Network Programming

Q1. How Firewall helps to secure PC?

A firewall is a system that is designed to prevent unauthorized access from entering a private network by filtering the information that comes in from the internet. A firewall blocks unwanted traffic and permits wanted traffic. So a firewall purpose is to create a safety barrier between a private network and the public internet because always on the internet there is going to be hackers and malaises traffic that tries to penetrates the private network to cause harm and the firewall is the main component on the network to prevent this and a firewall is especially important to a large organization that has a lot of computers and servers on them because we don't want all those devices accessible to everyone not the internet where a hacker can come in and totally disrupt that organization, That's why we need a firewall to protect them.

A firewall used in computer network is very similar to a firewall works in a building structure. In fact that is where the term came from, A firewall in the building structure provides a barrier so that in a event of an actual fire on another side of the building. The firewall is there to keep the fire contained and to keep it from spreading to the other side. So the firewall is then to keep the fire from destroying the entire building. But if the firewall isn't there the fire would spread to the other side and then the whole building is destroyed. Network firewall works in the similar way as the structure firewall. It stops harmful activities before it spread to the other side of the firewall and cause harm to private network. So in today's high-tech world a firewall is essential to every home and especially in business or an organization to keep their network safe.

Now a firewall works by filtering the incoming network data and determines by its rules if it allow entering a network. And these rules are also known as an access control list. These rules are customizable and are determined by the network administrator. The administrator decides not all network can enter a network but also can leave a network. So these rules either allow or deny permission.

Firewall rules can be based on:-

1. IP Address
2. Domain Names
3. Protocols
4. Programs
5. Ports
6. Keywords

Types of Firewall:-

1. Host-based firewall: - It is a software firewall that is installed on a computer. It protects that computer only.

2. Network Based firewall: - It is a combination of hardware and software. It operates at the network layer. And it is placed between the private network and the public network. It protects an entire network and it does this through management rules that are applied to the entire network. So that any harmful activities can be stopped before it reached the computer.

Name: - Ankur Raj

Roll: - 171210012