Computer Science & Engineering Department

National Institute of Technology, Delhi

ASSIGNMENT - CSB 27 (NETWORK PROGRAMMING)

Submitted To:	Submitted By:
Dr. Ravi Arya	Yogesh Kumar
Assistant Professor	171230055
NIT Delhi	CSE B. Tech (3rd- year)

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

What is a Firewall?

A firewall is a tool that monitors communication to and from your computer and sits between your computer and the rest of the network, and according to some criteria, it decides which communication to allow, and which communication to block.

What is It Good For?

Identifying and blocking remote access Trojans. The most common way to break into a home computer and gain control, is by using a remote access Trojan (RAT). A Trojan horse, is a program that claims to do something really innocent, but in fact does something much less innocent. You may sometimes get some program, and believe this program to be something good, while in fact running it will do something less nice to your computer. Such programs are called Trojan horses. Personal firewalls can identify and block remote communication efforts to the more common RATs and by thus blocking the attacker, and identifying the RAT.

⤢ 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.

- 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.

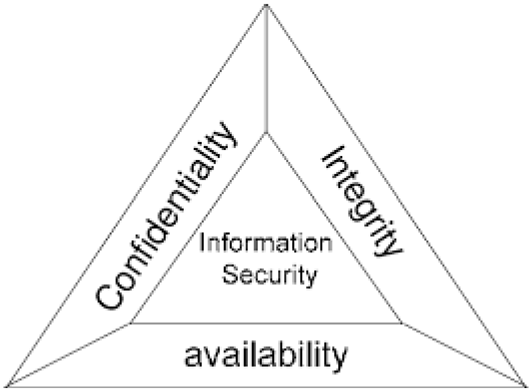
3. **Tiny Fragment Attacks:**

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 everyone wants. The different components of the triad are explained below.

Confidentiality:

When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone should be disallowed from learning anything about its contents.This is the essence of confidentiality

Integrity:

Integrity is the assurance that 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 the 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.

How we can secure our system?

1. Privilege and access control

One way to increase the security of the systems is to control what privileges individuals have and what data they are given permission to access. If users only have access to the information they need and can only do with it what you give them permissions for, there is less likelihood that either the network or your data will be compromised.

2. Limit unnecessary network shares

Malware can easily spread across a network, especially if there are a lot of unprotected network shares. To reduce the risk, remove those shares which are redundant or unnecessary and put security in place for essential ones, such as printers.

3. Run critical systems on an isolated network

Some elements of operations are going to be more vulnerable than others. If you endure those risks as part of your acceptable risk policy, then it makes sense that we should keep those risks separate from your critical systems.

4. Block unused IP ports

Every port is a door through which an attacker can gain entry to your system. If an unused port remains open, it enables malware like Trojans and worms to communicate with remote intruders who can hijack our network. Regularly check what ports we are using and using firewall to seal off those which are no longer needed

5. Control downloading from external networks

Controlling downloads from external networks will protect PCs from viruses.

6.Use a firewall

The importance of using a Firewall on your computer or on your network cannot be stressed enough. Just because you have all the latest security updates, you are still susceptible to unreported, unpatched, or unknown vulnerabilities that a hacker may know about. Sometimes hackers discover new security holes in a software or operating system long before the software company does and many people get hacked before a security patch is released. By using a firewall the majority of these security holes will not be accessible as the firewall will block the attempt.

****