CYBER SECURITY INTERNSHIP
Task 1: Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cyber Security refers to the practice of protecting systems, networks, applications, and data from digital attacks. These attacks aim to steal, alter, or destroy sensitive information, disrupt services, or gain unauthorized access. With the increasing dependence on digital platforms such as banking, healthcare, education, and communication, cyber security has become a critical requirement for individuals and organizations.

2. CIA Triad

The CIA Triad represents the three fundamental principles of cyber security: Confidentiality, Integrity, and Availability.

2.1 Confidentiality

Confidentiality ensures that sensitive information is accessed only by authorized users. Examples include encrypted banking transactions, private WhatsApp messages, and secured employee data.

2.2 Integrity

Integrity ensures that data remains accurate and unaltered. For example, financial transaction records must not be modified during transfer or storage.

2.3 Availability

Availability ensures that systems and services are accessible when needed. Downtime of banking or email services can cause serious financial and operational losses.

3. Types of Cyber Attackers

Common attacker types include Script Kiddies, Insiders, Hacktivists, Cyber Criminals, and Nation-State actors. Each has different motivations ranging from curiosity to financial or political objectives.

4. Attack Surface

An attack surface is the total number of entry points through which an attacker can attempt to access a system. Reducing the attack surface minimizes security risks.

5. Common Attack Surfaces

Attack surfaces include Web Applications, Mobile Applications, APIs, Network Infrastructure, and Cloud Platforms. Each surface presents unique security challenges and vulnerabilities.

6. OWASP Top 10

OWASP Top 10 is a globally recognized list of the most critical web application security risks. It helps developers and organizations focus on the most common and impactful vulnerabilities.

7. Data Flow and Attack Points

A typical data flow follows: User → Application → Server → Database. Attacks can occur at each stage through injection, misconfiguration, or unauthorized access.

8. Vulnerability, Threat, and Risk

A Vulnerability is a weakness, a Threat is a potential danger, and Risk is the likelihood of a threat exploiting a vulnerability.

9. Conclusion

This task builds a strong foundation in cyber security concepts, attacker awareness, and attack surface understanding, which are essential for secure system design and cyber defense.