Network Programming Assignment 1

Q1. How Firewall helps to secure PC?

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your
private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

- **Packet filtering** - Packets (small chunks of data) are analyzed against a set of **filters**. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- **Proxy service** - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- **Stateful inspection** - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

  Firewalls are customizable. This means that you can add or remove filters based on several conditions. Some of these are:

  IP addresses - Each machine on the Internet is assigned a unique address called an IP address. IP addresses are 32-bit numbers, normally expressed as four "octets" in a "dotted decimal number." A typical IP address looks like this: 216.27.61.137. For example, if a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address.

  Domain names - Because it is hard to remember the string of numbers that make up an IP address, and because IP addresses sometimes need to change,

all servers on the Internet also have human-readable names, called domain names. For example, it is easier for most of us to remember www.howstuffworks.com than it is to remember 216.27.61.137. A company might block all access to certain domain names, or allow access only to specific domain names.

Protocols - The protocol is the pre-defined way that someone who wants to use a service talks with that service. The "someone" could be a person, but more often it is a computer program like a Web browser. Protocols are often text, and simply describe how the client and server will have their conversation. The **http** in the Web's protocol. Some common protocols that you can set firewall filters for include:

- **IP** (Internet Protocol) - the main delivery system for information over the Internet
- **TCP** (Transmission Control Protocol) - used to break apart and rebuild information that travels over the Internet
- **HTTP** (Hyper Text Transfer Protocol) - used for Web pages
- **FTP** (File Transfer Protocol) - used to download and upload files
- **UDP** (User Datagram Protocol) - used for information that requires no response, such as streaming audio and video
- **ICMP** (Internet Control Message Protocol) - used by a router to exchange the information with other routers
- **SMTP** (Simple Mail Transport Protocol) - used to send text-based information (e-mail)
- **SNMP** (Simple Network Management Protocol) - used to collect system information from a remote computer
- **Telnet** - used to perform commands on a remote computer

A company might set up only one or two machines to handle a specific protocol and ban that protocol on all other machines.

Ports - Any server machine makes its services available to the Internet using numbered ports, one for each service that is available on the server. For example, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server

would be available on port 21. A company might block port 21 access on all machines but one inside the company.

Specific words and phrases - This can be anything. The firewall will sniff (search through) each packet of information for an exact match of the text listed in the filter. For example, you could instruct the firewall to block any packet with the word "X-rated" in it. The key here is that it has to be an exact match. The "X-rated" filter would not catch "X rated" (no hyphen). But you can include as many words, phrases and variations of them as you need.

Some operating systems come with a firewall built in. Otherwise, a software firewall can be installed on the computer in your home that has an Internet connection. This computer is considered a **gateway** because it provides the only point of access between your home network and the Internet.

With a hardware firewall, the firewall unit itself is normally the gateway. A good example is the Linksys Cable/DSL router. It has a built-in Ethernet card and hub. Computers in your home network connect to the router, which in turn is connected to either a cable or DSL modem. You configure the router via a Web-based interface that you reach through the browser on your computer. You can then set any filters or additional information.

Hardware firewalls are incredibly secure and not very expensive. Home versions that include a router, firewall and Ethernet hub for broadband connections can be found for well under $100.

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

1. Put In And Monitor Firewall Performance

A firewall is a piece or set of software or hardware designed to block unauthorized access to computers and networks. In very simple terms, a firewall is a series of rules that control incoming and outgoing network traffic; computers and networks that “follow the rules” are allowed into access points, and those that don’t are prevented from accessing your system.

Firewalls are becoming more and more sophisticated (right along with hackers) and the latest are integrated network security platforms that consist of a variety of approaches and encryption methods, all working in tandem to prevent breaches.

2. Update Passwords At Least Every Quarter

Hopefully, by now your employees know to avoid default passwords or phrases like “password,” “12345” and their dates of birth. In addition to using passwords that feature both letters, symbols and numbers — and some uppercase letters — for added security, require employees to regularly change any personal passwords used on systems that have access to business networks (your business will have its own, but many computers also allow personal passwords).

Let employees know that when choosing passwords, substituting letters with similarly shaped characters, like “pa$$w0rd” for “password,” is a bad idea. Hackers are onto that trick!

Every quarter is the recommended frequency, but more often is better. However, there is a fine line: changing passwords too often can cause confusion, leading employees to reach out to IT for reminders of their username and passwords (and we all know how much IT likes getting calls like that!).

Side note: Many businesses now require two-factor authentication to connect to the network. In addition to entering a username and password, users may also need to enter a code they receive via text or by another means to connect to a system or Wi-Fi network.

3. Create A Virtual Private Network (VPN)

VPNs create a far more secure connection between remote computers (home networks or computers used by people on the road) and other “local” computers and servers. These networks are essentially only available to people who should have access to your systems, including your wireless network, and to equipment that’s been authorized in your network settings. A VPN can dramatically decrease the likelihood that hackers can find a wireless access point and wreak havoc on your system.

4. Encrypt your data

Whether your computer houses your life’s work or a load of files with sentimental value like photos and videos, it’s likely worth protecting that information. One way to

ensure it doesn’t fall into the wrong hands is to encrypt your data. Encrypted data will require resources to decrypt it; this alone might be enough to deter a hacker from pursuing action. There are a plethora of tools out there to help you encrypt things like online traffic and accounts, communication, and files stored on your computer. For full disk encryption, some popular tools are VeraCrypt and BitLocker. You can find separate tools to help you encrypt your mobile device, with various apps available for both Android and iOS.

5. Multi-Factor Authentication

Multi-factor authentication is simple: users must provide two separate methods of identification to log into an account (for instance, typing in a password and then typing in a numeric code that was sent to another device). Users should present unique credentials from two out of three categories — something you know, something you have and something you are — for multi-factor authentication to be fully effective.