Network Programming Assignment

CSB 351

Submitted To:
Dr. Ravi Kumar Arya
Assistant Professor
NIT Delhi

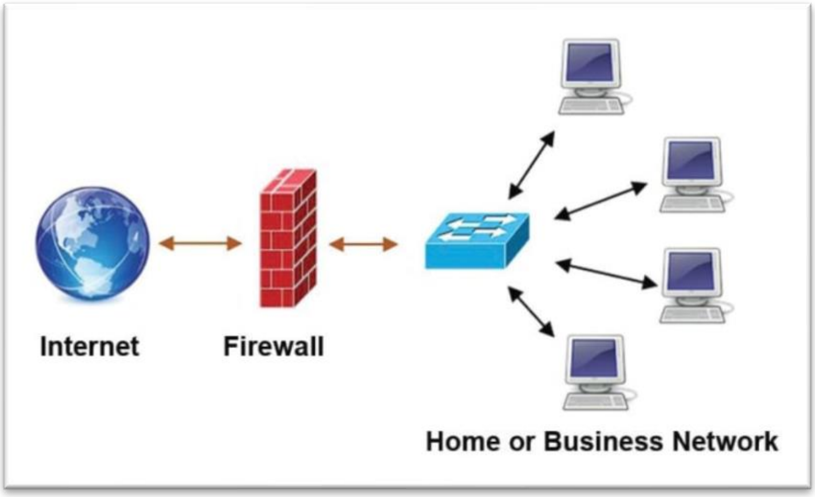
Submitted By:
Shubham Chandak
171220047
CSE 3rd Year

Q1. How does Firewall help to secure a PC ?

Ans:

A firewall is a network security system that monitors and controls over all the incoming and outgoing network traffic based on advanced and a defined set of security rules. It is a software program that prevents unauthorized access to or from a private network and enhances its security. Its purpose is to establish a barrier between our internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers. It is an integral part of a comprehensive security framework for our network.

There are two types of firewalls - hardware and software:
Hardware firewalls are built into network devices such as routers while **Software firewalls** usually come as stand-alone applications or as part of a complete anti virus protection software



Working of Firewall

A firewall absolutely isolates our computer from the Internet using a "wall of code" that inspects each individual "packet" of data based on pre-established rules as it arrives at either side of the firewall — inbound to or outbound from our computer- and filter the packets coming from unsecured or suspicious sources to prevent attacks. Technically, Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices.

The term 'packets' refers to pieces of data that are formatted for internet transfer. Packets contain the data itself, as well as information about the data, such as where it came from. Firewalls can use this packet information to determine whether a given packet abides by the rule set. If it doesn't, the packet will be barred from entering the guarded network.

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

- **Packet filtering** - The most basic form of firewall software uses pre-determined security rules to create filters. Packets (small chunks of data) are analyzed against these filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- **Proxy service** - A firewall proxy server is an application that acts as an intermediary between systems. Information from the internet is retrieved by the firewall and then sent to the requesting system and vice versa. Firewall proxy servers operate at the application layer of the firewall, where both ends of a connection are forced to conduct the session through the proxy.
- **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.

Aside from their main function of network protection, firewalls perform important logging and audit functions. Basically, good firewalls keep a record of events, which can be used by administrators to identify patterns and improve rule sets.

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

Ans: Technology continues to be a boon for entrepreneurs, offering increased mobility, productivity and ROI at shrinking expense. But they also present growing security concerns.

As we all know, the Internet is not a very safe place. There are hackers trying to access our computer, worms trying to infect us, malicious Trojans disguised as helpful programs, and spyware that reports our activities back to their makers.

To keep a system secure from these threats, we as a system admin should take the following precautions :

- **Keep up with system and software security updates**

A common method that computer infections use to infect our computer are security vulnerabilities in our installed programs. In order to make our computer as secure as possible, we need to make sure these programs are updated when new security fixes are released.

- **Install anti-virus software**

Any machine connected to the internet is inherently vulnerable to viruses and other threats, including malware, ransomware, and Trojan attacks. Therefore, it is very important that our computer has antivirus software running on our machine. By having an antivirus program running, files and emails will be scanned as we use them, download them, or open them. If a virus is found in one of the items we are about to use, the antivirus program will stop us from being able to run that program and infect ourself.

- **Use a firewall**

The importance of using a Firewall on our computer or on our network cannot be stressed enough. Just because we have all the latest security updates, we are still susceptible to unreported, unpatched, or unknown vulnerabilities that a hacker may know about. Sometimes hackers discover new security holes in a software or operating system long before the software company does and many people get hacked before a security patch is released. By using a firewall the majority of these security holes will not be accessible as the firewall will block the attempt.

- **Use Encryption**

An effective way to ensure that our personal data doesn’t fall into the wrong hands is to encrypt it. Encrypted data will require resources to decrypt it; this alone might be enough to deter a hacker from pursuing action.

- **Use a VPN**

A Virtual Private Network (VPN) is an excellent way to step up our security, especially when browsing online. While using a VPN, all of our internet traffic is encrypted and tunneled through an intermediary server in a separate location. This masks our IP, replacing it with a different one, so that our ISP can no longer monitor our activity.

- **Use secure passwords**

Many cyber attacks succeed precisely because of weak password protocols. Hence it is very important to use secure passwords for the applications we use. Also we must never use same password for all out accounts.

- **Adjust browser settings**

Most browsers have options that enable us to adjust the level of privacy and security while we browse. These can help lower the risk of malware infections reaching our computer and malicious hackers attacking our device.