Elevate Labs- cyber security task 1

1. What is Cyber Security?

Cyber Security is about protecting systems, networks, and data from digital attacks.

It is built on **three core principles** called the **CIA Triad**:

Confidentiality: Data should be seen **only by authorized people**.

Examples:

- **Banking apps**: Only *you* can see your balance and transactions.
- **Social media**: Your private messages are visible only to you and the recipient.

Threats: hacking, phishing, data leaks
Protection: passwords, encryption, authentication

Integrity : Data should **not be changed without permission**.

Examples:

- Bank transaction amount should not be altered.
- Social media posts should not be modified by others.

Threats: SQL injection, malware
Protection: hashing, access controls, validation

Availability

Systems should be **accessible when needed**.

Examples:

- Banking app must work during payments.
- WhatsApp should not go down frequently.

2. Types of Attackers

Different attackers have **different skills and motivations**:

Script Kiddies

- Beginners using ready-made tools
- Attack for fun or attention

Example: Defacing a website using downloaded scripts

Insiders

- Employees or trusted users
- Already have access

Example: Employee leaking customer data

Hacktivists

- Politically or socially motivated

Example: Hacking a website to spread a message

Nation-State Actors

- Government-backed hackers
- Very skilled and well-funded

Example: Cyber espionage, infrastructure attacks

3. Common Attack Surfaces

An **attack surface** is any place where an attacker can try to break in.

Web Applications

- Login forms, search boxes, file uploads
- Vulnerable to SQL injection, XSS

Mobile Applications

- Weak authentication
- Insecure storage of data

APIs

- Used for app–server communication
- Broken authentication or authorization

Networks

- Wi-Fi, routers, open ports
- Vulnerable to sniffing, MITM attacks

Cloud Infrastructure

- Misconfigured storage (public S3 buckets)
- Weak access policies

4. OWASP Top 10

OWASP Top 10 lists **most critical web vulnerabilities**.

Some key ones:

1. **Broken Access Control** – Users access data they shouldn't
2. **Injection (SQL, Command)** – Attacker sends malicious input
3. **Authentication Failures** – Weak login systems
4. **Sensitive Data Exposure** – Data not encrypted
5. **Security Misconfiguration** – Default passwords, open ports
6. **Vulnerable Components** – Outdated libraries
7. **XSS** – Malicious scripts run in browser
8. **Insecure Design** – Poor security planning
9. **Logging Failures** – Attacks go unnoticed
10. **SSRF** – Server makes unintended internal requests

These are dangerous because **one small bug can expose entire systems**.

5. Mapping Daily-Use Apps to Attack Surfaces

Email

- Phishing links
- Malware attachments
- Weak passwords

WhatsApp

- Account takeover
- Malware through links
- Network interception (if insecure Wi-Fi)

Banking Apps

- Credential theft
- API abuse
- Fake apps (trojans)

6. Data Flow: User → App → Server → Database

Typical flow:

1. **User** enters data (login, message, payment)
2. **Application** sends request
3. **Server** processes logic
4. **Database** stores or retrieves data
5. Response goes back to user

7. Where Attacks Can Happen in This Flow

Stage	Possible Attacks
User	Phishing, malware
App	XSS, insecure storage
Network	Man-in-the-middle
Server	Injection, authentication flaws

Database	Data breach, unauthorized access

Security is needed at every step, not just one place.

8. Final Summary (In My Own Words)

Cyber security is about protecting data and systems using confidentiality, integrity, and availability. Different attackers—from beginners to nation-state hackers—target various attack surfaces like web apps, mobile apps, APIs, and cloud systems. Everyday applications such as email, WhatsApp, and banking apps are constantly exposed to threats. By understanding how data flows from users to databases, we can identify where attacks may occur. OWASP Top 10 vulnerabilities highlight common mistakes that attackers exploit. Strong cyber security requires securing every stage of data flow and thinking like an attacker to prevent damage before it happens.

Security is needed at every step, not just one place.