CYBERSECURITY INTERNSHIP

Organization name: Elevate labs

TASK-1: Understanding Cybersecurity basics and attack surface

Cybersecurity:

Cybersecurity is the combination of methods, processes, tools, and behaviors that protect computer systems, networks, and data from cyberattacks and unauthorized access. The foundation of cyber security is built on the **CIA Triad.**

CIA triad:

The **CIA Triad** is the foundation of information security. It ensures that data is protected, accurate, and accessible when needed. **CIA** elaborates into **confidentiality**, **integrity** and **availability.**

- **Confidentiality:**
  Confidentiality ensures that information is accessible only to authorized users and is protected from unauthorized access or disclosure.

  Example: On platforms like Instagram or Facebook, private messages (DMs), saved passwords, and personal details such as email and phone numbers are kept confidential. Only the account owner can view private chats. End-to-end encryption protects messages. If confidentiality is compromised, private chats or photos may get leaked.

- **Integrity:**
  Integrity ensures that data remains accurate, complete, and unaltered during storage or transmission. It can be achieved by hashing, Digital signatures, Checksums, Access controls, Audit logs.

Example: When you transfer **₹10,000** to another account, the amount should not change to ₹1,000 or ₹100,000. The recipient account number must remain the same. Banks use transaction validation, hashing, and logs to ensure data is not tampered with during the transaction process. If integrity is compromised, financial records may be altered, causing fraud or incorrect balances.

- **Availability:**
  Availability ensures that systems, data, and services are accessible to authorized users whenever needed. It can be achieved by Backup systems, Redundant servers, Load balancing, DDoS protection, Disaster recovery plans.

  Example: Social media platforms must remain accessible even during peak hours or cyberattacks. Servers are distributed globally. DDoS protection prevents downtime. If availability is compromised, users cannot log in, post updates, or communicate.

Types of attackers:

Cyberattacks are often imagined as complex operations carried out by elite hackers sitting in dark rooms. In reality, attackers range from curious teenagers to well-funded government teams. Understanding these attacker profiles helps organizations design better defences and helps students grasp the real-world threat landscape.

1. **Script kiddies:**
   Script kiddies are the least skilled attackers, but they are also one of the most common. These individuals usually do not understand how attacks work internally. Instead, they rely on pre-written scripts, tools, or exploits downloaded from the internet. They often target easy and poorly secured systems, not because of a personal grudge, but simply because the system is vulnerable. Security blogs frequently describe script kiddies launching. They may not intend serious harm, but their actions can still cause damage.

2. **Insiders:**

   Insiders are individuals who already have legitimate access to systems. They may be Employees, Contractors, Vendors, Former staff with retained access. This makes insiders extremely dangerous because they bypass many security controls naturally. Insiders may act due to financial gain, Revenge or workplace conflict, Negligence (unintentional insider threat), Espionage. Security incident blogs repeatedly highlight that not all insider threats are malicious. Some occur because employees

- Click phishing emails
- Use weak passwords
- Misconfigure systems

3. **Hacktivists:**

   Hacktivists are attackers driven by ideology, politics, or social causes rather than money. Hacktivists see themselves as digital protestors, similar to street activists—but instead of banners, they use keyboards. While their intentions may feel moral to them, the damage they cause can still be severe. They usually target Government websites, Corporations, Institutions linked to controversial issues. Security blogs often report hacktivists performing Website defacement with messages, Data leaks ("name and shame" attacks), DDoS attacks during political events. Hacktivists often believe they are fighting for justice, even though their actions are illegal.

4. **Nation State actors:**

   Nation-state actors are the most sophisticated and dangerous attackers. Nation-state actors are like digital soldiers, silently operating behind the scenes. Their attacks may go unnoticed for months or years, but the damage can affect entire countries.
   According to threat intelligence blogs, nation-state attackers focus on:

- Power grids
- Financial systems
- Defence networks
- Healthcare and telecom sectors

  These attacks are often:

- Long-term
- Stealthy
- Highly targeted

Cyber attackers are not a single group, but a spectrum of individuals and organizations with different goals and abilities. From inexperienced script kiddies experimenting online, to insiders abusing trust, to hacktivists fighting for causes, and finally to nation-state actors waging silent cyber warfare—each attacker leaves a unique footprint.

