altering financial records or academic data, is considered a violation of integrity.

Availability ensures that systems and services are accessible to users whenever they are needed. Attacks like Distributed Denial of Service (DDoS) can affect availability by overloading systems and causing service disruptions.

3. Types of Cyber Attackers

Different types of attackers exist in the cyber space. **Script kiddies** are individuals with limited technical skills who use readily available tools to perform attacks. **Insiders** are trusted individuals, such as employees, who misuse their authorized access. **Hacktivists** carry out attacks to support political or social causes. **Nation-state actors** are highly skilled attackers supported by governments and usually target critical infrastructure or sensitive national data.

4. Attack Surface

An attack surface refers to all possible points where an attacker can attempt to compromise a system. Common attack surfaces include web applications, mobile applications, APIs, network infrastructure, and cloud environments. A larger attack surface increases the chances of potential security breaches.

5. OWASP Top 10

The OWASP Top 10 is a globally recognized list of the most critical web application security risks. It highlights common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, and Security Misconfiguration. Understanding these risks helps developers and security professionals build more secure applications.

6. Data Flow in Applications

In a typical application, data flows from the user to the application, then to the server, and finally to the database. At each stage, security controls are required to prevent unauthorized access or misuse of data.

7. Possible Attack Points

Security threats can arise at multiple stages of the data flow, including phishing attacks and weak passwords at the user level, malicious input at the application level, server-side attacks such as DDoS, and data breaches at the database level.

8. Conclusion

This task helped in understanding fundamental cyber security concepts, common attacker types, attack surfaces, and major security risks. It also provided insight into how real-world applications operate and where security threats can occur, forming a strong foundation for further learning in cyber security.