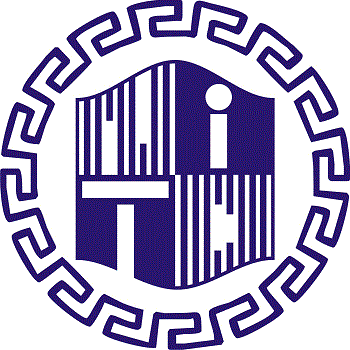
ASSIGNMENT 01

**Computer Science & Engineering Department**

**National Institute of Technology, Delhi**



**NETWORK PROGRAMMING**

**Submitted By: Submitted To: MD SARFARAJ ALAM**

**Dr Ravi Arya Roll NO:171210037**

**(Assistant Professor) Branch CSE**

**NIT DELHI Date: 09/03/2020**

Q.no 1) How firewell helps to secure pc?

A firewall is a device that is installed between the internal network and the external network (internet) to filter all incoming and outgoing traffic or data. This is also known as ‘packet filtering’.

A system administrator programs certain rules in a firewall which are used to evaluate incoming and outgoing data.

A firewall is a vital component of a firm’s network and it plays an extremely important part in securing and protecting it; network security refers to methods of addressing external and internal threats to a company’s network system. Firewalls can help secure a network from both internal and external dangers.

A firewall performs two major roles:

1) Provides defense against external threats by refusing unauthorized . connections to the router from potential attackers such as hackers

2) It also protects the network infrastructure from within. In other words, it blocks outgoing connections from the router. It mitigates the spread of viruses, keyloggers, or malware that have sneaked past the router and on the network. Such malicious software might transmit confidential data back to the hacker such as passwords. Only a firewall is able to prevent them from doing so by inhibiting their connection.

It is important that a firewall is installed and managed by a professional system administrator to provide the maximum amount of protection to your company’s network infrastructure. When done correctly, the advantages of using firewalls cannot be ignored.

Their main benefits are:

**Policing:**  A firewall acts as a security guard that monitors or polices the outgoing and incoming traffic from/to your network. It analyzes the information being sent or received and either allows it or blocks it, depending upon the rules established within the firewall.

**Blocks Malicious Programs:** Firewalls have the ability to block potential malware, viruses, and Trojan horses from infecting your network system. Trojan horses are the most dangerous because they attach themselves to files and when you transmit these files, they do further damage to other computer systems. Plus, they reveal your confidential information to web servers being hosted by potential hackers.

**No More Hackers:** A firewall can stop a hacker dead in their tracks. Hackers can cause loss of data and damage to an organization’s computer systems, while they might even use these systems to carry out illegal activities.

Q no 02)What precaution will take system admin to secure their system?

There are numerous ways to protect and remove malware from our computers. No one method is enough to ensure your computer is secure.

Some of these are following:

**Install Firewall:** A **firewall** enacts the role of a security guard. There are of two types of firewalls: a software firewall and hardware firewall. Each serves similar, but different purposes.

A firewall is the first step to provide security to the computer. It creates a barrier between the computer and any unauthorized program trying to come in through the Internet. If you are using a system at home, turn on the firewall permanently. It makes you aware if there are any unauthorized efforts to use your system.

Install Antivirus Software: [**Antivirus**](https://www.comodo.com/home/internet-security/antivirus.php?af=7639) is one other means to protect the computer. It is software that helps to protect the computer from any unauthorized code or software that creates a threat to the system. Unauthorized software includes viruses, keyloggers, trojans etc. This might slow down the processing speed of your computer, delete important files and access personal information. Even if your system is virus free, you must install an antivirus software to prevent the system from further attack of virus.

[Antivirus software](https://antivirus.comodo.com/?af=7639) plays a major role in real time protection, its added advantage of detecting threats helps computer and the information in it to be safe. Some advanced antivirus programs provide automatic updates, this further helps to protect the PC from newly created viruses.

## Install Anti-Spyware Software: Spyware is a software program that collects personal information or information about an organization without their approval. This information is redirected to a third party website. Spyware are designed in such a way that they are not easy to be removed. Anti-Spyware software is solely dedicated to combat spyware. Similar to antivirus software, anti-spyware software offers real time protection. It scans all the incoming information and helps in blocking the threat once detected.Comodo Antivirus comes with spyware protection built in.

## Use Complex and Secure Passwords: The first line of defence in maintaining system security is to have strong and complex passwords. Complex passwords are difficult for the hackers to find. Use a password that is at least 8 characters in length and include a combination of numbers, letters that are both upper and lower case and a special character. Hackers use certain tools to break easy passwords in few minutes.