



**STUDY MATERIAL – 12**  
**TOPIC – NETWORKING**

**SUBJECT: COMPUTER APPLICATION**

**CLASS: XII**  
**DATE: 03.08.2020**

---

## **Network Security**

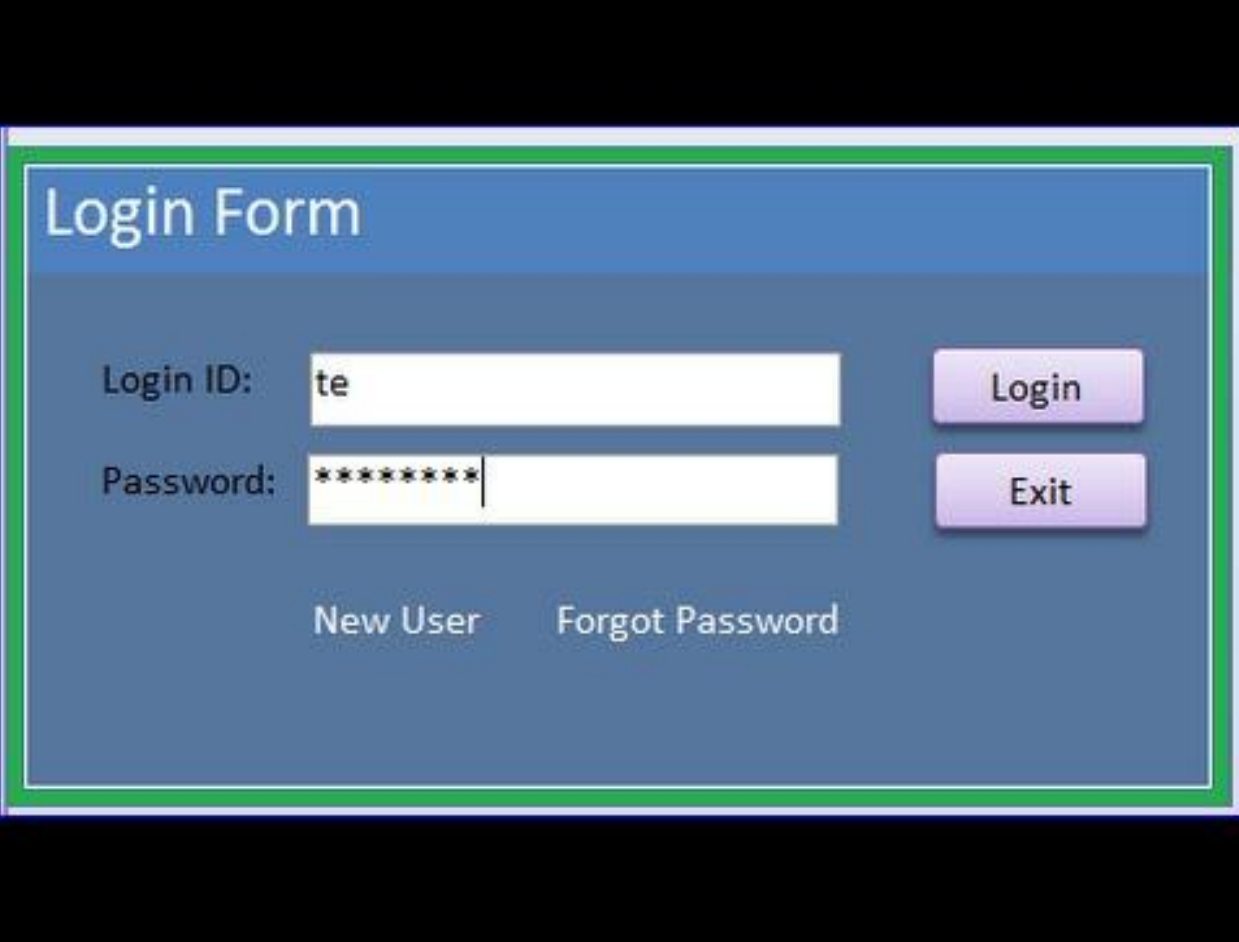
*Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.*

Various methods of security control are:

- ✓ Individual Security
- ✓ Use of Firewall

## ➤ Individual Security:

Attacks on individual computers can be minimized by using login IDs & passwords. These passwords should ideally be a combination of alphabets, digits and special characters of proper length. A complicated password makes it difficult to break it.



Login Form

Login ID: te

Password: \*\*\*\*\*

Login

Exit

New User      Forgot Password

## ➤ **Use of Firewall**

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

### **❑ Advantages:**

#### **1. Monitor Traffic**

A major responsibility of a firewall is to monitor the traffic passing through it. Whatever the information travelling through a network is in the form of packets. Firewall inspects each of these packets for any hazardous threats. If any chance the firewall happens to find them it will immediately block them.

#### **2. Protection against Trojans**

Malwares especially the type Trojans are dangerous to a user. A Trojan silently sits on your computer spying over all the works you do with it. Whatever the information they gather will be sent to a web server. Obviously you will not know their presence until the strange behaviours of your computer. A firewall in this instance will immediately block Trojans before they cause any damages to your system.

