Elevate Labs – Task 1:

Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cyber security refers to the practice of protecting computer systems, networks, applications, and data from unauthorized access, misuse, disruption, or damage. In today's digital environment, cyber security is essential because sensitive information such as personal details, financial data, and business records are stored and transmitted electronically. A strong cyber security framework helps organizations and individuals maintain trust, privacy, and system reliability.

2. CIA Triad

The CIA triad represents the three fundamental principles of information security: Confidentiality, Integrity, and Availability.

Confidentiality

Confidentiality ensures that information is accessible only to authorized individuals. It prevents unauthorized users from viewing or stealing sensitive data.
Example: Online banking credentials, OTPs, and private social media messages must only be accessible to the intended user.

Integrity

Integrity ensures that data remains accurate, complete, and unaltered unless modified by an authorized user.
Example: A bank account balance should not be changed by an attacker during a transaction.

Availability

Availability ensures that systems and services are accessible to users whenever required.
Example: Email services, UPI payments, and cloud platforms should remain available without unnecessary downtime.

A failure of any one of these three principles can result in a security breach.

3. Types of Cyber Attackers

Different attackers have different motivations and skill levels:

- **Script Kiddies:** Individuals with limited technical knowledge who use pre-built tools or scripts to perform attacks.
- **Insiders:** Employees or trusted individuals who misuse their authorized access to steal or damage data.
- **Hacktivists:** Attackers motivated by political or social ideologies, often targeting organizations to spread a message.

- **Cyber Criminals:** Attackers focused on financial gain through activities such as fraud, ransomware, and identity theft.
- **Nation-State Actors:** Government-sponsored attackers involved in espionage, surveillance, or cyber warfare.

4. Attack Surface

An attack surface refers to all the possible points where an attacker can attempt to gain unauthorized access to a system or exploit a vulnerability.

Common Attack Surfaces Include:

- Web applications
- Mobile applications
- Application Programming Interfaces (APIs)
- Networks and Wi-Fi connections
- Cloud infrastructure
- Databases
- User input fields and file uploads

Reducing the attack surface helps minimize the chances of a successful cyber attack.

5. Importance of OWASP Top 10

The OWASP Top 10 is a globally recognized list of the most critical web application security risks. It helps developers and security professionals understand common vulnerabilities and take preventive measures.

Examples of OWASP vulnerabilities include:

- SQL Injection
- Cross-Site Scripting (XSS)
- Broken Authentication
- Security Misconfiguration

These vulnerabilities are dangerous because they can lead to data breaches, unauthorized access, and complete system compromise. Organizations use the OWASP Top 10 as a baseline for securing web applications.

6. Mapping Daily-Used Applications to Attack Surfaces

Everyday applications also have potential attack surfaces:

Application	Possible Attack Surface
Email	Phishing emails, malware attachments
WhatsApp	Account takeover, OTP interception
Banking Apps	Credential theft, insecure APIs
Social Media	Session hijacking, XSS attacks

This shows that cyber security risks exist in applications used daily.

7. Data Flow in an Application

A typical data flow in an application is:

User → Application → Server → Database

- The user provides input through the application.
- The application sends the request to the server.
- The server processes the request.
- The database stores or retrieves data.

8. Possible Attack Points in the Data Flow

Attacks can occur at multiple stages:

- **User Level:** Phishing attacks and malware infections.
- **Application Level:** SQL Injection and Cross-Site Scripting.
- **Server Level:** Improper configuration and unpatched systems.
- **Database Level:** Unauthorized access and data breaches.

Understanding these points helps in implementing proper security controls.

9. Conclusion

This task provided a clear understanding of cyber security fundamentals, including the CIA triad, types of cyber attackers, and attack surfaces. By analyzing daily-used applications and studying OWASP Top 10 vulnerabilities, it becomes evident that security must be considered at every stage of data flow. This knowledge forms a strong foundation for identifying threats and protecting digital systems effectively.