ASSIGNMENT

Q.1 How the firewall help to secure the PC?

Ans. 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. Everything else is not allowed. There are several different methods firewalls use to filter out information, and some are used in combination. These methods work at different layers of a network, which determines how specific the filtering options can be.

Firewalls can be used in a number of ways to add security to your home or business.Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.Firewalls may also be a component of your computer's operating system. For example, Windows Firewall is a Microsoft Windows application that notifies users of any suspicious activity. The app can detect and block viruses, worms, and hackers from harmful activity.

Firewall Filtering Techniques

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

1.)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.

2.)Application Gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

3.)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.

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

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

Q.2) If you are a system admin what precaution /step you will you will take to secure it?

Ans.When setting up infrastructure, getting your applications up and running will often be your primary concern. However, making your applications to function correctly without addressing the security needs of your infrastructure could have devastating consequences down the line.In this guide, we will talk about some basic security practices that are best to configure before or as you set up your applications.

1.)SSH Keys

SSH keys are a pair of cryptographic keys that can be used to authenticate to an SSH server as an alternative to password-based logins. A private and public key pair are created prior to authentication. The private key is kept secret and secure by the user, while the public key can be shared with anyone.To configure the SSH key authentication, you must place the user's public key on the server in a special directory. When the user connects to the server, the server will ask for proof that the client has the associated private key. The SSH client will use the private key to respond in a way that proves ownership of the private key. The server will then let the client connect without a password.

2.)Firewalls

A firewall is a piece of software (or hardware) that controls what services are exposed to the network. This means blocking or restricting access to every port except for those that should be On a typical server, a number services may be running by default. These can be categorized into the following groups:

Public services that can be accessed by anyone on the internet, often anonymously. A good example of this is a web server that might allow access to your site.

Private services that should only be accessed by a select group of authorized accounts or from certain locations. An example of this may be a database control panel.Internal services that should be accessible only from within the server itself, without exposing the service to the outside world. For example, this may be a database that only accepts local connections. Firewalls can ensure that access to your software is restricted according to the categories above. Public services can be left open and available to everyone and private services can be restricted based on different criteria. Internal services can be made completely inaccessible to the outside world. For ports that are not being used, access is blocked entirely in most configuration.

3.)VPNs and Private Networking

Private networks are networks that are only available to certain servers or users. For example, DigitalOcean private networks enable isolated communication between servers in the same account or team within the same region.

A VPN, or virtual private network, is a way to create secure connections between remote computers and present the connection as if it were a local private network. This provides a way to configure your services as if they were on a private network and connect remote servers over secure connections.

4.)Public Key Infrastructure and SSL/TLS Encryption

Public key infrastructure, or PKI, refers to a system that is designed to create, manage, and validate certificates for identifying individuals and encrypting communication. SSL or TLS certificates can be used to authenticate different entities to one another. After authentication, they can also be used to established encrypted communication.

5.)Service Auditing

Up until now, we have discussed some technology that you can implement to improve your security. However, a big portion of security is analyzing your systems, understanding the available attack surfaces, and locking down the components as best as you can.

Service auditing is a process of discovering what services are running on the servers in your infrastructure. Often, the default operating system is configured to run certain services at boot. Installing additional software can sometimes pull in dependencies that are also auto-started.

Service auditing is a way of knowing what services are running on your system, which ports they are using for communication, and what protocols are accepted. This information can help you configure your firewall settings

6.)File Auditing and Intrusion Detection Systems

File auditing is the process of comparing the current system against a record of the files and file characteristics of your system when it is a known-good state. This is used to detect changes to the system that may have been authorizied.An intrusion detection system, or IDS, is a piece of software that monitors a system or network for unauthorized activity. Many host-based IDS implementations use file auditing as a method of checking whether the system has changed.

7.)Isolated Execution Environments

Isolating execution environments refers to any method in which individual components are run within their own dedicated space.This can mean separating out your discrete application components to their own servers or may refer to configuring your services to operate in chroot environments or containers. The level of isolation depends heavily on your application’s requirements and the realities of your infrastructure.