

Task - 1: Cyber Security Fundamentals & Attack Surface

Internship Task – Elevate Labs

Cyber Security focuses on protecting systems, networks, and data from unauthorized access, misuse, and attacks. This task explains the core cyber security concepts and how real-world applications become vulnerable.

Cyber Security Fundamentals – CIA Triad

Confidentiality: Ensures sensitive information is accessed only by authorized users. Examples include encrypted banking data, private social media messages, and secured email accounts.

Integrity: Ensures data is accurate and not altered. Bank transactions, social media content, and emails must remain unchanged.

Availability: Ensures systems and services are accessible when needed. Downtime caused by attacks directly impacts users.

Types of Cyber Attackers

Script Kiddies: Low-skill attackers using ready-made tools.

Insiders: Authorized users misusing access.

Hacktivists: Ideology-driven attackers.

Nation-State Attackers: Highly skilled government-backed groups.

Common Attack Surfaces

Web applications, mobile apps, APIs, networks, and cloud infrastructure are vulnerable due to misconfigurations, weak authentication, and coding flaws.

OWASP Top 10

OWASP Top 10 highlights the most critical web application vulnerabilities such as SQL Injection, Broken Authentication, and Cross-Site Scripting.

Data Flow

User → Application → Server → Database

Attack Points

Attacks can occur at the user level, during data transmission, on servers, and within databases.

Learning Outcome

This task improved my understanding of cyber security fundamentals, attack surfaces, and real-world application security.

