Network Programming Assignment 1

Kimmi
CSE, NIT Delhi
171210034@nitdelhi.ac.in

Q1. How Firewall helps to secure PC?

Sol. Firewall is not like a wall. It's more like a filter. Firewalls are used to *filter* threatening communications. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic like viruses and hackers.

There are two types of firewalls: network firewalls and host-based firewalls. Network firewalls are used by businesses that contain a network of multiple computers, servers, and users. The network firewall monitors the communications between the company computers and outside sources. Host-based firewalls work similarly but are stored locally on a single computer. This functions as a defense against cyber criminals and various online scams and attacks. Host-based firewalls are also recommended for business computers that are network connected but not protected by a network firewall. They can also be useful for homes with multiple computers sharing the same network.

Firewalls and antivirus work hand-in-hand to protect our computer and other computers on the network. Antivirus detects any malware running on the computer, and a firewall blocks malicious connections. A firewall blocks any incoming requests from the Internet to your internal network. You probably don't want any random person browsing your network, so you block them with a router firewall. Firewalls aren't useful for just incoming requests. Viruses and other types of malware sometimes attempt to connect to the Internet to send private data from your computer to the hacker's private web server. Hackers steal passwords, financial information and other data to sell on the black market. Instead of gaining access to your computer, the hacker writes software that you install and this software uploads data to the hacker's server. If your antivirus does not detect the software as malicious, your next protection is the firewall application. Your computers firewall detects that an application is attempting to access the Internet and sends you an alert. You then have the option to allow the connection or deny it. If you deny it, then you know that malicious software could be an issue on your computer.

Q2. If you are a system administrator, what steps will you take to secure it?

Sol. The system administrator is sometimes called the *sysadmin* or the *systems administrator.* Small organizations may have just one system administrator, whereas larger enterprises usually have a whole team of system administrators.

A system administrator is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. System administrators manage all the servers, network equipment and any other IT infrastructure for an organization. In many companies, those system administrators are part of the organization's IT team or department. They are the one who setup the network within the organization, installing mail servers, file servers and many other servers required by the organization, installing all the required applications to support the organization's business, applying operating system updates, patches and configuration changes, among others. They are responsible to ensure that all the services are running properly.

If I am a System Administrator, then I will take the following steps to secure it:

1. Maintaining system properly
2. Verify that peripherals are working properly
3. Quickly arrange repair for hardware in case of hardware failure
4. Monitor system performance
5. Create file systems
6. Install software
7. Create a backup and recovery policy
8. Monitor network communication
9. Update system as soon as new version of Operating Software and application software comes out
10. Implement the policies for the use of the computer system and network
11. Setup security policies for users. A system admin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems)
12. Documentation in form of internal wiki
13. Password and identity management

The sysadmin must coordinate with multiple teams to resolve issues, communicate with and update customers, maintain 100% uptime, hold discussions with the audit team, prepare weekly/monthly/quarterly reports, do continuous monitoring of servers and services using appropriate tools, and maintain the hardware console and respond to any triggered alarms.

The sysadmin is always a single point of content (SPOC) in the data center or network operations center for issues related to web hosting, application and server outages, and other critical IT operations problems.