ELEVATE LABS
TASK 1
Understanding Cyber Security Basics & Attack Surface

1. **Cyber Security**

   1. Cyber security refers to the practice of protecting systems, networks, devices, and data from cyber threats such as hacking, data breaches, malware, phishing, and unauthorized access.

   2. Its main goal is to ensure that digital information remains safe, accurate, and accessible only to authorized users.

2. **CIA Traid**

   1. The CIA Triad represents three core principles of information security:

   Confidentiality
   Integrity
   Availability

   2. Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized users and remains protected from unauthorized access.

3. Integrity

Integrity ensures that data remains accurate, complete, and unaltered during storage or transmission.

4. Availability

Availability ensures that systems, services, and data are accessible when needed by authorized users.

5. Example:-

ATM transaction: Confidentiality uses your card and PIN (multi-factor auth) to keep your info private; Integrity ensures the transaction amount is accurately recorded in your account; and Availability means the ATM is accessible for you to use it whenever you need.

3. Types of Attackers

Cyber attackers vary widely in skill level, motivation, and resources. Understanding who the attackers are helps organizations design better security controls and response strategies

1. Script Kiddies

Script kiddies are low-skill attackers who rely on pre-written tools and scripts created by others rather than developing their own exploits.

2. Insider Threats

Insiders are individuals within an organization who misuse their authorized access to systems or data. Insider threats can be intentional or accidental.

3. Hacktivists

Hacktivists use cyber attacks to promote political, social, or ideological causes rather than financial gain.

4. Nation-State Actors

Nation-state attackers are highly sophisticated groups backed by governments. They conduct cyber operations for espionage, sabotage, or geopolitical advantage.

4. Attack Surfaces

An attack surface refers to all possible entry points where an attacker can attempt to gain unauthorized access to systems, applications, or data. The larger the attack surface, the higher the risk of exploitation.

1. Web Applications

Web applications are one of the most frequently targeted attack surfaces because they are publicly accessible over the internet.

2. **Mobile Applications**

Mobile apps store sensitive data and interact with back-end servers, making them attractive targets.

3. **APIs (Application Programming Interfaces)**

APIs act as bridges between applications, enabling data exchange. Poorly secured APIs can expose sensitive data.

Networks

Networks form the backbone of digital communication and are vulnerable to both internal and external attacks.

5. Cloud Infrastructure

Cloud environments introduce shared responsibility and complex configurations, making misconfigurations a major risk.

5. OWASP Top 10

The OWASP Top 10 is a globally recognized list of the most critical web application security risks. It is created by the Open Web Application Security Project (OWASP) and is widely used by developers, security professionals, and organizations to understand common weaknesses in web applications.

1. Broken Access Control

Occurs when users can perform actions or access data beyond their intended permissions.

2. Cryptographic Failures

Sensitive data is not properly protected using encryption.

3. Injection

Untrusted input is sent to an interpreter (SQL, OS, LDAP), causing unintended execution.

4. Insecure Design

Security weaknesses caused by poor architecture or lack of security planning.

5. Security Misconfiguration

Improper security settings in applications, servers, or cloud services.

6. Vulnerable and Outdated Components

Using libraries or software with known vulnerabilities.

7. Identification and Authentication Failures

Weak authentication mechanisms allow attackers to impersonate users.

8. Software and Data Integrity Failures

Code or data integrity is not verified during updates or execution.

9. Security Logging and Monitoring Failures

Lack of proper logging and alerting for security events.

10. Server-Side Request Forgery (SSRF)

An attacker tricks the server into making unauthorized requests.

Application Type	**Key Attack Surfaces**	**Typical Threats**
Email	**Links, attachments, web login**	**Phishing, malware**
Messaging Apps	**Media files, backups, OTP**	**Social engineering**
Banking Apps	**APIs, authentication, network**	**Fraud, MitM**
Cloud Backups	**Storage access**	**Data leakage**

6. **Data Flow**

   1. User

   Enters data such as login details, messages, or payment information.

   2. Application (Frontend)

   Collects input, performs basic validation, and securely sends data to the server.

   3. Server (Backend)

   Authenticates the user, processes requests, and applies business logic.

   4.Database

   Stores, retrieves, and updates data, then sends results back to the server.

Summary

Cyber security protects systems and data from attacks by ensuring confidentiality, integrity, and availability (CIA triad). Different attackers such as script kiddies, insiders, hacktivists, and nation-state actors target systems for various motives. Common attack surfaces include web apps, mobile apps, APIs, networks, cloud services, and daily-used apps like email, messaging, and banking. The OWASP Top 10 highlights critical vulnerabilities that can lead to data breaches and fraud. Data flows from user → application → server → database, and each layer must be secured to prevent attacks.