WEEK-1

Asad Muhammad Channar
DHC-56

Task-1:

Learn Cybersecurity Basics:

Required:

- Read: Research key concepts like the CIA Triad (Confidentiality, Integrity, Availability) and common threats (e.g., malware, phishing).
- Task: Write a 1-page summary in your own words.

CIA Triad:

The CIA Triad—Confidentiality, Integrity, and Availability—is a guiding model in information security. A comprehensive information security strategy includes policies and security controls that minimize threats to these three crucial components.

In this context, **Confidentiality** is a set of high-level rules that limits access to all types of data and information. **Integrity** is the assurance that the information is trustworthy and accurate. And **Availability** is a form of risk management to guarantee reliable access to that information by authorized people.

Now we will take a look on each of CIA triad’s Principles in detail.

- **Confidentiality:**

  Roughly equivalent to privacy, confidentiality measures are designed to prevent sensitive information from unauthorized access attempts.Data is frequently categorized based on the kind and extent of harm that could be caused if it ended up in the wrong hands. Based on those categories, more or less strict data security measures can then be put in places.

  In simple words it means that data should be accessible by only those who are authorized and have right to access it .

  Confidentiality can be achieved by applying the principle of **Access Control.**

- **Integrity:**

  Throughout its whole existence, data must be kept reliable, accurate, and consistent. Data must not be modified while in transit, and precautions must be taken to prevent unauthorized parties from changing it, as in the case of data breaches.

  The most valuable asset of any organization is it’s data . Malicious actors and always try to sneak in and manipulate the data so that the authenticity of the data is lost and also the confidence of the people . So, it is essential to maintain integrity of the data.

  One common way to preserve integrity is to apply **Least Previlage Principle**.

- **Availability:**

  Information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

Availability should be ensured that rightful persons can access resources any time without any kind of interference . Sufficient security measures should be applied to maintain continuous availability . Fast, adaptive disaster recovery (DR) plans are essential for the worst-case scenarios and require a comprehensive approach.

Common Threats:

- **Malware:**

  Malware (malicious software) is designed to damage, or exploit computers and networks without the user's consent. It comes in various forms such as viruses, worms, trojans, ransomware, and spyware, each with distinct methods of attack. Malware can steal sensitive information, disrupt system operations, or allow unauthorized access to systems. It often spreads through email attachments, downloads, or vulnerabilities in software. Effective protection includes using antivirus programs, keeping software updated, and practicing safe browsing habits.

- **Phishing:**

  Phishing is a type of cyber attack where attackers attempt to deceive individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details, by pretending to be a trustworthy entity. This is often done through fake emails, messages, or websites that appear legitimate. Phishing attacks exploit human psychology, relying on urgency, fear, or curiosity to prompt users to act without caution. Protecting against phishing involves being vigilant, verifying the authenticity of requests for sensitive information, and using security tools like email filters and multi-factor authentication.