Cyber Security Internship – Task 1

1. Introduction to Cyber Security
Cyber Security refers to the practice of protecting computer systems, networks, applications, and digital data from unauthorized access, cyber attacks, and damage. In today's digital world, cyber security plays a crucial role in safeguarding sensitive information such as banking data, personal messages, and online transactions.

2. CIA Triad
Confidentiality: Ensures that sensitive information is accessible only to authorized users. For example, banking credentials and personal chats should not be visible to unauthorized individuals.

Integrity: Ensures that data remains accurate and is not altered without permission. For instance, a user's bank balance should not be modified by an attacker.

Availability: Ensures that systems and data are available to users whenever required. Online services like banking applications should be accessible without unnecessary downtime.

3. Types of Cyber Attackers
Cyber attacks are carried out by different types of attackers. Script kiddies use pre-built tools without deep technical knowledge. Insiders are employees who misuse their authorized access. Hacktivists attack systems for political or social motives, while nation-state attackers are government-backed groups targeting critical infrastructure or sensitive information.

4. Attack Surface
An attack surface includes all possible points where an attacker can attempt to enter or exploit a system. Common attack surfaces include web applications, mobile applications, APIs, networks, and cloud infrastructure.

5. OWASP Top 10
OWASP Top 10 is a widely recognized list of the most critical security risks affecting web applications. It helps developers and security professionals understand common vulnerabilities and implement secure coding practices to reduce the risk of cyber attacks.

6. Data Flow and Possible Attack Points
In a typical application, data flows from the user to the application, then to the server, and finally to the database. Attacks can occur at various stages such as phishing at the user level, SQL injection at the application level, man-in-the-middle attacks on the network, or data breaches at the database level.

7. Conclusion
This task provides a clear understanding of fundamental cyber security concepts including the CIA triad, types of attackers, attack surfaces, and the importance of OWASP Top 10. Learning these basics helps build a strong foundation for identifying and preventing real-world cyber threats.