Computer Science & Engineering Department
National Institute of Technology, Delhi

Assignment-1
Subject – Network Programming
(CSB 351)

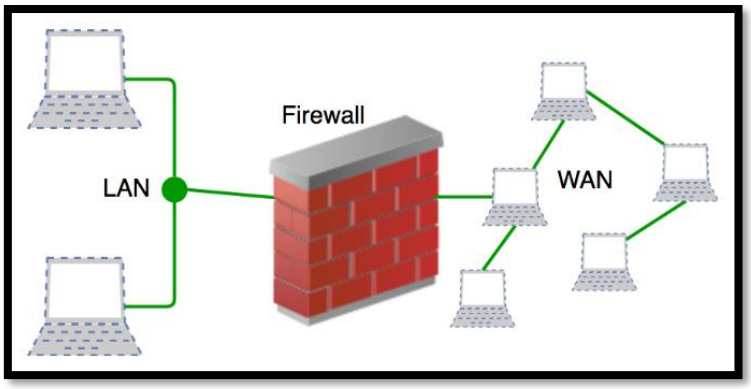
Submitted To:
Dr. Ravi Kumar Arya
Assistant Professor
Department of Electronics & Communication Engineering
NIT Delhi

Submitted By:
Parth Vashist
171220036
CSE B. Tech (3rd Year)

Network Programming Assignment-1

Q1) How firewall helps to secure PC?

Ans) In Computer Networks, firewall plays a vital role in network security and helps to protect networks and our computers (PCs) from a wide range of security risks such as unauthorized access from outside the network. Technically, a firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules.



Firewalls can be software such as the Windows firewall for the operating system or hardware such as filtering set on a router.
In other words, a software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a hardware firewall is a piece of equipment installed between your network and gateway.

Firewall protects our PC data from various threats:

Firewalls can help to prevent a number of different security risks using filters around our network and devices (PCs). These can include: backdoors, denial of service, macros, remote logins, spams and viruses etc.

Working of firewalls:

Firewalls scan the data packets for malicious codes that have already been identified as established threats. If a data packet is flagged and determined to be a security risk, the firewall prevents it from entering the network or reaching our computer using the set of rules. Rule sets can be based on several things indicated by packet data, including their source, destination and content.
These characteristics may be represented differently at different levels of the network. As a packet travels through the network, it is reformatted several times to tell the protocol where to send it. Different types of firewalls exist to read packets at different network levels.

Types of firewalls:

Firewalls use one or a combination of the following methods to control traffic flowing in and out of the network:

Packet filtering: It is the most basic form of firewall software which uses pre-determined security rules to create filters used to secure our PC. When a packet passes through a packet-filtering firewall, its source and destination address, protocol and destination port number are checked. If the packet does not comply with the firewall's rule set, it is dropped i.e. it's not forwarded to its destination. For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for Transmission Control Protocol (TCP) i.e. port number 23, the port where a Telnet server application would be listening.

Proxy service: These firewalls are incredibly secure, but work more slowly than other types of firewalls and are often limited to the sorts of applications they can support. Instead of serving as a filtration system that data passes through, proxy servers function as go-betweens. By creating a mirror of the computer behind the firewall, they prevent direct connections between our PC and the incoming packets, protecting our network location from hackers and other potential threats.

Stateful inspection: These firewalls are also known as dynamic packet-filtering firewalls. They secure our PC by maintaining a table that keeps track of all open connections. When new packets arrive, the firewall compares information in the packet header to the state table and determines whether it is part of an established connection. If it is part of an existing connection, then the packet is allowed to pass through. Whereas, if the packet doesn't match an existing connection, it is evaluated according to the rule set for new connections.

Next Generation Firewalls (NGFW):

They filter network and Internet traffic based upon the applications or traffic types using specific ports. Next Generation Firewalls (NGFWs) blend the features of a standard firewall with quality of service (QoS) functionalities in order to stop modern security breaches like advance malware attacks and application-layer attacks and thus provide smarter and deeper inspection.

For network security, firewall and antivirus work together to protect our computer and other computers on the network. A firewall blocks malicious connections while an antivirus detects any malware running on the computer.
Hence, both are necessary for securing our PCs and personal data.

Q2) If you are a system admin, what precautions will you take to secure it?

Ans) Being a system admin, it becomes important to adopt various security precautions in order to protect individual users, companies and government agencies from various threats, viruses or from a malicious hacker trying to steal data. Some of the precautionary measures are given below:

Authentication:

Authentication is used to verify the identity of the person accessing the information. For example: User ID and password can be used for ensuring security and prevent unauthorised access to the data. Moreover, biometric authentication using fingerprint or retinal scan can be used for additional security.

Password Security:

Require complex passwords: A password should not be simple like a word that can be found in a dictionary. A good password policy is one that requires minimum of eight characters and at least one upper-case letter, one special character and one number. Further, an admin should never have superuser credentials that cannot be removed by simply removing his user account or move the user account to a group that lacks the permission.

Access Control:

It is used to ensure data abstraction i.e. the users can only access the information resources that are appropriate. Here, a list of users is maintained to know which users are authorized to read, modify, add, and/or delete information. Hence, it helps prevent stealing or modification of data by malicious hackers.

Data Encryption:

In data encryption, data is encoded upon its transmission or storage so that only authorized individuals can access it. This encoding is achieved by a computer program, which encodes the plain text that needs to be transmitted; then the recipient receives the cipher text and decodes it (decryption).

Patch and Update:

It must be ensured that the operating system, software and other applications are updated on a regular basis with the latest patches to prevent threats from exploiting security gaps.

Training employees and users in security awareness:

Train employees and users should be done to ensure that they do not give away passwords. It is essential as one of the primary methods that is used to steal passwords is by simply asking the users or administrators. Further, the users must be made aware of malicious practices such as phishing attacks.

Backup and Disaster Recovery Planning:

The data on the corporate servers along with individual computers used throughout the organization should be backed up. Regular backups of all the essential data must be ensured however frequency of backup may vary. Critical data should be backed up daily, while less critical data could be backed up weekly.

Disaster recovery drills: Data restoration mock drills should be conducted every month or quarterly to ensure that the data can be restored in case of an emergency.

Firewalls:

Firewalls should be used to increase security of the network. A firewall can exist as hardware or software (or both). It protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria/rule. A firewall may also be configured to restrict the flow of packets leaving the organization.

Intrusion Detection System (IDS):

An IDS provides the functionality to identify if the network is being attacked. It can also log various types of traffic on the network for analysis later.

Physical Security:

Physical security is the protection of the actual hardware and networking components that store and transmit information resources. Physical Security measures include: physical intrusion detection using security cameras, securing equipment such as hard drives containing critical information, environmental monitoring of the place where servers are located, employee training to prevent thefts etc.

Monitoring tools:

The network traffic must be monitored in order to detect any suspicious activity. It can be done by installing and configuring live monitoring tools like Nagios etc. to monitor the network and issue alerts about potential problems.