NATIONAL INSTITUTE OF TECHNOLOGY DELHI
राष्ट्रीय प्रौद्योगिकी संस्थान दिल्ली

Network Programming

[CSB 351]

Assignment 1

Submitted to:

Dr. Ravi Arya

Assistant Professor

ECE Department

Submitted By:

Srijan Gupta

B.Tech

(CSE, 3rd year)

1. How does a firewall protect the PC?

In the world of today, where a blindfolded person crossing a highway is still at less risk than the brat not being careful about his data put over a network. Really! A lot is at stake while we share our data through network. From bank passwords to personal messages, from secret wish lists to self analysis reports; without a firewall, it is all unsafe.

Well now, what is this Firewall? Dwelling upon the resources available, it is known that firewall is not actually a wall but rather it is more like a filter. By this it is meant that they are not built up to keep everything out but are designed to filter threatening communications. Firewalls function using a system of either inclusive or exclusive parameters, allowing specific types of communication in or excluding others.

In a nutshell, a firewall can be defined as a system designed to prevent unauthorised access from or to a private computer network. Today, when we cannot afford a chance with data security, firewall is needed to protect the confidential information from those not authorised to access it and to protect against malicious users and accidents that originate outside the network.

The specific functions provided by the firewall are: -

- Gateway defence
- Carrying out defined security policies
- Segregating network activity between the trusted network, the Internet and the protected zone that lies somewhere midway between them
- Hiding and protecting the internal network addresses called NAT.
- Reporting on threats and activity.

There are several different methods that are used by firewalls to filter out information and some are used in combination. These methods work at different layers of a network which determines how specific the filtering options can be. Like large corporations have very complex firewalls to protect their extensive networks while for home use, firewalls work much more simply.

2. *If you are system admin, what precautions/steps you will take to secure it?*

Pondering over the network analysis, attention is sought by the network infrastructure devices, which are essential components of a network that transport communications needed for data, applications, services and multimedia. Routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems and storage area networks, etc. fall under this category.

And to be necessarily mentioned that these devices are ideal targets for malicious cyber actors because most or all organizational and customer traffic must pass through them. Organizations and individuals that use legacy, unencrypted protocols to manage hosts and services make successful credential harvesting easy for malicious cyber actors. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network.

To secure the network infrastructure in a better way, as the network administrator, the key points that our focus should remain to are: -

- Segmentation and segregation of network and functions: Separate sensitive information and security requirements into network segments.

- Limiting unnecessary lateral communications: Restrict communications using host-based firewall rules to deny the flow of packets from other hosts in the network. The firewall rules can be created to filter on a host device, user, program, or internet protocol (IP) address to limit access from services and systems.

- Hardening of network devices: Disable unencrypted remote admin protocols used to manage network infrastructure (e.g., Telnet, File Transfer Protocol [FTP]) and unnecessary services (e.g., discovery protocols, source routing, Hypertext Transfer Protocol [HTTP], Simple Network Management Protocol [SNMP], Bootstrap Protocol).

- Securing access to infrastructure devices: Implementing Multi—factor authentication and managing privileged access.

- Performing out-of-band (OoB) network management: Segregating standard network traffic from management traffic and ensuring that management traffic on devices comes only from OoB.

- Validating integrity of hardware and software: Maintain strict control of the supply chain and purchase only from authorized resellers.