NETWORK PROGRAMMING ASSIGNMENT

Submitted By:

- Pranshu Sharma
- 171210043
- CSE 3rd Year

Ans 1:

A firewall is a software program that prevents unauthorized access to or from a private network. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as LAN or the Internet. A firewall can be a software or hardware-based system that prohibits any traffic that we don't want inside our network. All messages entering or leaving the intranet (the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firewalls are often categorized as either **network firewalls** or **host-based firewalls**. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

Hardware and Software Firewalls

Hardware firewalls can be purchased as a stand-alone product but are typically found in broadband routers, and should be considered an important part of your system security and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, a business networking firewall solution is available.

Software firewalls are installed on your computer, like any software program, and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.

Several types of firewalls exist:

- ***Packet filtering:*** The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

- ***Circuit-level gateway implementation:*** This process applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

- ***Acting as a proxy server:*** A proxy server is a type of gateway that hides the true network address of the computers connecting through it. A proxy server connects to the internet, makes the requests for pages, connections to servers, etc., and receives the data on behalf of the computers behind it. The firewall capabilities lie in the fact that a proxy can be configured to allow only certain types of traffic to pass (for example, HTTP files, or web pages). A proxy server has the potential drawback of slowing network performance, since it has to actively analyse and manipulate traffic passing through it.

- ***Application Gateway:*** Application firewalls function by determining whether a process should accept any given connection. Application firewalls filter connections by examining the process ID of data packets against a rule set for the local process involved in the data transmission. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers. Application firewalls that hook into socket calls are also referred to as socket filters. It applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

In practice, many firewalls use two or more of these techniques in concert.

Ans 2:

The person who is responsible for setting up and maintaining the system or server is called as the system administrator. A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. This can be achieved by:

- User account access controls and cryptography can protect systems files and data, respectively.
- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.
- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.
- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks etc. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

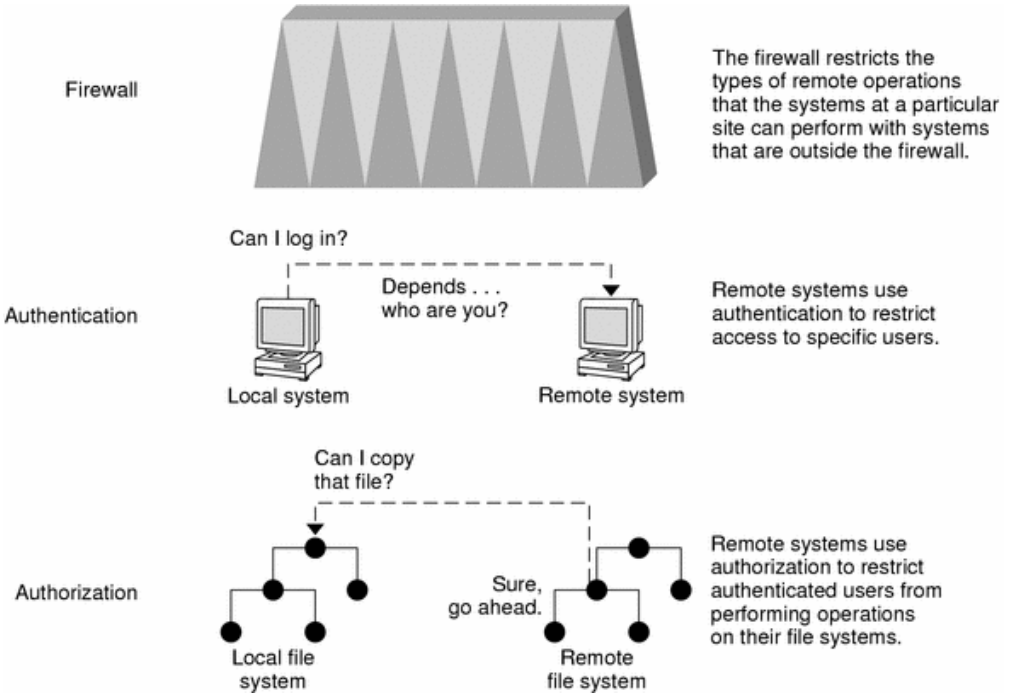
The first line of security defense is to control access to your system. We can control and monitor system access by doing the following:

- Maintaining physical site security
- Maintaining login control
- Restricting access to data in files
- Maintaining network control
- Monitoring system usage
- Setting the path variable correctly
- Securing files
- Installing a firewall
- Reporting security problems

We can set up two security barriers on a system. The first security barrier is the ‘Login’ command. To cross this barrier and gain access to a system, a user must supply a user name and a corresponding password that is known by the local system or by the name service.

The second security barrier is ensuring that the system files and programs can be changed or removed by superuser only. A would-be superuser must supply the ‘Root’ user name and its correct password.

The more the available access across a network, the more advantageous it is for networked systems. However, free access and the sharing of data and resources create security problems. Network security is usually based on limiting or blocking operations from remote systems. The following figure describes the security restrictions that you can impose on remote operations:



We can set up a firewall system to protect the resources in our network from outside access. The firewall acts as a gateway that passes data between the networks, and it acts as a barrier that blocks the free passage of data to and from the network. The firewall requires a user on the internal network to log in to the firewall system to access hosts on remote networks. Similarly, a user on an outside network must log in to the firewall system before being granted access to a host on the internal network.

Authentication is a way to restrict access to specific users when they access a remote system, which can be set up at both the system level or network level. Once a user gains access to a remote system, **authorization** is a way to restrict operations that the user can perform on the remote system.