Briefly explain the following terms associated with network threats or security defense in a distribu-  
ted computing system:

a.Denial of service (DoS)

step 1:

A denial-of-service attack is a type of cyber-attack in which the perpetrator attempts to render a computer or network resource unavailable to its intended users by temporarily or indefinitely interrupting the services of a host connected to a network.

A Denial-of-Service (DoS) attack is one that attempts to bring a machine or network to a halt, rendering it unreachable to its intended users. DoS attacks work by inundating the target with traffic or delivering it information that causes it to crash.

Step 2:

For example, denials of service are common during Black Friday deals, when thousands of users are clamouring for a bargain. They can, however, be harmful. In this example, an attacker is attempting to exhaust the site's resources in order to prevent legitimate visitors from accessing it.

b.Trojan horse

step 1:

A Trojan Horse is a type of malware that masquerades as legitimate software and infects your computer, altering your files and data. Some Trojan Horses have the potential to offer hackers access to your personal data. Continue reading to learn about the most frequent Trojan Horse Viruses.

A Trojan horse is a type of malware that can harm your data or computer network by destroying, stealing, or otherwise harming it. This malicious software, commonly referred to as a Trojan, is frequently disguised as a legal computer programme. Once downloaded and installed on your computer, it allows hackers to monitor your internet activities, access and copy files from your hard drive, edit and delete your data, slow down your machine's performance, and even steal your personal information.

An example of how a Trojan horse could be used to infect a computer is as follows: An official-looking email containing an attachment is sent to the victim. The attachment contains malicious code that starts running as soon as the victim clicks on it.

c.Network worm

step 1:

The worm can, for example, carry ransomware, viruses, or other malware, all of which can harm afflicted computers. In the event of a blackmail assault, these can, for example, remove or encrypt files on the PC.

An Internet worm is a sort of harmful software (malware) that duplicates itself and spreads copies throughout its network. These self-contained virtual viruses circulate via the Internet, infect computers, and proliferate without the intervention of and without the knowledge of computer users.

Morris Worm, Storm Worm, SQL Slammer, and other worms are examples. Morris created a few lines of code to determine the size of the internet, but the codes contained faults that wrecked the host computers and caused millions of dollars in damage.

D .Service spoofing

step 1:

Spoofing is a term used in cybersecurity to describe when fraudsters appear to be someone or something else in order to gain a person's trust. Gaining access to systems, stealing data, stealing money, or spreading malware are the most common motivations.

Spoofing usually consists of two parts: the spoof itself, such as a forged email or website, and the social engineering component, which encourages victims to act. Spoofers may, for example, write an email posing as a trusted senior coworker or manager, requesting that you transfer money online and offering a compelling explanation for the request. Spoofers typically know how to pull the right threads to get a victim to do what they want — in this case, authorising a fraudulent wire transfer – without raising suspicion.

Step 2:

When an email is sent from a bogus sender address and asks the receiver to give sensitive information, this is an example of spoofing. This email may also include a link to a malicious website with malware.

e.Authorization

step 1

The process by which a server evaluates whether a client has permission to use a resource or access a file is known as authorization. Authentication is frequently used in conjunction with authorization so that the server knows who the client is who is requesting access.

Step 2:

The process of granting someone access to a resource is known as authorization. Of course, this description may appear cryptic, but many real-life scenarios can help you understand what authorisation implies and how to apply those notions to computer systems. A good example is house ownership.

f.Authentication

step 1:

The process of ascertaining whether someone or something is who or what they claim to be is known as authentication. Authentication technology checks if a user's credentials match those in a database of authorised users or in a data authentication server to offer access control for systems.

Something the user knows, something the user is, and something the user has are the three categories in which someone can be authenticated. Identification and real authentication are two independent aspects of the authentication process. The user's identity is sent to the security system during the identification step.

Step 2:

Passwords are the most commonly used type of authentication for websites and applications when it comes to protecting your information online. Passwords, on the other hand, are one of the least secure modes of user authentication out there.

g.Data integrity

step 1:

Integrity refers to the consistency, accuracy, and reliability of data throughout its lifecycle. It must not be changed in transit to retain integrity, and measures must be taken to ensure that data cannot be manipulated by an unauthorised person or programme.

Step 2:

Data integrity is a concept and a procedure that assures that an organization's data is accurate, full, consistent, and valid. Organizations that follow the method ensure not only the integrity of the data, but also that the data in their database is accurate and correct.

Data integrity processes, for example, may be referred to as error checking and validation methods.

h.Confidentialit

step 1:

One of the most important aspects in cybersecurity is confidentiality. Simply defined, confidentiality protects confidential information from unwanted disclosure. Confidentiality is a joint duty between technologists and the rest of the organisation.

Step 2:

Data Confidentiality is concerned with preventing information from being disclosed by ensuring that access to the data is restricted to those who are authorised or by portraying the data in such a manner that its semantics are only accessible to those who have access to crucial information (e.g., a key for decrypting the enciphered data).

For example, a computer file's secrecy is preserved if only authorised users have access to it, while unauthorised users are denied access.