Computer Science & Engineering Department

National Institute of Technology, Delhi

ASSIGNMENT - CSB 27
(NETWORK PROGRAMMING)

Submitted To:

Dr. Ravi Arya
Assistant Professor
NIT Delhi

Submitted By:

Binshumesh Sachan
171210021
CSE B. Tech (3rd- year)

Q1: What is firewall and How it is used to secure the system?

- It is a software or hardware device.

- It helps to filter the information coming from the internet and provides some kind of restriction on it's usage.

- If the information the user is trying to access get flagged by any of the filtering channels which have been created than the resultant information won't be displayed to the user.

- The system of interconnected computers in any organization who are connected to internet or personal computers are secured using firewall.

- It gives the head of organization the ability to completely control the system of computers which their workers are using and can define which type of information each one of them can access.

- **For ex-:** There are 10 peoples working in your company and each one has given a computer which is connected to internet through central computer or server in which firewall is installed. Than each incoming or outgoing packet will be passed through the firewall.So, now you can set the bandwidth of each computer. Allow only one computer to use File Transfer Protocol (FTP).

- These are some of the common methods used in firewall to control the flow of traffic:

  1. **Packet Filtering-:** As we know the network communication takes place using packets which are nothing just small chunks of data which contains valuable information. So, these packets are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.

  2. **Proxy Service-:** First, the complete requested information will be downloaded using some different address which is not the actual address of your system and than it will be analyzed against the set of rules. If it satisfies all the rules than it will be passed to the actual system otherwise it will be discarded.

  3. **Stateful inspection-:** It is also called dynamic packet filtering. It filters the packet based on Network layer and Transport layer.
  - It keeps track of the state of active connections and maintain one table of it for given active session.
  - **For ex**-: if you want to receive some information from the domain "example.com" than first all policies and rules will be checked from firewall, if it allows than one entry in the table for that website will be saved with various information such as ipaddress, type of protocol used(TCP/UDP), port accessed etc.
  - Now next time the table will be checked for allowing the request. So basically Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics.

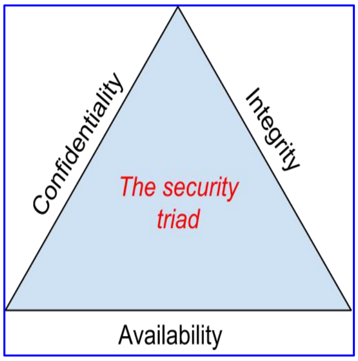
- Some common attacks and how firewall prevent these attacks:

  1. IP address Spoofing:
  In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.
  Prevention:
  Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.

  2. Source Routing Attacks:
  In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.
  Prevention:
  Firewall can defeat this attack if it discards all the packets that use the option of source routing aka path addressing.

  3. Tiny Fragment Attacks:
  Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be fragmented, so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.
  Prevention:
  Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. Dynamic Packet Filters allow incoming TCP packets only if they are responses to the outgoing TCP packets.

Q2: If you are a system admin what precautions/steps you will take to secure it?



- As shown in the figure above, the information security triad that every company wants. It's different components are explained below:

  Confidentiality:
  When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality.
  For example, federal law requires that universities restrict access to private student information. The university must be sure that only those who are authorized have

access to view the grade records.

Integrity:
Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. An example of this would be when a hacker is hired to go into the university's system and change a grade.

Availability:
Availability means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe. Depending on the type of information, appropriate timeframe can mean different things.
For example, a stock trader needs information to be available immediately, while a sales person may be happy to get sales numbers for the day in a report the next morning.

- Tools for Securing the system:

1. **Firewall:** As explained above, firewall is a very useful tool to put restrictions on how user will be accessing the internet and helps to minimize the risk of any attacks getting successful.

2. **Authentication:** Authentication can be accomplished by identifying someone through one or more of three factors: something they know, something they have, or something they are.
- For first part, user-id and password is the most common way to secure system.
- For second one, some id card or key chain.
- And lastly the biometric.This factor identifies a user through the use of a physical characteristic, such as an eye-scan or fingerprint.

3. **Access Control:** It determines which users are authorized to read, modify, add, and/or delete information. The two methods in this regard are access control list (ACL) and role-based access control(RBAC).
In ACL, specific capabilities are assigned, such as read, write, delete, or add. Only users with those capabilities are allowed to perform those functions.
In RBAC, users are assigned to roles and then those roles are assigned the access to information.

4. **Encryption:** Many times, an organization needs to transmit information over the Internet or transfer it on external media . In these cases, even with proper authentication and access control, it is possible for an unauthorized person to get access to the data.
Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it. This encoding is accomplished by a computer program, which encodes the plain text that needs to be transmitted; then the recipient receives the cipher text and decodes it (decryption).

5. **Backups:** It means storing the copy of data somewhere else, so that in case of system failure the lost data can be recovered. Not only should the data on the

corporate servers be backed up, but individual computers used throughout the organization should also be backed up.

6. **Intrusion Detection system:** An IDS does not add any additional security; instead, it provides the functionality to identify if the network is being attacked. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs.

7. **Making Security Policies:** These policies are the starting point in developing an overall security plan. A good information-security policy lays out the guidelines for employee use of the information resources of the company and provides the company recourse in the case that an employee violates a policy.

****