Network Programming Assignment

Submitted by Akash Kapoor(171210003)

Q: How firewall helps to secure PC?

A: A firewall is a network device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Network security is a broad term that covers a multitude of technologies, devices and processes. It is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Firewall's purpose is to establish a barrier between your internal network and incoming traffic from external sources in order to block malicious traffic like viruses and hackers.

For this reason we have network security management tools and applications to address individual threats and exploits and also regulatory non-compliance. Firewall is one of the way to ensure this, network security.

Firewall: It analyses carefully incoming traffic based on pre-establishes rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. It guards traffic at computer's entry point i.e. ports. Hence firewall acts as an authenticator for the traffic to permit which ports he is free to access.

Types of firewalls:

Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications.

1. **Next-generation firewalls (NGFW)**
2. **Proxy firewalls**
3. **Network address translation (NAT) firewalls**
4. **Stateful multilayer inspection (SMLI) firewalls**

Q: If I am the system admin, what precautions I would take to secure it?

A: In order to secure my system, I would take following precautions :-

1. Installing and Monitoring firewall performance: Firewalls are becoming more and more sophisticated (right along with hackers) and the latest are integrated network security platforms that consist of a variety of approaches and encryption methods, all working in tandem to prevent breaches.

2. Update passwords frequently: regularly change any personal passwords used on systems that have access to business networks.

3. Installing latest version of the antivirus software: not performing regular updates of your anti-virus software, we're putting our network at greater risk and creating potential cyber security issues, as hackers find ways to "crack" these tools and can deploy new viruses. Staying ahead of them by using the latest versions of software is critical.

4. Creating VPNs (Virtual Private Network): VPNs create a far more secure connection between remote computers (home networks or computers used by people on the road) and other “local” computers and servers. These networks are essentially only available to people who should have access to your systems, including our wireless network, and to equipment that’s been authorized in your network settings.

5. Training Ourselves: Educating ourselves and others about how to avoid major security risks is possibly the greatest weapon you have in combating cybercrime.

6. **Use whole disk encryption** on all laptops that will ever leave home. You never know when someone will steal your data or break into your car or hotel room and lift the laptop.

7. Speaking of Web servers on the Internet, if you have them, you should **scan regularly for exploits**.

8. In a wireless network, I would hide my SSID(Service Set Identifier) also disable its Web management interface.

9. Always use authentication on wireless access points.

10. Keep your system and its application updated.