Assignment -1

Session : 2019-20

B.Tech. 3rd Year 6th Semester

Network Programming

Submitted To:

Dr. R. K. Arya
Dept. of Computer
Science &
Engineering
NIT, Delhi

Submitted By:

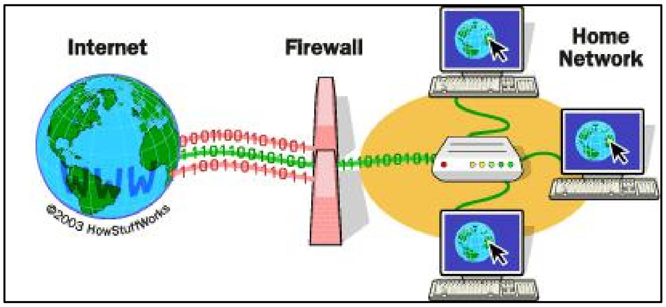
Vikas Dhurwey
171210057
Date : 10 / 3/2020

Q1) How Firewall helps to secure PC?

Solution:-

What Is a Firewall?

A firewall is the first line of defense for your network. The basic purpose of a firewall is to keep uninvited guests from browsing your network. A firewall can be a hardware device or a software application that is usually positioned at the perimeter of the network to act as the gatekeeper for all incoming and outgoing traffic.



A firewall allows you to establish certain rules to identify the traffic that should be allowed in or out of your private network. Depending on the type of firewall that is implemented, you can restrict access to only certain IP addresses and domain names or you can block certain types of traffic by blocking the TCP/IP ports they use.

How Does a Firewall Work?

There are basically four mechanisms used by firewalls to restrict traffic. One device or application may use more than one of these to provide in-depth protection. The four mechanisms are packet filtering, circuit-level gateway, proxy server, and application gateway.

Packet Filtering

A packet filter intercepts all traffic to and from the network and evaluates it against the rules you provide. Typically the packet filter can assess the source IP address, source port, destination IP address, and destination port. It is these criteria that you can filter to allow or disallow traffic from certain IP addresses or on certain ports.

Circuit-Level Gateway

A circuit-level gateway blocks all incoming traffic to any host but itself. Internally, the client machines run software to allow them to establish a connection with the circuit-level gateway machine. To the outside world, it appears that all communication from your internal network is originating from the circuit-level gateway.

Proxy Server

A proxy server is generally put in place to boost the performance of the network, but it 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. If User A goes to Yahoo.com, the proxy server sends the request to Yahoo.com and retrieves the webpage. If User B then connects to Yahoo.com, the proxy server just sends the information it already retrieved for User A so it is returned much faster than having to get it from Yahoo.com again. You can configure a proxy server to block access to certain websites and filter certain port traffic to protect your internal network.

Application Gateway

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. All communications go through two connections — client to application gateway and application gateway to the destination. The application gateway monitors all traffic against its rules before deciding whether to forward it. As with the other proxy server types, the application gateway is the only address seen by the outside world, so the internal network is protected.

Q2)If you are system admin ,what precaution you will take to secure it?

Solution:- Following Steps I will take:-

1. Do you need to be connected to the internet all the time?

The answer to this for me (and I suspect more and more people) is a resounding ‘‘yes!’’, but if you have a computer running for long periods of time and you don’t need to be connected to the internet, then it’s probably quite prudent to switch your internet router off. Hackers tend to prefer to exploit ‘‘always on’’ connections, and if your internet connection is more sporadic, you’ll be less attractive to them.

However, for most people, this just isn’t going to be practical. More and more of the stuff we do these days requires an internet connection. With Windows 8 coming later this year and new versions of the Mac operating system, our computers will be demanding ‘‘always on’’ connections. It’s not just computers either- it’s our digital TV boxes and even our fridges and dishwashers (assuming you have an internet ready one!). If this is the case, you’ll need to ensure that you protect your connection to the internet at it’s entry point- usually your router.

2. Make sure your router has a decent firewall

A firewall is a piece of software or hardware that (simply speaking) lets the good stuff in and the bad stuff out. Most internet service providers offer a free router and modem when you sign up with them. Make sure that it has a decent firewall. If you are a tech-savvy person then you can even upgrade the firmware (using the likes of Tomato or DD-WRT) on many routers to improve the security amongst other things. This Lifehacker article gives some good tips on how to do this.

