NETWORK PROGRAMMING
ASSIGNMENT 1

by – 171210005 (Akhil)

Questions:

1. How firewall helps to secure PC?
2. If you are system admin, what precautions/steps you will take to secure it?

Solutions:

1. Let us first understand what a firewall is. A firewall is a safety feature that provides security to a network. It is a barricade that keeps an eye on every incoming as well as outgoing network traffic and blocks the malicious traffic. It is a software program or a hardware device that sits in a system and checks the data coming through any network into the private network to which the system is connected. Data on the internet is transferred in form of data-packets. Every incoming packet is scanned (or you can say checked for threat), and if it raises any flags then it is blocked and taken out from traffic, hence making it stop from transferring/travelling ahead. Even if there is no malicious content on the packets, firewall acts like the interface between two networks, thus blocking outer entities the direct access to systems of same network. Firewalls are there after every sub-network. It also checks the packets being sent from inside network to outside, to detect any leak in the organization. So, you can say that firewall gives very strong control to organizations over how people use its network.
Now that we know what a firewall is, let us understand how they work and the types of network they block which can lead to even system-failure.
Firewalls have mulltiple ways of controlling the flow of traffic through the network. Some are as follows-
  -> Packet filtering – packets are analyzed against pre-programmed filters. If any flags are raised then those packets are discarded, otherwise they are sent ahead in the network flow.
  -> Proxy service – Information from internet is retrieved by firewall and then sent to requesting system, and vice versa. What this means is, that the firewall acts like an intermediate agent between communication of a system with the internet. The firewall checks the data coming from either side and if it is okay, it is sent to the other side.
  -> Stateful inspection – It is one of the new methods which is faster, because it doesn't inspect each packet one by one. It compares content of packets partially with the trusted data from database. This trusted information in database is created by monitoring the outgoing traffic. If the comparison is matching above a threshold accuracy, then the information is allowed to let through. Otherwise the packets are discarded.

These are how firewalls work, but they can be customized according to the needs. This means that there are systems in a network having special access – unrestricted access and much more. It can be done by using IP addresses, domain names, ports, etc.

Some operating systems come with a built-in firewall. Otherwise this is done by antivirus software.

As we know a firewall tries to block threats or malicious content which broadly are – remote login, SMTP session hijacking, application backdoors, operating systems bug exploits, denial of service, e-mail bombs, macros, viruses, spams, source routing.
These all cannot be taken care by a firewall, because they are complex to figure out and handle, this is why anti-virus softwares are built and installed on systems to keep it safe.

2. The tasks of a system adminisrator are mainly installing, supporting and maintaining servers, planning for and responding to service outages and other problems. In other words, to keep the systems running in full fledged states and handling all issues that cause distruption of services. And sometimes these tasks also involve projects or system related work. If we are system admininstrator, we will ensure the security of the system/network by performing following duties:

-> User administration (handling the users and their accounts)

-> Maintaining system

-> Verify that the peripherals are working properly

-> Having backup hardware in case of failure of any hardware to keep the services running

-> Monitoring the system performance parameters to detect any unusual activity

-> Creating file systems – for example Unified Planetary File System (UPFS) can be used if we have small storage capacity and multiple users.

-> Monitoring the network communication

-> Keeping the systems up to date with the new technologies and versions so that there are no holes in the security and also to keep the performance smooth.

-> Knowledge of computer security should be very strong, as it is needed to handle the authorization and access of users as well as help in keeping them as well as the systems secure.

-> Password management – there should be extremely secure way to store and manage passwords, because they in turn determine the user access, which in turn determine the access over systems and firewall/network privileges

-> Disabling unnecessary services

-> Restricting root access to all users by keeping only one administrator account, which is us

-> Disabling auto-mount feature of devices as they can have scripts ready for execution if they are mounted.

-> Encrypting the file system

-> Backup all the data – in case of any systems failure it is needed to have all the systems

-> Keeping a clone server running to handle the request if main server crashes or is overloaded

-> Reading on system and network security everyday to stay ahead of future possiblities