Computer Science & Engineering

National Institute of Technology, Delhi

NETWORK PROGRAMMING

ASSIGNMENT -1

Submitted To:

Dr. RAVI ARYA

Assistant Professor

NIT DELHI

Submitted By:

KRISHAN KUMAR

Roll No.- 171210035

Date: 09/03/2020

Q1) How Firewalls helps to secure PC?

Ans:->*In order to understand how firewalls, help to protect our PCs, firstly* ***we have to understand that what is firewall.*** *Secondly* ***from what kind attacks do firewalls protect our PC****.*

*In a nutshell****, Firewalls are hardware or software used to prevent unauthorized access to your computer network.*** *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 firewalls catch anything suspicious, it denies it access to your computer system and private network.*

Kind of Attacks Do Firewalls Protect our PC:

Firewalls prevent hackers from gaining access to your personal information. The issues include, but are not limited to:

- ***Backdoor Access****: A backdoor refers to any security holes or bug that, when exploited, allow unauthorized control over the program. Even entire operating systems like Windows, mac Window etc 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 system from another location over the internet. However, hackers can hijack the login, access your machine, and steal your files from your system.*
- ***Email Abuse****: This kind of attack targets an individual in which the perpetrator sends thousands of emails to clog the victim's inbox. Spam email is popular and while most is merely annoying, some may contain viruses and malware.*
- ***Source Routing****: When data packets are traveling through an 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 also.*

Method used by Firewalls protect our PC from above attacks (to block unwanted traffic):

Static Packet filtering: *Every message you send back and forth from your computer to the Internet uses packets. The message is segmented into a certain number of packets, and each packet is packaged with certain information including the destination and source IP, the destination and source port, the number that indicates the sequence for*

the packet for the destination computer to put the entire message back together and the data. A static packet filtering technique looks at the port.

Let take example how firewalls used static packet filtering method to identify malicious content. For instance, websites run on port 90, outgoing SMTP email uses port 25 and DNS requests work on port 53. When you use a router, the firewall blocks all incoming traffic based on packet analysis unless you allow a specific port to forward to a specific server. For example, if you run a web server, you then use the router's port forwarding capabilities to send the packets to the web server. With the incoming traffic, you want to white list any traffic. In other words, block all the traffic except any traffic on a specific list. In this case, port 90 is allowed so port 90 requests are sent to the web server. Sometimes, we want traffic to enter the network such as a VPN or private network with connections over the Internet. In this case, we can use a firewall as a proxy. Proxy servers (lets you connect to the server) and then your messages are forwarded to the intended recipient. The recipient uses the same proxy server to send you a return message. Security in above technique is that the recipient and sender never see the technical detail such as local IP addresses. When you allow transfer of data from one computer to another over the Internet, then source IP and port are included in the packet. When we use firewall proxy, that information is eliminated from the packet and the proxy's IP address is shown instead. The result of this that an attacker does not see the internal computers local IP address, which is one piece of information needed to send a calculated attack to a specific server on a corporate network.

Dynamic packet filtering: *It is also called "Stateful inspection". It is advancement of static packet filtering. With static packet filtering, only header information is analyzed. With dynamic packet filtering, the packets are analyzed down to the application layer, which means more of the actual data is reviewed. Packets are compare with the outgoing packets from the source internal computer. If packet information matches the data from outgoing packets, the firewall generally lets the packets flow. If a reply does not match the intended request from the source computer, the firewall then drops the packet and rejects the connection.*

Q2) What precaution will be taken by system admin to secure their system?

Ans-> *There are many ways to protect or secure computer. If you are admin of a system, the following are some steps/precautions should be taken by you to secure your system :->*

- **Always update operating system updates**:-> *This is most important step to secure system always install updates, especially security updates, when they become available for your operating system. When operating systems are developed then bugs or programs errors are unfortunately created that could cause security vulnerabilities or make your system act unexpectedly. To overcome these bugs or errors, companies will routinely release updates and patches to fix any security vulnerabilities or errors as they are discovered.*

- **Do not use same password at every site:->** *if you use the same password at every site, and one of those sites was hacked, the hacker now has your account information everywhere that you have an account. They can login to your email, see what other accounts you have, banks that you use, etc and gather even more private information about you.*

- **Make all applications up-to-date:->** *Most commonly method used by computer infections to infect our system are security vulnerabilities in your installed programs. The common program that are targeted due to their large install base are like web browsers, Microsoft Office, Adobe Reader, Adobe Flash, Adobe Shockwave etc. In order to make system as secure as possible, system admin need to make sure these programs are updated when new security fixes are released.*

- **Install and make anti-virus software up-to-date:->** *It is very important that your computer has antivirus software running on your machine. On having antivirus, program running, files and emails will be scanned as you use them, download them, or open them. If any virus is found in anyone of the files/folders you are about to use, the antivirus program will stop you from being able to run that program and infect yourself.*

- **Use a firewall :->** *The importance of using a Firewall on your computer is that you have all the latest security updates, you are still susceptible to unreported, unpatched or unknown vulnerabilities that a hacker may know about your system. Sometimes hacker discover new security holes in a software or in operating system long before the company does and many people get hacked before a security patch is released. By using firewalls, the majority of these security holes will not be accessible as the firewall will block the attempt.*

- **Ignore and close the web pop ups that pretend to be a Windows alert:->** *Some software vendors use another tactic to display web pop ups that pretend to be an alert from your operating system. These alerts look like a Windows or Mac window, but are instead a web popup trying to get you to click on the ad. If you see these types of advertisements then just close your browser to close the message.*

- **Be vigilant when you are using Peer-To-Peer Software:**-> *Using a program like Bit-torrent for legitimate applications is perfectly fine. On other side, if you use P2P applications for copyrighted movies or software there is a good chance that they may contain Trojans as well. It is common for malware developers to distribute malware on P2P networks that pretends to be a program required to view a movie or play a game. However, it is strongly suggested that you do not use Peer-to-Peer software for illegal activities.*