Computer Science And Engineering Department

National Institute of Technology, Delhi

Network Programming

CSB 351

Assignment 1

Submitted to-

Dr. Ravi Arya

Submitted by-

Ankit Sinha

Roll no-171210011

B Tech 3rd year

Q1. How firewall helps to protect a personal computer?

Answer –

Firewall works like a filter between computer or network and the Internet. We can program what we want to get out and what we want to get in.

It is also a combination of systems that supervises the flow of traffic between distinctive parts of the network. It is used to guard the network against nasty people and prohibit their actions at predefined boundary levels.

A good firewall should be sufficient enough to deal with both internal and external threats and be able to deal with malicious software such as worms from acquiring access to the network. It also provisions your system to stop forwarding unlawful data to another system.

The main goal of the firewall is to protect the personal computer from the malicious mischief.

Malware, malicious software, is the primary threat to the home computer and this contains the viruses. A virus can be transmitted to your computer through email or over the Internet and can quickly cause a lot of damage to your files. Other malware includes Trojan horse programs and spyware.

There are two types of firewalls: network firewalls and host-based firewalls.

> Network firewalls are typically used by businesses that contain a comprehensive network of multiple computers, servers, and users. The network firewall monitors the communications occurring between the company computers and outside sources. If a company wishes to restrict certain websites, IP addresses, or services like Instant Messenger, it can do so using a network firewall. This type of firewall is not practised for a general personal computer.
>
> Host-based firewalls work similarly but are stored locally on a single computer. Every home or personal computer should have some kind of host-based firewall installed on it. This functions as the first line of defence against cyber criminals and various online scams and attacks.

Q2. If you are a system administrator, then what precautions should you will take to secure the personal computer.

Answer:

If I would be a system administrator, I would take the following precautionary measures to secure it:

1. It can be prevented by installing regular system updates as it symphysis more on database security and cyber security. Installing regular updates provide us the pathway to secure the pc from the latest cyber bugs and the dangerous Trojans available online to mapped our data to their systems.

2. Using the concepts of database security:

Since the threads of databases include Integrity, Confidentiality and Availability, following countermeasures can be used:

1> ACCESS CONTROL: The security mechanism must include provisions for restricting access to the personal computer. It can be controlled by creating the accounts and the corresponding passwords to control login. This very concept also known as USER ACCESS SECURITY.

2> FLOW CONTROL: It prevents information from flowing in such a way that it should not reaches unauthorized users.

3> DATA ENCRYPTION: It is used for protecting the sensitive data, but it is practiced when the computer contains highly sensitive data.

3. Renewing and updating the antivirus software so that the pc can handle the latest ransomware available on the internet.

4. Programs can be installed that scans the computer for known adware and other system invaders. If any possible thread is detected then it is compared to a database of known threads to determine if it is really malicious.

5. Regularly scan the RAM, Registry, hard drives and external storage drives and maintaining a higher degree of privacy while we surf any website.

6. Using the best security management to keep out hackers, viruses and other threads.

7.Craft better passwords and automate them. This can be done by including numeric, special characters and capital letters, all at once.

8. It would be wiser to know if the following site may be trusted to give the email and other credentials.