**1.  CIA Triad (Confidentiality, Integrity, Availability) and common threats (e.g., malware, phishing).**

* **Task: Write a 1-page summary in your own words.**

As we all knew, the CIA Triad as a security framework is one of values applicable here with in more traditional enterprise IT environments. Taking together, these two pillars enable the defense of sensitive data and systems with protection whatever messages are exposed outside facing either internal or external threats.

* Confidentiality

Privacy means keeping data from being accessed by people who are not authorized to look at it. Confidentiality : Organizations making information and the related resources confidential they do this by having access controls, implementation of encryption procedures along with tokenization and also use data masking techniques. Approaches that allow only the right people with credentials to see or interact with sensitive data like Personally Identifiable Information (PII) or Protected Health Information (PHI). EverydayMeasures: Multi-factor authentication (MFA) is a significant control that helps with this, not allowing access to restricted data without proper due course.

* Integrity

Data integrity guarantees that data is preserved and kept accurate throughout its lifecycle. Sensitive data breaches~ Malicious attacks or even accidental errors result in invalid insights, bad decisions & wastage of resources These cyberattacks bypass IDS can result in unauthorized changes to Data, affecting corporate decisions and all the way up to control of critical infrastructure. Widespread threats to data integrity like hacktivism, espionage and propaganda. Distrust in data integrity can seriously damage the reputation and reliability of an organization.

* Availability

Authorized users can access the data when required. Availability, meanwhile is also achieved through: secure storage systems; robust paths for data transmission, and reliable authentication mechanisms. B) Trust in the tools which claim that data is available for purchase, but different attacks can target communication platforms like phishing making it harder to differentiate between real and fake aviation info. Availability — Downtime or the inability to access data cripples operations and results in major losses, effectively making availability as important as confidentiality & integrity.

**2.Task: Document the setup steps briefly setting up a virtual machine using VirtualBox or VMware with a Linux distribution (e.g., Ubuntu or Kali Linux).**

**1. Download VirtualBox or VMware**

* First, head over to the VirtualBox or VMware website and download the installer for your system. Install it by following the simple on-screen instructions.

**2. Get a Linux ISO**

* Choose your favorite Linux distribution, like Ubuntu or Kali Linux, and download the **ISO file** from their official website. This file is essentially the operating system you'll install in your virtual machine.

**3. Create a New Virtual Machine**

* Open VirtualBox or VMware, and start by creating a new virtual machine. You’ll give it a name, choose **Linux** as the operating system, and allocate at least **2 GB of RAM** and around **20 GB of storage**. For VirtualBox users, make sure to select **VDI** as the virtual hard disk format. If you’re using VMware, you’ll load the Linux ISO file during setup.

**4. Install Linux**

* Once your VM is ready, start it up and point it to the ISO file you downloaded earlier. The Linux installer will guide you through setting up things like language, username, and password. Just follow the prompts to complete the installation.

**5. Reboot and Log In**

* After installation finishes, restart the virtual machine, log in with your new username and password, and you’ll be up and running with your Linux environment.

**6. (Optional) Install Guest Additions**

* If you're using VirtualBox and want a smoother experience, you can install **Guest Additions** to enable features like full-screen mode and better performance. Simply insert the Guest Additions from the VirtualBox menu, follow the instructions, and reboot the VM once it's done.

**3. Choose a Tool:Task: Perform a simple task with the tool, such as capturing network traffic or running a basic network scan. Write a short report (1 page) on what you did and learned.**

In this exercise, I began by downloading and installing Wireshark, a network protocol analyzer. After setting it up, I captured real-time network traffic by selecting my computer's network interface. I learned how to analyze these packets, identifying key details such as the source, destination, and protocols like TCP or UDP.

Additionally, I explored filtering options, which allowed me to focus on specific traffic, such as packets related to certain websites. This highlighted the distinction between encrypted and unencrypted traffic, demonstrating the potential risks of unsecured data transmission. Using Wireshark, I now understand how to analyze network behavior and spot security risks, making it a powerful tool for network analysis and troubleshooting.