Network Programming

Assignment - 1

Submitted By:
Gaurav Mehra
171210025

Submitted To:
Dr. Ravi Kumar Arya
Assistant Professor
Department of CSE, NIT
Delhi

1. How does Firewall keep the secure a computer

When talking in the context of Computers, Networking, Internet or Security a firewall refers to a program or device or a combination of both that is responsible to ensure that our personal system or network is involved in inflow and outflow of reliable and safe internet traffic. Firewall literally acts like a wall and keeps malicious and unreliable traffic away from your personal network. The firewall filters the network traffic based on some predefined rules that the user or the admin establishes. The firewall prevents attackers from accessing your servers. As a user, based on the type of firewall that you use, you can set up rules that define what IP address to block and what to allow. Also, you can block certain sets of traffic that use some specific TCP/IP ports they use. A firewall may use one for more of the four mechanisms to restrict traffic. The four mechanisms are **Packet Filtering**, **Circuit Level Gateway**, **Proxy Server** and **Application Gateway.**

A **Circuit Level Gateway** acts as a bridge between the host and the outside networks. Any traffic that wants to arrive at the network directly goes to the Circuit Level Gateway instead of directly to the client machine. Then the client machine internally establishes their connection with the Circuit Level Gateway instead of a direct connection to the outside networks. This keeps the host safe from any malicious attacks.

A **Packet Filter** intercepts all the incoming and outgoing traffic in your network all filters it based on the rules of the firewall. It considers the rules as the criteria for the selection of preferred IP addresses and traffic from all the traffic that the network is served with.

A **Proxy Server** can act as a sort of firewall as well. Proxy servers hide your internal addresses so that all communications appear to originate from the proxy server itself. A proxy server caches pages that have been requested. You can configure a proxy server to block access to certain websites and filter certain port traffic to protect your internal network.

An **Application Gateway** is essentially another sort of proxy server. The internal client first establishes a connection with the application gateway. The application gateway determines if the connection should be allowed or not and then establishes a connection with the destination computer.

2. As a system admin what precautions I need to take to keep my system secure

A network admin can perform various precautionary steps to secure its network/system from any malicious attacks from any possible infiltrator. I enlist some of these useful steps below.

Identify entry points: Install proper scanning software programs to identify all entry points from the internet into the internal network. Any attack on the network needs to start from these points. Identifying these entry points, however, is not at all an easy task. It is better to take the help of skilled ethical hackers who have taken special network security training to perform this task successfully.

Perform attack and penetration tests: By running the attack and penetration tests, you can identify those vulnerable points in the network that can be easily accessed from both external and internal users. After identifying these points, you would be able to thwart attacks from external sources and correct the pitfalls that could become the entry points for intruders to hack into your network. The test must be done from both the internal as well as external perspectives to detect all the vulnerable points.

Configure firewalls: A firewall, if not configured properly, can act as an open door for an intruder. Hence, it is vitally important to set the rules to allow traffic through the firewall that is important to the business. A firewall must have its own configurations depending upon the security aspect of your organization. From time to time, proper analysis of the composition and nature of the traffic itself is also necessary to maintain security.

Use password-less authentication: Regardless of the policies above, passwords are less secure than SSH or VPN keys, so think about using these or similar technologies instead. Where possible, use smart cards and other advanced methods.

Install anti-virus software: Both intrusion detection systems and anti-virus software must be updated regularly and, if possible, on a daily basis. The updated version of anti-virus software is necessary as it helps in detecting even the latest virus.

Use virtualization: Not everyone needs to take this route, but if you frequent sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment like Parallels or VMware Fusion that sidesteps your operating system to keep it safer.
Use encryption: Even if someone is able to steal your data or monitor your internet connection, encryption can prevent hackers from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker or FileVault, encrypt any USB flash drive that contains sensitive information, and use a VPN to encrypt your web traffic. The only shop at encrypted websites – you can spot them immediately by the "https" in the address bar accompanied by a closed padlock icon.