Network Programming

Assignment 1

Submitted by
Aniket
171210008
CSE -3rd Year

Submitted To
Dr.Ravi Kumar Arya,PhD
Assistant Professor
NIT Delhi

Question 1:How does firewalls helps to secure PC.

Firewall:A firewall around a computer is like the wall around a castle or city. It protects the computer or network by limiting points of access and providing criteria that must be met before being allowed to enter.

A firewall may be implemented as a hardware device (such a Linksys or Netgear firewall) or in software, such as the Windows Firewall or the MacOS Firewall..

Firewalls function using a system of either inclusive or exclusive parameters, allowing specific types of communication in or excluding others. Generally, a firewall is controlled by an access control list, which has a particular set of guidelines that allow or resist access to specific computer communications. These guidelines can be customized to fit any need on just about any device capable of going online.

There are two types of firewalls: network firewalls and host-based firewalls. Network firewalls are typically used by businesses that contain a comprehensive network of multiple computers, servers, and users. The network firewall monitors the communications occurring between the company computers and outside sources. If a company wishes to restrict certain websites, IP addresses, or services like Instant Messenger, it can do so using a network firewall.

Firewalls stop intruders from accessing this information and protect the business from cyber attacks.

Host-based firewalls work similarly but are stored locally on a single computer. Every home computer should have some kind of host-based firewall installed on it. This

functions as the first line of defense against cyber criminals and various online scams and attacks.

Host-based firewalls are also recommended for business computers that are network connected but not protected by a network firewall. They can also be useful for homes with multiple computers sharing the same network.

Most of the time, home computers are covered by a hardware firewall, like a router, which protects the network. But every home computer should also have a host-based system kind in place to guard against specific types of attacks.

Host-based firewalls are easy to install and protect your computer from malware, cookies, email viruses, pop-up windows, and more. Along with desktop computers, mobile devices can be installed with firewalls to protect online activity on the go

Question 2:If you are a system admin ,what precautions/steps you will take to secure it ?

1. Privilege and access control

One way to increase the security of the systems is to control what privileges individuals have and what data they are given permission to access. If users only have access to the information they need and can only do with it what you give them permissions for, there is less likelihood that either the network or your data will be compromised.

2. Limit unnecessary network shares

Malware can easily spread across a network, especially if there are a lot of unprotected network shares. To reduce the risk, remove those shares which are redundant or unnecessary and put security in place for essential ones, such as printers.

3. Run critical systems on an isolated network

Some elements of operations are going to be more vulnerable than others. If you endure those risks as part of your acceptable risk policy, then it makes sense that we should keep those risks separate from your critical systems.

4. Block unused IP ports

Every port is a door through which an attacker can gain entry to your system. If an unused port remains open, it enables malware like Trojans and worms to communicate with remote intruders who can hijack our network. Regularly check what ports we are using and using firewall to seal off those which are no longer needed

5. Control downloading from external networks

Controlling downloads from external networks will protect PCs from viruses.

6. Use a firewall

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