Network programming

Assignment-1

1. How does firewall helps to secure pc ?

Ans.- At their most basic, firewalls work like a filter between your computer/network and the Internet. You can program what you want to give inputs and what you want to get out.

It is a network security system designed to prevent access to or from a private network without permission. Firewalls can be implemented as a hardware or software or a combination of both. These prevent unauthorized Internet users from accessing private networks especially intranets. Firewall examines each message which enter or leave the intranet and blocks those the messages which do not meet the specified security criteria.

These are used to protect both home and corporate networks. A typical firewall program filters all the information coming through the Internet to your network or computer system.

There are several types of firewall techniques for filtering :

Packet Filter: Accepts or rejects the packets leaving or entering the network based on user-defined rules. Packet filtering is difficult to configure. In addition, it is susceptible to IP spoofing.

Application Gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers.

Circuit-level Gateway: Applies security mechanisms after establishing TCP or UDP connection and then the packets can flow between the hosts without further checking.

Proxy Server: Intercepts all messages which enter and leave the network. The proxy server effectively doesn't show the true network addresses.

Stateful inspection: It is a new method that doesn't check the contents of each packet but it compares certain important parts of the packet to the database .

Information traveling from inside the firewall to the outside is compared to some specific defining characteristics. If the information matches maximum, it is allowed through. Otherwise it is discarded.

In practice, many firewalls use more than one technique. A firewall is the first step in defense for protecting private information. For more secure transmission of data, it can be encrypted.

Next Generation Firewall (NGFW)

These work by filtering network and Internet traffic based upon the applications or traffic types using specific ports. These firewalls along with the features of a standard firewall and quality of service (QoS) functionalities provide smarter and deeper inspection.

The need of Firewalls for Personal Use

- Firewalls work much more simply for use in home.
- We use a personal firewall is to protect private network and your personal computer and from malicious mischief.
- Malware, malicious software, is the main threat to your personal computer. The first type of malware that comes to mind is viruses. A virus can quickly cause a lot of damage to your files and can be transmitted to your computer from anywhere, that is through email or over the Internet.
- These malicious programs are programmed to steal your personal information for the purposes of identity theft.
- There are two ways a Firewall can prevent this stealing of information by prohibiting all traffic unless it meets a set of criteria already specified.

2. If you are a system admin, what precautions /steps you need to take to secure it ?

Ans.-A sysadmin must know everything about the system's underlying platform (i.e., Windows, Linux) as well as should be familiar with networking, backup, data restoration, IT security, database operations, middleware basics, load balancing, and more. Sysadmin tasks include server management, maintenance, and repair, but also any functions that support a smoothly running production environment with minimal (or no) complaints from customers and end users.

The following practices should be followed by sysadmin:

1.Documentation

Sysadmins keep records of hardware and software types, counts, and licenses. If there is an problem, documentation helps to find it by identifying the hardware, virtual machine, appliance, software, etc., that may be involved.

2.Hardware inventory

Maintain lists of all servers with the following details:

- **OS:** Linux or Windows, hypervisor with versions
- **RAM:** DIMM slots in physical servers
- **CPU:** Logical and virtual CPUs
- **HDD:** Type and size of hard disks
- **Open ports:** Ports opened at the server end for incoming traffic
- **IP address:** Management and interface IP address with VLANs
- **Engineering appliances:** e.g., Exalogic, PureApp, etc.

3. Software inventory

- **Third-party software:** Any software not shipped with the installed OS

4. Server health checkup

- **Running processes:** Check for processes consuming more resources than expected, and take action to fine-tune the applications (with the help of the application team).
- **Memory utilization:** Check memory utilization and clear the cache, if required.
- **Zombie processes**

5. Backup and disaster recovery planning

The recommended backup criteria for production servers is:

- **Incremental backups:** Daily, Monday to Friday
- **Full backup:** Saturday and Sunday
- **Disaster recovery drills**

6. Patching

OS patches for known vulnerabilities must be implemented. The types and levels of patches include:

- Security
- Critical
- Moderate

When a patch is released, check to how it applies to your system (e.g., does the vulnerability affect the hardware in your system?), and take any necessary actions to apply the patches when required.

7. Application compatibility

Check the application's compatibility with your hardware and OS , and load testing (with the support of application team).

Server hardening

Linux:

- **Set a BIOS password:** This prevents users from altering BIOS settings.
- **Sudo users:** Make sudo users and assign limited privileges to invoke commands.
- **TCP wrappers:** This is the weapon to protect a server from hackers.
- **Firewall/iptables:** Configure firewalld and iptables rules for incoming traffic to the server.
- **Secure and audit logs:** Check the logs regularly and when required.

Windows:

- **Set a BIOS password:** This prevents users from altering BIOS settings.
- Install antivirus software.
- Prevent unauthorized access from your systems.