Cyber Security Internship – Task 1

Understanding Cyber Security Basics & Attack Surface.

Cyber Security : It is protecting systems, networks, and data from digital attacks, unauthorized access, damage, or theft. The foundation of cyber security is based on the CIA Triad, which stands for Confidentiality, Integrity, and Availability.

Confidentiality ensures that sensitive information is accessible only to authorized users.

For example, online banking passwords should only be known to the account holder, and private WhatsApp messages should not be readable by outsiders.

Integrity ensures that data remains accurate and unaltered.

For example, bank transaction amounts should not be modified by attackers, and academic records stored in databases should remain correct.

Availability ensures that systems and data are accessible whenever required. Banking applications, email services, and cloud platforms must remain operational and protected from attacks like Denial of Service.

Cyber attackers can be classified into different types:

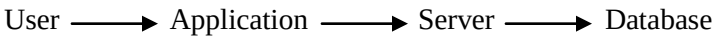
1. Script kiddies are beginners who use ready-made hacking tools without understanding them, mainly for fun or curiosity.
2. Insiders are employees or trusted individuals who misuse their access, either intentionally or accidentally.
3. Hacktivists attack systems to promote political or social causes
4. Nation-state attackers are government-sponsored hackers involved in espionage or cyber warfare.

An attack surface refers to all possible points where an attacker can attempt to enter a system. Common attack surfaces include web applications, mobile applications, APIs, networks, cloud infrastructure, and user devices. A larger attack surface increases security risks.

The OWASP Top 10 is a globally recognized list of the most critical web application security risks. It includes vulnerabilities such as SQL Injection, Cross-Site Scripting, Broken Authentication, and Security Misconfiguration. These vulnerabilities are dangerous because they can lead to data breaches and system compromise.

Daily-use applications also have attack surfaces. Email applications are vulnerable to phishing and malicious attachments. Messaging apps like WhatsApp face risks such as malware links and social engineering. Banking applications are targeted through insecure networks, fake apps, and credential theft.

Data flow in applications typically follows a path where the user inputs data, the application processes it, the server handles logic and authentication, and the database stores the data securely. Attacks can occur at each stage, including phishing at the user level, injection attacks at the application level, server misconfigurations, and database breaches.



Conclusion : This task provided a strong foundation in cyber security concepts. Understanding the CIA triad, attacker types, attack surfaces, OWASP Top 10 vulnerabilities, and data flow helps build awareness of cyber threats and prepares for advanced security learning.

SUMMARY :

This task has helped me understand the basics of cyber security, including how data is protected use the CIA triad, how attacks occur and, who the attackers are and where the systems are vulnerable in real world applications.