NETWORK PROGRAMMING ASSIGNMENT

MAHENDRA SONI, CSE, NIT DELHI
171210036@nitdelhi.ac.in

Ques1: How firewall helps to secure your PC?

Ans: A firewall is a system designed to prevent unauthorized access to or from a private network. We can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. Firewalls work like a filter between your computer/network and the Internet. You can program what you want to get out and what you want to get in. Everything else is not allowed.

In protecting private information, a firewall is considered as a first line of defense. Firewalls are generally designed to protect network traffic and connections, and therefore do not attempt to authenticate individual users when determining who can access a particular computer or network.

By putting protective filters in place around your network and devices, firewalls can help to prevent a number of different security risks. These can include:

- **Denial of service.** This type of cyberattack can slow or crash a server. Hackers utilize this method by requesting to connect to the server, which sends an acknowledgment and attempts to establish a connection. While there are ways firewalls can be used to identify and protect against certain forms of denial of service attacks, they tend to be easily fooled and are usually ineffective.
- **Macros.** Macros are scripts that applications can run to streamline a series of complicated procedures into one executable rule. These executable fragments can also be embedded data attempting to enter your network, which firewalls can help identify and discard.
- **Viruses.** Viruses are small programs that replicate themselves from computer to computer, allowing them to spread between devices and across networks. Some firewalls include virus protection, but using a firewall alongside antivirus software is a smarter and more secure choice.

Because there are so many varieties of potential cyberattacks, it can be difficult for firewalls to filter out every threat. While firewalls are extremely beneficial in securing networks, it is essential to also pair firewalls with other security programs and hardware.

Ques2: If you are a system administrator, what steps will you take to secure it?

Ans: A system administrator is a professional who is held accountable for network setup, annual server maintenance such as mail servers and file servers, and much more. In an organization, every task that is performed by the system administrator requires an uninterrupted internet connection, which is maintained by the system administrator. For example, the successful sending and receiving of work emails happen only when mail servers are working fine. The System Administrator will collaborate and offer necessary technical support for firewall and network system.

If I am a system admin, then I will take the following steps to secure it-

- Install and configure software and hardware
- Manage network servers and technology tools
- Set up accounts and workstations
- Review memory usage
- Monitor performance and maintain systems according to requirements
- Troubleshoot issues and outages

Check application log

- Check security log
- Ensure security through access controls, backups and firewalls
- Upgrade systems with new releases and models
- Develop expertise to train staff on new technologies
- Build an internal wiki with technical documentation, manuals and IT policies
- Review CPU usage

There are different types of computer systems administrators based on their roles and responsibilities:

1. Server Administrator – maintains the operating system of the servers (and sometimes the applications as well), such as the mail services, the web services, etc., and is also in charge of troubleshooting any hardware, operating system or application-related problems.
2. Network Administrator – maintains the network infrastructure, such as the routers and switches, and troubleshoots network-related problems.
3. Database Administrator (DBA) – maintains the database system used by the company or organization. In bigger organizations, there is a DBA which is specifically responsible for this role. In smaller organizations, this role would normally be shared by the server administrator.
4. Security Systems Administrator - maintains the daily operation of security systems, and can handle things like systems monitoring and running regular backups; setting up, deleting and maintaining individual user accounts; and developing organizational security procedures.