Ques. 1:- how firewall helps to secure the pc ?

Ans. :- security is the most important aspect in a network. Firewall is one of the most important concepts related to the network security. The term "firewall" was came to use in 1764, to describe walls which distinct the parts of a building most likely to have a fire from the rest of a structure. Firewall can be software or hardware .In computer world the firewall protection refers to protect the network or computer from to block certain kinds of network traffic. It creates a barrier between trusted and untrusted network. A firewall is designed in order to prevent or slow the spread of harmful events using firewall technologies to secure the network. Packet filtering, the firewall technologies that are currently existing can be named as Network addressing translation, Circuit-Level gateways, virtual private network, Proxy service, Application proxies and Application-Level gateway.

There are two policies for firewall to work

1. Default- Deny Policy
2. Default – Allow Policy

Default-Deny Policy:

In Default –Deny policy the administrator of firewall create a list of allowed network services and rest of the
network services are blocked.

Default – Allow Policy:

In Default –Allow policy the administrator of firewall create a list of not allowed network services and rest of the network services are allowed.
A default-deny way to deal with firewall security is by a wide margin the more secure, however because of the trouble in designing and dealing with a system in that form, numerous systems rather utilize the default-permit approach. How about we expect for the minute that your firewall administration project uses a default-deny approach, and you just have certain administrations empowered that you need individuals to have the capacity to use from the Internet. For instance, you have a web server which you need the overall population to have the capacity to get to.
Serval types of Firewall:-

- Packet filtering firewall: This kind of firewall has a rundown of firewall security rules which can protect traffic based on IP protocol, IP location and/or port number. Under this firewall administration program, all web activity will be permitted, including electronic assaults.

- Stateful firewall: This is like a packet separating firewall, yet it is more wise about staying informed regarding dynamic associations, so you can characterize firewall administration standards, for example, "just permit bundles into the system that are a piece of an officially settled outbound association.
- Deep packet inspection firewall: An application firewall really inspects the information in the bundle, and can accordingly take a gander at application layer assaults.
- Application-aware firewall: Like deep packet assessment, aside from that the firewall comprehends certain conventions and can parse them, so that marks or guidelines can particularly address certain fields in the convention.
- Application proxy firewall: An application intermediary goes about as a middle person for certain application activity, (for example, HTTP, or web, movement), capturing all solicitations and accepting them before passing them along. Once more, an application intermediary firewall is like sure sorts of interruption counteractive action.

Ques. 2:- if you are a system admin what steps/precautions will you take to secure it?

Ans. :- The duties of a system administrator are wide-ranging, and vary widely from one organization to another. Sysadmins are usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems. Other duties may include scripting or light programming, project management for systems-related projects.

Protect Remote Access. If your employees are allowed access to your private network from remote networks, this access should only be through a firewall that protects your private network.

Use Encryption Programs. When used properly, encryption technologies can virtually prevent files, directories, or disks from falling into unauthorized hands.

Secure Your Private Network. Many intranet or private networks consist of multiple local area networks (LANs) designed to connect your computers to resources, such as printers, servers and other applications.

Trace department business functions from users computers back to the physical servers that house their data.

Lock down VPN access. Virtual private network clients are an enormous internal security threat because they position unhardened desktop operating systems outside the protection of the corporate firewall. Be explicit about what VPN users are allowed to access. Avoid giving every VPN user carte blanche for the entire internal network.

Shut off unused network services. A large corporate network might have four or five servers actively enlisted in delivering e-mail, but a typical corporate network might also have 95 other servers listening on the SMTP port. Guess which 95 hosts are most likely to harbour latent mail server vulnerabilities. Audit the network for services that shouldn't be running.

Examine Password Credentials. Passwords are an essential element for keeping your institution's data secure. Ensure that all employees with rights to sensitive data have complex passwords that have the appropriate length and strength.

Keep Your Firewall Updated. Remember, the FFIEC requires quarterly audits to review your institution's firewall security. However, just sticking to the bare minimum of these requirements exponentially increases both your risk and vulnerability—putting your institution at the mercy of cybercriminals eager to steal passwords, customer data and even funds.

Verify Rule Efficiency. Firewalls operate on a set of rules that allow certain traffic in and out of your network. Be sure to update this ruleset regularly, accounting for new threats, and that all current rules are still efficient and relevant. Often, breaches result from old configuration that's no longer applicable or relevant at the time of the breach.

Set Clear Administrator Privileges. An important first step in providing security for your network is to establish and enforce administrator privileges, managing who has authorization to install software and change system configuration settings.