Name: Jay Prakash Kumar

Roll no.:171210030

Branch: CSE(3^rd year)

ASSIGNMENT : 1

Network Programming

1.Question: How firewall helps to secure pc ?

Ans: A firewall is a system designed to prevent unauthorised access to or from a private computer network. Firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet (often described as intranets).

All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

You need a firewall to protect your confidential information from those not authorised to access it and to protect against malicious users and accidents that originate outside your network.

One of the most important elements of a firewall is its access control features, which distinguish between good and bad traffic.

There are various types of firewall. In ascending order, they are

* Packet layer : This analyses network traffic at the transport protocol layer.

* Circuit level : This validates that packets are either connection or data packets.

* Application layer : This ensures valid data at the application level before connecting.

* Proxy server : This intercepts all messages entering or leaving the network.

In the real world, threats have evolved over the years and firewalls have evolved to deal with them. While it is still possible to buy packet only firewalls, they are not adequate for business use.

Protection against combination threats is best provided by firewalls which combine all of the above elements.

Specific functions performed by firewalls include:

* Gateway defence

* Carrying out defined security policies

* Segregating activity between your trusted network, the Internet and your DMZ (a protected zone midway between your network and the Internet, where you would perhaps have your web or email server).

* Hiding and protecting your internal network addresses (NAT)

* Reporting on threats and activity.

2.Question : if you are a system admin what precautions/steps you will take to secure it

Ans:8 easy steps to secure your computer

Whether you use your computer primarily for work tasks or personal use or both, it’s highly likely you want to keep it and its contents safe and secure. When it comes to computer security, a broad range of threats should be considered, including malicious attacks by hackers and people physically stealing your computer and the information it houses.

Thankfully, there are steps you can take to mitigate the risk of having your computer compromised. The measures you go to to keep your information safe will depend on several factors. For example, if you have particularly sensitive information stored, then you might be willing to invest more time and resources protecting it. Similarly, if you think there’s a particularly high risk of someone wanting to hack into your system or steal your computer, you may want to go to extra lengths.

For the average user, taking several basic measures should be sufficient enough secure your computer and its contents. In this post, we’ll outline eight easy steps you might want to consider. While they’re all fairly straightforward to implement, some take a bit more time than others or involve paid options. As such, you might need to weigh up which solutions are necessary in your situation. Let’s jump in!

1. Keep up with system and software security updates

While software and security updates can often seem like an annoyance, it really is important to stay on top of them. 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.

Typically if an update is available for your OS, you’ll get a notification. You can often opt to update immediately or set it to run at a later time. While it can be inconvenient to stop what you’re doing for half an hour for an update to take place, it’s often best to just get it done out of the way.

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.

Even though they are usually a good thing, it’s prudent to be wary of updates. Sometimes software companies will offer pre-release versions to try. These may be unstable and should be used at your own risk. Even with stable release versions, you may want to wait a day or two in case there are any obvious bugs. Just remember to go back to it when you’re ready.

Another thing to watch out for is a fake update. These might be used by hackers to persuade you to click a link or enter credentials. You can avoid falling prey to these by doing a little research into the latest updates from the software company. Simply search for the latest version to see if the alert you received makes sense. Alternatively, you can plug the popup text in a search engine to find out if it’s a known scam.

2. Have your wits about you

It should go without saying, being suspicious is one of the best things you can do to keep your computer secure. Admittedly, with hacker techniques becoming increasingly sophisticated, it can be difficult to tell when you're under attack. All it takes is one email open or link click and your computer could be compromised.

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. It can also help prevent your data leaving your computer.

If your computer ports are open, anything coming into them could be processed. This is bad if it's a malicious program sent by a hacker. While it's possible to close ports manually, a firewall acts as a simple defence to close all ports. The firewall will open the ports only to trusted applications and external devices on an as needed basis.
If your operating system comes with a firewall (e.g. Windows XP onward), you can simply enable the built-in firewall. In

Windows, this can be found by navigating to **Control Panel>System** and **Security**. You might choose to install an additional firewall as an extra layer of defense or if your OS doesn’t already have one. A couple of free options are comodo and Tinywall. Antivirus software often comes with a built-in firewall too.

The firewalls discussed above are software firewalls. There is a second type known as a hardware firewall. While these can be purchased separately, they often come built into home routers. It could just be a simple case of checking if yours is turned on.

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.

However, many of the options are disabled by default, so you could unwittingly be exposing far more than you need to each time you browse. Thankfully, it should only take a few minutes to go into your browser settings and make the necessary adjustments. Chrome ,firewall, and Edge all provide detailed instructions to help. While using these browsers you can add an additional layer of protection by installing an anti-tracking browser extension like Disconnect or uBlock Origin.

On the topic of browsers, you should choose yours carefully. The ones mentioned above are generally considered safe. But

since updates and patches occur all the time, you never know when a new hole could appear and how big it will be. If you want more privacy, you can consider steering away from traditional options and look at privacy-focused alternatives like Epic privacy Browser, Comodo Dragon
or Tor Browser.

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. There are free options out there, but they’re limited, and besides, the paid programs won’t set you back a whole lot. Bitdefender , is a popular option that I recommend. For alternatives take a look at this data backed comparison of antivirus.

Spyware is a specific type of malware that is designed to secretly infect a computer. It then sits in the system, gathers information, and sends it to a third party. The information is typically of a sensitive nature, such as credentials or banking information. This can ultimately lead to identity theft, a multi-billion dollar industry.

many antivirus programs have anti spyware built in, but there are some dedicated solutions.

If spyware has found its way onto your computer, then it’s very possible you can remove it. There are a ton of options for spyware removal, including many free offerings and some paid single use tools.

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. 2SV usually kicks in when you log into a website or app from a new or unrecognized device requiring you to verify your identity with a PIN code.

While many security steps relate to intangible threats, there is always the possibility that someone could get their hands on your actual computer. A simple line of defence here is to have a strong computer password to at least make it more difficult for them to enter.

Other forms of verification include biometric methods like a fingerprint or retina scan. Alternative physical verification methods might involve key cards and fobs, such as those offered by Yubico . Any of these can be combined with each other and/or a password as part of a two-step authentication (2FA) process.

If you’re concerned about someone actually walking away with your computer, another option is a physical lock. This is an ideal solution for laptops but can also be used on home or work computers. Kensington locks and other similar brands are small locks that insert into a special hole in the device. Some require a physical key while others work using a code. There *are* solutions for tablets, although these tend to be more cumbersome and more suitable for things like point-of-sale.

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).

When it comes to choosing a provider, there are some okay free offerings out there, but monthly rates for paid services can be pretty low, even as little at $3 per month. The free ones are typically limited in features but can be good for getting a feel for what’s available. Some paid options have free trial periods for the full service and most offer generous money-back guarantee periods.