### **3. Prevent Hackers**

Hackers on the internet constantly look for computers in order for carrying out their illegal activities. When the hackers happen to find such computers they will start to do even malicious activities such as spreading viruses. Apart from those hackers there can be unknown people such as the neighbours looking out for an open internet connection. Hence to prevent such intrusions it is a good idea to be with a firewall security.

### **4. Access Control**

Firewalls comes with an access policy that can be implemented for certain hosts and services. Some hosts can be exploited with the attackers. So the best in case is to block such hosts from accessing the system. If a user feels that they need protection from these types of unwanted access, this access policy can be enforced.

### **5. Better Privacy**

Privacy is one of the major concerns of a user. Hackers constantly look out for privacy informations for getting clues about the user. But by using a firewall many of the services offered by a site such as the domain name service and the finger can be blocked. Hence the hackers are with no chance of getting privacy details. Additionally firewalls can block the DNS informations of the site

system. Due to this the names and the IP address will not be visible to the attackers.

## **❑ Disadvantages:**

### **1. Cost**

Firewalls does have an investment depending on the types of it. In general hardware firewalls are more expensive than the software firewalls. Besides that hardware firewalls require installations and maintenance which can be costly. These types of configurations cannot be done without an expert IT employee. Comparing this to a software firewall, there is no much investment and it is easy enough for an average user to deploy them.

### **2. User Restriction**

It is no doubt that firewalls prevent unauthorized access to your system from the network. While this can be advantageous for an average user, this can actually be a problem for large organizations. The policies used by the firewall my be strict enough to prevent employees from doing certain operations. As a result of this, the overall productivity of the company may be affected severely. Sometimes this can also prompt employees from using backdoor exploits. However this can lead to security problems since the data travelled through these backdoor exploits are not examined properly.

### **3. Performance**

Firewalls especially the software based has the capability

to limit your computer's overall performance. The processing power and the RAM resources are some of the factors which decides the computer's overall performance. When the software firewalls constantly run on the background they consume more the processing power and the RAM resources. This can lead to a diminished system performance. However hardware firewalls does not impact the system performance since they do not rely upon the computer resources.

#### **4. Malware Attacks**

Even though firewalls has the capability to block the basic types of Trojans, it is proved to be defenceless against other types of malwares. These types of malwares can enter your system in the form of trusted data. Therefore even if you have firewall, it is still recommended to have an anti-malware software installed on your PC. Because the only way to remove them is through an anti-malware scan.

#### **5. Complex Operations**

Even though for small businesses the firewall maintenance is made easy, it is definitely not for large organizations. Firewalls for large organizations require separate set of staffs for operating them. These people make sure that the firewall is safe enough to protect the network from intruders.

## Computer Virus

- ❑ A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.
- ❑ Viruses can erase data, change program & system files or cause severe damage to operating system files to make the computer useless.
- ❑ Viruses come in variety of forms and cause variety of damage:
  - **Boot Sector Virus** – This type of virus infects the master boot record and it is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media.
  - **Direct Action Virus** – This is also called non-resident virus, it gets installed or stays hidden in the computer memory. It stays attached to the specific type of files that it infect. It does not affect the user experience and system's performance.
  - **Resident Virus** – Unlike direct action viruses, resident viruses get installed on the computer. It is difficult to identify the virus and it is even difficult to remove a resident virus.

- **Polymorphic Virus** – These type of viruses are difficult to identify with a traditional anti-virus program. This is because the polymorphic viruses alters its signature pattern whenever it replicates.
- **Overwrite Virus** – This type of virus deletes all the files that it infects. The only possible mechanism to remove is to delete the infected files and the end-user has to lose all the contents in it. Identifying the overwrite virus is difficult as it spreads through emails.
- **Multipartite Virus** – This type of virus spreads through multiple ways. It infects both the boot sector and executable files at the same time.
- **Macro Virus** – They are usually associated with office documents and launch themselves when the document file to which they are attached is opened.
- **Trojan Virus** – A Trojan is usually a program that disguises itself as a normal helpful program but in fact is a virus. It is not always an easy job to remove the damage done by a Trojan.
- **Worms** – These are virus programs designed to infect networks such as the Internet. They travel from one networked computer to another and in the process replicate themselves along the way.



## Antivirus Program

- ❑ An antivirus program usually has two main components:
  - ✓ **The Virus Engine** – It is the program responsible for detecting and cleaning a system from viruses. It automatically checks a file for virus infection and scans all files in a computer for viruses.
  - ✓ **The Virus Information Database** - This is a database that contains an updated list of known viruses.
- ❑ When an antivirus program detects a virus there are three things that can be done:
  - **Clean the file:** This is used to clean a file that has already been infected by a virus. The software will try to get the file back to its original form.
  - **Delete the file:** The file is permanently deleted, when unable to repair it.
  - **Isolate the file:** Some antivirus programs create a separate folder, where the infected files are isolated and stored. The process is called Quarantine. Later such a file can be deleted.

\*\*\*

PRITHWISH DE