**1. Explain briefly the CIA triad of computer security. Can we survive with any two of the triad leaving the third one? Explain your reasoning with examples.**

CIA stands for Confidentiality, Integrity, and Availability. For every system to survive, it needs to have these three letters embedded in it to have a longer run of that system. Ideally, when all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents.

**Confidentiality**:

Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

For example, if we take any web application that aids clients in registering and logging in, we can facilitate registration and login. To prevent intruders, we must build these systems more carefully. While creating accounts, it is a mess if every user has admin access and can edit any customer or business-related information. To prevent unwanted access to data within or out of a system, it must be confidential. If not, without any knowledge any customer can change the details of other customers' passwords.

**Integrity:**

Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.

For example, any organization runs on the trust of their customers. To gain trust in the longer term, the details shared with the customers should be genuine. If any job posting company had posted an opening, then lot of applications might be come in for the post. If no interview happened regarding the post, did the applicant show any interest in applying for jobs using the same way? I hope not.

**Availability:**

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to and getting to the data should not take an inordinate amount of time.

For example, I had data in my cloud storage, and I wanted to move to one of my personal databases. To access the data in cloud storage, first I need access to the storage. If not, that data is unavailable to me to push to my personal database even though I have it in my cloud storage system. Once getting access to the cloud storage there might be another constraint which makes data unavailable like in this case platform to push data from cloud storage to personal storage. To achieve this, we need to use some tools or services to do it with the access we got in the first place. So, if any of these gets compromised the data availability is compromised.

So, to recover data if the system gets crashed to make it online in no time. Their needs to be a system to recover faster.

Confidentiality – Integrity -- Availability

Protect – trustworthy – visible

**2. Why is computer security so challenging? Who are the attacker agents that we defend against?**

When is system is leaked, it might be because of software malware, hardware malware, an intruder trying to theft some files or place some files into the system, or if someone is inside the system, helping intruder to gain access to the system. In the above-mentioned scenario there might be any one among or even out of those scenarios.

To deal with computer security, first we need to analyze the cause of the attack. Could be able to identify the type of attack that happened and do the reverse engineering to solve the attack and find a solution to make the system even more secure.

**3. Define vulnerability, threat and control. Give your own example to explain them.**

**Vulnerability:**

Vulnerability can be anything from improper software to a secured server which got attacked by a phishing mail. It can be an issue in customers identification, authentication, modification, or subtle software. Vulnerability can be a clerk who shares the internal information without side of system.

**Threat:**

Threats are the starting point of an attack, usually caused by intruders with the intention of theft in different forms. It might be hardware, software, or data of all kinds. The threat can be a phishing mail or a link which me open without any knowledge by which the intruder is in our system without our knowledge.

**Control:**

Control helps us in making our system strong and withhold to all vulnerable and threats caused by intruders or happened due to poor software. These can be done in stages by eliminating some key issues for computer security. Access control helps in securing details like authentication, or authorization and other sensitive information. CIA helps in covering some of the controls to the key issues to computer security.

**4. What is the difference between hub and switch? From the security perspective, which one is preferable and why?**

**Hub:**

Hub is the connection for a network of systems handling different channels using that point. A network hub is a device that connects multiple units in an intricately connected network channel. So, hubs are preferred to be used in LAN networks. A hub does not use either MAC address or IP address to guide the data to its destination device, so it broadcasts the message in the entire network, and this way, all the devices receive the same message, creating an excess of network traffic.

**Switch:**

A network switch is a device responsible for guiding data using the source address and destination address encapsulated in the header of the incoming message. This prevents the broadcasting of the message to the entire network and, in turn, prevents network congestion.

The switch uses the MAC address for forwarding the data to the data-link layer in the network model and guarantees that the data frame is received without issues. It uses a full-duplex data exchange method and performs unicast or multicast network connections.

**5. Briefly mention the 7 layers of OSI model and functionality of each layer. Imagine you are sending a confidential message to your friend via a chat application. Using the knowledge of layers, explain how this communication will take place through the network.**

The open Systems Interconnection (OSI) Model helps in creating some rules and requirements to pass the data from one source to another without any security leakage. To do so, it helps to bind some piece of memory to the data segments while moving from one layer to another to identify the data segments among many while receiving and acknowledging without missing any data segments and the order of data segments while receiving will be handled by the OSI Layer.

The 7 layers of OSI layer are:

1. Application Layer

This is the topmost layer which helps in interacting with the users. When data is sent from one system to another, we need user interface to send or receive data which is understandable to the user while receiving and to system while sending so that system can move data from one system to another. This is done by Application Layer where the application takes care of user interface so that the communication transfer at the top level is done without any issues.

1. Presentation Layer

The presentation layer helps in providing data to the application layer which is understandable by the user in the topmost layer. It helps in encrypting and decrypting data that will happen in this layer. When the data arrives in the layer from the top level it will be in the user understandable format and to push the same to below layers it will be converted to different format using encrypting and passed to below layers to protect the data privacy. Vice versa happens when pushing the data to above layers which is application layer, where data from below comes in encrypted format and needs to decrypt so that user can understand in the application layer while pushing to above layer.

1. Session Layer

The Session layer helps in handling the opening and closing of Network while transferring the data. This layer is also responsible for handling the IP address of the system. The session layer makes sure the session is open for enough time, so the transaction is finished. It also helps in setting up the checkpoints because in worst case due to any maintenance if any transfer failed in between we do not have to do it from the beginning, we can start from checkpoints created by the session layer. In our example until all the data segments from the message got delivered our session will not get expired.

1. Transport Layer

The Transport Layer helps in end-to-end communication between the devices to interact between the users. Transport Layer deals with different transfer protocols to set rules and requirements to decide the way we transfer the data between the devices for user interaction. TCP and UDP will be come into picture in this layer. We will add memory to the data segments related to the protocol we are going to follow while transferring the data.

1. Network Layer

The Network Layer handles transfer of data when two networks are communicating with each other. If those two devices are communicating in the same network, we do not need to use Network Layer. The Network Layer helps in dividing the segments into packets. The whole message will divide which got from Transport Layer nothing but called as segments to packets.

In our example, the message with Ip address, tcp/upd protocol details and the message will be divided into smaller packets (Hello is a segment, packets are H, e, l, l, o with address added to each message).

1. Datalink Layer

The data link layer is like the network layer, except that the data link layer facilitates data transfer between two devices using the same network. In the data link layer, packets are broken into pieces referred to as frames. Like the network layer, the data link layer handles flow and error control. The transport layer is different in that it only manages the flow of data and errors when two networks are communicating with each other.

Within the data link layer, you have two sublayers, the media access control (MAC) and logical link control (LLC) layers. Most switches perform their duties at Layer 2. In some cases, switches work at Layer 3 because they are facilitating communication between two networks or virtual local-area networks (VLANs). This must happen at Layer 3 because, in these situations, the data needs to be routed, which is a Layer 3 task.

1. Physical Layer

The physical layer involves the physical equipment that transfers data, like switches and cables. In this layer, the data is converted into strings of 1s and 0s. In the physical layer, the devices must agree on a method of distinguishing the 1s from the 0s, which enables the digital data to be properly interpreted by each device.

The physical layer includes a variety of components, such as cables, the radio frequency used to transmit data, Wi-Fi, and the other physical structures for transmitting data, such as pins, necessary voltages, and types of ports.