Exploring Common Attack Surfaces:

An attack surface includes all the possible entry points where an attacker can attempt to exploit vulnerabilities in a system. In modern digital environments, attack surfaces have expanded rapidly due to increased connectivity and technology adoption. Web applications are common targets because they are publicly accessible and often suffer from vulnerabilities like SQL injection, cross-site scripting, or broken authentication. Mobile applications can expose sensitive data through insecure storage, weak permissions, or poorly implemented APIs. APIs themselves are critical attack surfaces since they allow communication between applications and services; if authentication or authorization is weak, attackers can extract or manipulate data. Networks present risks through open ports, outdated protocols, or misconfigured firewalls. Cloud infrastructure adds another layer of complexity, where misconfigured storage buckets, exposed access keys, or poor identity management can lead to massive data breaches. Understanding attack surfaces helps organizations reduce exposure by minimizing unnecessary services, applying security controls, and continuously monitoring systems.

Understanding OWASP Top 10 Vulnerabilities:

The OWASP Top 10 is a globally accepted awareness document that highlights the most critical security risks affecting web applications. These vulnerabilities are not theoretical; they are based on real-world data breaches and attack trends observed across industries. Issues like broken access control allow users to perform actions beyond their authorization, while injection attacks enable attackers to manipulate backend databases. Security misconfigurations, such as default passwords or exposed admin panels, create easy entry points for attackers. What makes these vulnerabilities dangerous is their widespread presence and severe impact, often leading to data theft, financial loss, or reputational damage. By studying OWASP Top 10, learners gain insight into why secure coding practices, proper

authentication, regular testing, and patch management are essential. This knowledge is especially important for beginners, as it introduces them to the most common mistakes developers make and how attackers exploit them.

Mapping Daily-Used Applications to Attack Surfaces:

Everyday applications that people rely on—such as email services, messaging apps like WhatsApp, and banking applications—are also exposed to cyber threats. Email systems are frequent targets of phishing attacks, where attackers trick users into revealing passwords or clicking malicious links. Messaging apps may be exploited through fake links, malicious attachments, or account takeover attempts. Banking applications face high-risk threats such as credential theft, insecure APIs, malware infections, or session hijacking. Mapping these commonly used applications to their respective attack surfaces helps users and learners understand that cyber security is not limited to large organizations—it directly affects individuals as well. This awareness encourages safer online behavior, such as using strong passwords, enabling two-factor authentication, and avoiding suspicious links.

Understanding Data Flow from User to Database:

Data flow describes how information moves within an application, starting from the user and ending at the database. Typically, data is entered by the user, processed by the application, transmitted to the server, and finally stored or retrieved from the database. For example, when a user logs into an application, the credentials are captured by the user interface, sent securely to the server, validated, and then matched against stored records in the database. Each stage of this flow introduces potential security risks if not properly protected. Understanding data flow is essential for identifying where security controls such as authentication, encryption, logging, and validation should be applied. A clear understanding of this process helps security professionals design systems that protect data at every stage of its journey.

Identifying Where Attacks Can Occur in the Data Flow:

Attacks can occur at multiple points throughout the data flow, making layered security essential. At the user level, attackers may use phishing techniques or fake websites to steal

credentials. At the application level, vulnerabilities like improper input validation or broken authentication can be exploited. During data transmission, attackers may intercept information through man-in-the-middle attacks if encryption is weak or absent. At the database level, attacks such as SQL injection can allow unauthorized access or data manipulation. Identifying these attack points enables organizations to implement specific safeguards—such as HTTPS, firewalls, intrusion detection systems, and database security controls—rather than relying on a single security mechanism.

Conclusion:

By clearly explaining the CIA triad, attacker types, attack surfaces, OWASP vulnerabilities, and data flow, learners move beyond rote memorization and develop conceptual clarity. This step helps connect theoretical knowledge with practical scenarios, making it easier to apply concepts in real-world environments, interviews, and future tasks. A well-written summary reflects analytical thinking, confidence, and readiness to progress further in the cyber security field.