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 get out and what you want to get in.

It is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially 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.

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

There are several types of firewall techniques that will prevent potentially harmful information from getting through:

Packet Filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it 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. This is very effective, but can impose a performance degradation.

Circuit-level Gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy Server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Stateful inspection: A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Next Generation Firewall (NGFW)

Firewalls called next generation firewalls (NGFW) , work by filtering network and Internet traffic based upon the applications or traffic types using specific ports. Next Generation Firewalls (NGFWs) blend the features of a standard firewall with quality of service (QoS) functionalities in order to provide smarter and deeper inspection.

The need of Firewalls for Personal Use

- For home use, firewalls work much more simply.
- The main goal of a personal firewall is to protect your personal computer and private network from malicious mischief.
- Malware, malicious software, is the primary threat to your home computer. Viruses are often the first type of malware that comes to mind. A virus can be transmitted to your computer through email or over the Internet and can quickly cause a lot of damage to your files. Other malware includes Trojan horse programs and spyware.
- These malicious programs are usually designed to acquire your personal information for the purposes of identity theft of some kind.
- There are two ways a Firewall can prevent this from happening.
- It can allow all traffic to pass through except data that meets a predetermined set of criteria, or it can prohibit all traffic unless it meets a predetermined set of criteria.

Comodo Firewall

Comodo Firewall uses the latter way to prevent malware from installing on your computer. This free software firewall, from a leading global security solutions provider and certification authority, use the patent pending "Clean PC Mode" to prohibit any applications from being installed on your computer unless it meets one of two criteria. Those criteria are a) the user gives permission for the installation and b) the application is on an extensive list of approved applications provided by Comodo. With this feature, you don't have to worry about unauthorized programs installing on your computer without your knowledge.

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

Ans.- System administrators are critical to the reliable and successful operation of an organization and its network operations center and data center. A sysadmin must have expertise with the system's underlying platform (i.e., Windows, Linux) as well as be familiar with multiple areas including networking, backup, data restoration, IT security, database operations, middleware basics, load balancing, and more. Sysadmin tasks are not limited to 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.

Although sysadmins have a seemingly endless list of responsibilities, some are more critical than others. If you work in a sysadmin role (or hope to one day), make sure you are ready to follow these best practices.

1.Documentation

Documentation is how sysadmins keep records of assets, including hardware and software types, counts, and licenses. Should there be any issues in the production environment, documentation helps identify the hardware, virtual machine, appliance, software, etc., that may be involved.

2.Hardware inventory

Maintain lists of all your physical and virtual 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
- **External storage (SAN/NAS):** Make and model of storage with management IP address and interface IP address
- **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

- **Configured applications:** e.g., Oracle WebLogic, IBM WebSphere Application Server, Apache Tomcat, Red Hat JBoss, etc.
- **Third-party software:** Any software not shipped with the installed OS

4. Server health checkup

- **Running processes:** Check for processes that are consuming more resources than expected, and take action to fine-tune the applications (with the help of the application team).
- **CPU utilization:** Consistently monitor and check the CPU utilization of the critical process like "java", "http", "mysql" etc. to ensure that these are not consuming the CPU resources more than expected. If it is so, then coordinate with the application team to check it at application level and fine tune the same. Parallely analyse the OS parameters like "Ulimits".
- **Memory utilization:** Check memory utilization and clear the cache, if required.
- **Zombie processes:** Check for processes where the PID still exists in the process table after it is terminated. Zombie processes degrade server performance, so find and kill any that exist.
- **Load average:** If you're having performance issues, check the load average and tune the server for performance.
- **Disk/SAN/NAS utilization:** Check the I/O reports for externally attached storage to track and check the speed of read/write operations. If you find any issues, coordinate with the storage and network teams immediately to correct them.

5. Backup and disaster recovery planning

Communicate with the backup team and provide them the data and client priorities for backup. The recommended backup criteria for production servers is:

- **Incremental backups:** Daily, Monday to Friday
- **Full backup:** Saturday and Sunday
- **Disaster recovery drills:** Perform restoration mock drills once a month (preferably, or quarterly if necessary) with the backup team to ensure the data can be restored in case of an issue.

6. Patching

Operating system patches for known vulnerabilities must be implemented promptly. There are many types and levels of patches, including:

- Security
- Critical
- Moderate

When a patch is released, check the bug or vulnerability details to see 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. Make sure to cross-verify applications' compatibility with patches or upgrades.

7. Application compatibility

Before going live with any application, check its compatibility with your hardware and operating system, and make sure to do load testing (with the support of application team).

Server hardening

Linux:

- **Set a BIOS password:** This prevents users from altering BIOS settings.
- **Set a GRUB password:** This stops users from altering the GRUB bootloader.
- **Deny root access:** Rejecting root access minimizes the probability of intrusions.
- **Sudo users:** Make sudo users and assign limited privileges to invoke commands.
- **TCP wrappers:** This is the weapon to protect a server from hackers. Apply a rule for the SSH daemon to allow only trusted hosts to access the server, and deny all others. Apply similar rules for other services like FTP, SSH File Transfer Protocol, etc.
- **Firewall/iptables:** Configure firewalld and iptables rules for incoming traffic to the server. Include the particular port, source IP, and destination IP and allow, reject, deny ICMP requests, etc. for the public zone and private zone.
- **Antivirus:** Install antivirus software and update virus definitions regularly.
- **Secure and audit logs:** Check the logs regularly and when required.
- **Rotate the logs:** Keep the logs for limited period of time like "for 7 days", to keep the sufficient disk space for flawless operation.

Windows:

- **Set a BIOS password:** This prevents users from altering BIOS settings.
- **Antivirus:** Install antivirus software and update virus definitions regularly.
- **Configure firewall rules:** Prevent unauthorized parties from accessing your systems.
- **Deny administrator login:** Limit users' ability to make changes that could increase your systems' vulnerabilities.

8. Use a syslog server

By configuring a syslog server in the environment to keep records of system and application logs, in the event of an intrusion or issue, the sysadmin can check previous and real-time logs to diagnose and resolve the problem.

9. Automation

Many sysadmin tasks (such as server health checkups, resource utilization, backup triggers, transfer files and logs, etc.) must be done at specific times. Therefore, the sysadmin must write scripts or use external tools and configure them as cron jobs to do the tasks automatically at the proper time.

10. Monitoring tools

Install and configure live monitoring tools like Nagios, HP, etc., to monitor your IT infrastructure and issue alerts about potential problems.

Conclusion

While these are the most important tasks a sysadmin is responsible for, there is much more to the role than the duties on this list.

For example, the sysadmin must coordinate with multiple teams to resolve issues, communicate with and update customers, maintain 100% uptime, hold discussions with the audit team, prepare weekly/monthly/quarterly reports, do continuous monitoring of servers and services using appropriate tools, and maintain the hardware console and respond to any triggered alarms.

The sysadmin is always a single point of content (SPOC) in the data center or network operations center for issues related to web hosting, application and server outages, and other critical IT operations problems.