ASSIGNMENT 1 (NETWORK PROGRAMMING)

[BHAVNA VERMA , 171210019, B.TECH 3RD YEAR (CSE)]

Q1. How firewall helps to secure PC?

Ans.

A firewall is simply a *program or hardware device* that filters the information coming through the Internet connection into your private network or computer system.

They can be used by both individuals and large businesses to filter the information going in and out of your computer via the internet. If the firewall filter catches anything suspicious, it denies it access to your computer system and private network.

*Firewalls are vital for stopping dangerous or fraudulent traffic from accessing your network***.** They block specific programs from accessing the internet if the activity is deemed too risky.

In this day and age, every computer needs a firewall in order to protect your sensitive data.

How it works?

Let's say that you work at a company with 500 employees. The company will therefore have hundreds of computers that all have network cards connecting them together. In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make FTP connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole.

With a firewall in place, the landscape is much different. A company will place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The firewall can implement security rules.

What Kind of Attacks Do Firewalls Protect Against?

Firewalls prevent cybercriminals from gaining access to your personal information. The issues include:

- *Backdoor Access: A backdoor* refers to any security holes or bugs that, when exploited, allow unauthorized control over the program. Even entire operating systems like Windows can have backdoors, and an experienced hacker knows how to take advantage of them.
- *Remote Login Hijacking:* A remote desktop allows you to connect and control your computer from another location over the internet. However, hackers can hijack the login, access your machine, and steal your files.
- *Email Abuse:* This type of attack targets an individual in which the perpetrator sends thousands of emails to clog the victim's inbox. Spam email is also popular and while most is merely annoying, some may contain viruses and malware.
- *Source Routing:* When data packets are traveling through an online network, they are typically "passed along" by multiple routers before reaching its destination. Some hackers take advantage of this system by making malicious data packs look like they're coming from a trusted source. Many firewalls disable source routing for this reason.

Q2. If you are system admin, what precautions or steps you will take to secure it ?

Ans.

1. Keep up with system and software security updates
Aside from adding extra features, they often cover security holes. This means the provider of the operating system (OS) or software has found vulnerabilities which give hackers the opportunity to compromise the program or even your entire computer.

It's not just your OS that should be kept up-to-date. All software that you run on your computer could potentially have flaws. When updates are available, you might see a popup when you open the software.

2. Have your wits about you.
Make sure you have your wits about you and think twice about opening or clicking on anything that doesn't look legit. Don't rely on spam filters to always catch sketchy

emails. Criminals are constantly trying to outsmart these settings and now and again they'll get through.

3. Enable a firewall

A firewall acts as a barrier between your computer or network and the internet. It effectively closes the computer ports that prevent communication with your device. This protects your computer by stopping threats from entering the system and spreading between devices.

4. Adjust your browser settings

Most browsers have options that enable you to adjust the level of privacy and security while you browse. These can help lower the risk of malware infections reaching your computer and malicious hackers attacking your device. Some browsers even enable you to tell websites not to track your movements by blocking cookies.

5. Install antivirus and anti spyware software

Any machine connected to the internet is inherently vulnerable to viruses and other threats, including malware, ransomware, and Trojan attacks. An antivirus software isn't a completely foolproof option but it can definitely help.

6. Password protect your software and lock your device

Most web-connected software that you install on your system requires login credentials. The most important thing here is not to use the same password across all applications. This makes it far too easy for someone to hack into all of your accounts and possibly steal your identity.

If you're having trouble remembering a whole bunch of passwords, then you could try a password manager. This will keep all of your passwords safe and you only have to remember one. A password can be combined with an email or SMS as part of a two-step verification (2SV) method for extra security.

7. Encrypt your data

Whether your computer houses your life’s work or a load of files with sentimental value like photos and videos, it’s likely worth protecting that information. One way to ensure it doesn’t fall into the wrong hands is to encrypt your data. Encrypted data will require resources to decrypt it; this alone might be enough to deter a hacker from pursuing action.

There are a plethora of tools out there to help you encrypt things like online traffic and accounts, communication, and files stored on your computer. For full disk encryption, some popular tools are VeraCrypt and BitLocker. You can find separate tools to help you encrypt your mobile device, with various apps available for both Android and iOS.

8. Use a VPN

A Virtual Private Network (VPN) is an excellent way to step up your security, especially when browsing online. While using a VPN, all of your internet traffic is encrypted and tunneled through an intermediary server in a separate location. This masks your IP, replacing it with a different one, so that your ISP can no longer monitor your activity.

What’s more, you can typically choose the server location based on your needs, such as getting the fastest speeds or unblocking geo-locked content. Additionally, a VPN can help you browse securely while using open wifi networks and access censored material (e.g. Facebook in China).