Task 1: Cyber Security Basics & Attack Surface Research

1. The CIA Triad

The CIA Triad is a foundational model used to develop security policies. It consists of three pillars:

- **Confidentiality:** Ensures that sensitive information is only accessed by authorized parties.
    - **Banking Example:** Using **encryption** and **Multi-Factor Authentication (MFA)** to ensure only the account holder can see their balance.
    - **Social Media Example:** Ensuring your **private messages (DMs)** are only visible to you and the recipient, not other users or the platform's public feed.
- **Integrity:** Guarantees that data is accurate, complete, and has not been tampered with by unauthorized users.
    - **Banking Example:** Ensuring that a transfer of **$100** is not modified to **$1000** during transmission to the bank's server.
    - **Social Media Example:** Ensuring a post you write remains exactly as you typed it and isn't altered by a hacker to spread misinformation.
- **Availability:** Ensures that systems and data are accessible to authorized users whenever they are needed.
    - **Banking Example:** Maintaining **99.9% uptime** so customers can withdraw cash from an ATM or use the mobile app at any time.
    - **Social Media Example:** Protecting servers against **DDoS attacks** to ensure the platform doesn't crash during a major global event.

2. Common Cyber Attackers

Cybersecurity threats come from various actors with different skills and motivations:

- **Script Kiddies:** Amateurs with low technical skills who use pre-written scripts or "off-the-shelf" hacking tools to launch attacks, often for thrill or minor disruption.
- **Insiders:** Current or former employees or contractors who have legitimate access to a network and misuse it—either maliciously (for revenge/profit) or accidentally (through negligence).
- **Hacktivists:** Attackers motivated by political or social causes; they use hacking (like website defacement or data leaks) to spread a message or protest against an organization.
- **Nation-State Actors:** Highly sophisticated, government-sponsored groups that conduct long-term espionage or sabotage against other nations' critical infrastructure.

3. Attack Surfaces & Application Mapping

An **attack surface** is the total sum of all points where an unauthorized user can try to enter or extract data from a system.

Common Attack Surfaces:

- **Web Applications:** Vulnerable login forms and user input fields.
- **Mobile Apps:** Insecure storage on the device or weak session management.
- **APIs:** The "bridges" between software that can be exploited if they lack proper authentication.
- **Network:** Unsecured Wi-Fi, open ports, or weak firewalls.
- **Cloud Infrastructure:** Misconfigured storage buckets (like AWS S3) that expose private data.

Application Mapping Table:

Daily Application	Primary Attack Surfaces
Email	**Network** (phishing links), **Web Application** (browser login portal)
WhatsApp	**Mobile App** (local storage), **API** (message transmission endpoints)
Banking Apps	**Mobile App** (biometric bypass), **Network** (MitM attacks on public Wi-Fi)

4. Data Flow & Attack Points

In a standard web architecture, data moves through several "trust boundaries":

User → Application → Server → Database

Where Attacks Occur:

1. **User to Application: Phishing** or **Credential Stuffing** (using stolen passwords).
2. **Application to Server: Man-in-the-Middle (MitM)** attacks where hackers intercept data in transit.
3. **Server to Database: SQL Injection (SQLi)** where an attacker sends malicious code through an input form to steal the entire database.

5. OWASP Top 10

The **OWASP Top 10** is a globally recognized list of the most critical web application security risks.

- **Why it's important:** It provides a universal standard for developers to prioritize security fixes.
- **Key Risks:** Includes **Broken Access Control** (allowing users to see others' data) and **Cryptographic Failures** (failing to encrypt sensitive info like SSNs).