CYBER SECURITY INTERNSHIP – TASK 1 REPORT

Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cybersecurity refers to the practice of protecting computer systems, networks, applications, and data from unauthorized access, attacks, damage, or disruption. The primary objective of cybersecurity is to ensure that data remains secure, accurate, and accessible only to authorized users while systems continue to function reliably.

2. CIA Triad (Core Principles of Cyber Security)

The CIA Triad forms the foundation of cybersecurity and defines three essential security goals.

Confidentiality

Ensures that sensitive information is accessible only to authorized users. Examples include passwords, OTPs, biometrics, and end-to-end encryption.

Integrity

Ensures that data remains accurate and unaltered unless authorized. Examples include secure financial transactions and protected database records.

Availability

Ensures that systems and services are accessible when required, preventing downtime and denial of service.

3. Types of Cyber Attackers

Script Kiddies, Insiders, Hacktivists, and Nation-State attackers all pose different levels of risk depending on their skills and motivations.

4. Attack Surface

An attack surface includes all possible entry points where an attacker can attempt to exploit a system, such as web apps, mobile apps, APIs, networks, and cloud services.

5. OWASP Top 10

OWASP Top 10 highlights the most critical web application security risks, including SQL Injection, Broken Authentication, and Security Misconfiguration.

6. Mapping Daily Applications to Attack Surfaces

Email, banking, and messaging applications all expose multiple attack surfaces across users, applications, servers, and databases.

7. Data Flow and Attack Points

User → Application → Server → Database. Attacks can occur at each stage through phishing, injection attacks, misconfiguration, or unauthorized access.

8. Vulnerability, Threat, and Risk

Vulnerability is a weakness, threat is a potential attacker, and risk is the likelihood of a threat exploiting a vulnerability.

9. Conclusion

This task establishes a strong foundation in cybersecurity concepts, attacker awareness, and attack surface identification.