3. Make sure your Computer or Device has a decent firewall

Most computers these days have an integrated firewall built in to the operating system. Windows has the imaginatively titled ‘‘Windows Firewall’’ and Mac OS X has an integrated one too (see here for more information on how to enable the Mac OS X firewall in Snow Leopard). For Linux, it depends on your flavour, but this article from Tech Radar gives a list of decent firewalls you could consider.

4. Install Decent Anti-virus Software

I know some people believe the conspiracy theory that some of the software houses that produce anti-virus applications actually generate the viruses in the first place. The thought is that they do this in order to whip up some hysteria so that more people will buy their product.

Although it's tempting to believe this, I don't think there is much truth in it. This article from Computer Hope gives some excellent points against the view. There are some people that say having anti-virus software is a waste of time as long as your careful and that all they do is slow down your computer.

The truth is, anti-virus software is a must for almost everyone. Yes, they will slow down your computer a little, but I think that is a pill worth swallowing as opposed to being infected by a virus. You don't need to spend any money on it either. One of the best anti-virus applications for PCs is Microsoft's own Security Essentials which will be built in for the first time to the forthcoming Windows 8.

It's a complete myth that Mac users are exempt from viruses as the recent Mac Flashback virus outbreak shows. There aren't many free anti-virus applications for the Mac, as this article from the Guardian recommends, you could always try ClamXav.

Finally, anti-virus applications have to be updated regularly- I'd recommend at least twice a day. Make sure you check the settings. Also if you use USB thumb drives or external hard drives, do scan them for viruses- particularly if the drive belongs to someone else. I know of many friends whose computers have been infected by using an infected drive belonging to a friend.

5. Keep Your Computer Up to Date!

I know it's annoying, but make sure you check your computer for updates! I've seen so many cases of computers that have never had any updates done to the operating system. Both Microsoft and Apple roll out updates regularly to their operating systems. These can be important security patches and you may be compromised if you don't install them!

6. Don't Visit Porn Sites (or any other dodgy or affected site)!

Did I really write that? Erm, yes I did. The problem is, that there are sites out there that are out to get you. They may have been affected by a worm that modifies the website with the intention to infect your computer with a virus. Some sites are there to deliberately get you. Things are a little better these days, but there are still plenty of cases of infected sites. Be careful where you're browsing- and again make sure you're anti-virus software is up to date.

7. Keep Your Password Safe and Hard to Guess.

I wrote an article before about how easy it is for your password to be compromised. The truth is you can't trust any site that you give your password to because you don't know how they store it. It's best to use a different password for each website your sign up to. I know that sounds hard, but it's quite easy to do- more information in my earlier article.

I'd also highly recommend the password manager- Last Pass. This manages all your passwords securely so that you never have to type it on your computer (in case you are infected by a keyboard sniffer) or store them anywhere insecurely. It also has a password generator, so you can effectively have a different strong complicated password for each site you visit. It is highly recommended!

Finally, be careful about saving passwords on applications on your computer. Famously, the FTP client Filezilla stores your passwords in plain text. Not great for security.

8. Use a Decent Web Browser

Most people still use Internet Explorer or Safari for browsing. They’ve come on in recent years- especially Internet Explorer. Still, my personal recommendation is to use Google Chrome as your browser as it’s been hailed as the most secure of browsers again and again.

9. Don’t Trust Public Wifi

If you surf the web whilst sipping your latte in your local coffee shop beware! Did you know that much of your internet connection (web browsing and email) is being sent over the connection unencrypted? Anyone malicious in the coffee shop could be listening in and stealing your passwords. If you have a 3G connection then use that, but if not, you’ll need to secure your connection. Websites that use https (Facebook and Twitter for example) encrypt your data, but most websites won’t. For this, you’ll need to use a VPN or virtual private network. This encrypts your connection by connecting to a secure server in the middle. You can build your own (as this Lifehacker article tells you), but it’s probably easier to use a VPN service. Again, Lifehacker comes to the rescue with a list of the best VPNs. Personally, I use the VPN service from Private Internet Access* which is reliable and very secure.

10. Never Leave Your Computer Unattended

I know this is obvious, but don’t leave your computer on if you’re not around. I suppose it depends on where the computer is. I have a server at home that is on all the time, but I do trust my wife not to hack in to the computer and install a virus! It’s not enough to go to the lock screen either, as someone could just connect a device to your computer and steal your data or even your whole computer. It’s probably a good idea to look at encrypting your hard drive, but that’s for another time…!