**Q.32. Explain any six Server Security Principles.**

**Ans:**

When addressing server security issues, it is an excellent idea to keep in mind the following general information security principles: ­

**Simplicity**—

* Security mechanisms (and information systems in general) should be as simple as possible. Complexity is at the root of many security issues. ­

**Fail-Safe**—

* If a failure occurs, the system should fail in a secure manner, i.e., security controls and settings remain in effect and are enforced. It is usually better to lose functionality rather than security. ­

**Complete Mediation**—

* Rather than providing direct access to information, mediators that enforce access policy should be employed. Common examples of mediators include file system permissions, proxies, firewalls, and mail gateways. ­

**Open Design**—

* System security should not depend on the secrecy of the implementation or its components. ­

**Separation of Privilege**—

* Functions, to the degree possible, should be separate and provide as much granularity as possible. The concept can apply to both systems and operators and users. In the case of systems, functions such as read, edit, write, and execute should be separate. In the case of system operators and users, roles should be as separate as possible. For example, if resources allow, the role of system administrator should be separate from that of the database administrator. ­

**Least Privilege**—

* This principle dictates that each task, process, or user is granted the minimum rights required to perform its job. By applying this principle consistently, if a task, process, or user is compromised, the scope of damage is constrained to the limited resources available to the compromised entity.

**Psychological Acceptability**—

* Users should understand the necessity of security. This can be provided through training and education. In addition, the security mechanisms in place should present users with sensible options that give them the usability they require on a daily basis. If users find the security mechanisms too cumbersome, they may devise ways to work around or compromise them. The objective is not to weaken security so it is understandable and acceptable, but to train and educate users and to design security mechanisms and policies that are usable and effective. ­

**Least Common Mechanism—**

* When providing a feature for the system, it is best to have a single process or service gain some function without granting that same function to other parts of the system. The ability for the Web server process to access a back-end database, for instance, should not also enable other applications on the system to access the back-end database. ­

**Defense-in-Depth**—

* Organizations should understand that a single security mechanism is generally insufficient. Security mechanisms (defenses) need to be layered so that compromise of a single security mechanism is insufficient to compromise a host or network. No “silver bullet” exists for information system security. ­

**Work Factor**—

* Organizations should understand what it would take to break the system or network’s security features. The amount of work necessary for an attacker to break the system or network should exceed the value that the attacker would gain from a successful compromise. ­

**Compromise Recording**—

* Records and logs should be maintained so that if a compromise does occur, evidence of the attack is available to the organization. This information can assist in securing the network and host after the compromise and aid in identifying the methods and exploits used by the attacker. This information can be used to better secure the host or network in the future. In addition, these records and logs can assist organizations in identifying and prosecuting attackers.

**Q.33. How the Server Security is Planned?**

**Ans:**

* Security should be considered from the initial planning stage at the beginning of the systems development life cycle to maximize security and minimize costs. It is much more difficult and expensive to address security after deployment and implementation.
* Organizations are more likely to make decisions about configuring hosts appropriately and consistently if they begin by developing and using a detailed, well designed deployment plan.
* Developing such a plan enables organizations to make informed tradeoff decisions between usability and performance, and risk.
* A deployment plan allows organizations to maintain secure configurations and aids in identifying security vulnerabilities, which often manifest themselves as deviations from the plan.

In the planning stages of a server, the following items should be considered:

* ­ Identify the purpose(s) of the server.

– What information categories will be stored on the server?

– What information categories will be processed on or transmitted through the server? – What are the security requirements for this information?

– Will any information be retrieved from or stored on another host (e.g., database server, directory server, Web server, Network Attached Storage (NAS) server, Storage Area Network (SAN) server)?

– What are the security requirements for any other hosts involved? – What other service(s) will be provided by the server (in general, dedicating the host to only one service is the most secure option)?

– What are the security requirements for these additional services?

– What are the requirements for continuity of services provided by the server, such as those specified in continuity of operations plans and disaster recovery plans?

– Where on the network will the server be located? ­

* Identify the network services that will be provided on the server, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network File System(NFS), or database services (e.g., Open Database Connectivity [ODBC]). The network protocols to be used for each service (e.g., IPv4, IPv6) should also be identified. ­
* Identify any network service software, both client and server, to be installed on the server and any other support servers. ­
* Identify the users or categories of users of the server and any support hosts. ­
* Determine the privileges that each category of user will have on the server and support hosts. ­
* Determine how the server will be managed (e.g., locally, remotely from the internal network, remotely from external networks). ­
* Decide if and how users will be authenticated and how authentication data will be protected. ­
* Determine how appropriate access to information resources will be enforced. ­
* Determine which server applications meet the organization’s requirements. Consider servers that may offer greater security, albeit with less functionality in some instances. Some issues to consider include—

– Cost

– Compatibility with existing infrastructure

– Knowledge of existing employees

– Existing manufacturer relationship

– Past vulnerability history

– Functionality. ­

* Work closely with manufacturer(s) in the planning stage.

The choice of server application may determine the choice of OS. However, to the degree possible, server administrators should choose an OS that provides the following: ­

* Ability to granularly restrict administrative or root level activities to authorized users only ­
* Ability to granularly control access to data on the server ­
* Ability to disable unnecessary network services that may be built into the OS or server software ­
* Ability to control access to various forms of executable programs, such as Common Gateway Interface (CGI) scripts and server plug-ins for Web servers, if applicable ­
* Ability to log appropriate server activities to detect intrusions and attempted intrusions
* ­ Provision of a host-based firewall capability to restrict both incoming and outgoing traffic ­
* Support for strong authentication protocols and encryption algorithms

**Q.34. How the server security is maintained?**

**Ans:**

**Logging:**

* Logging is a cornerstone of a sound security posture. Capturing the correct data in the logs and then monitoring those logs closely is vital.35 Network and system logs are important, especially system logs in the case of encrypted communications, where network monitoring is less effective. Server software can provide additional log data relevant to server-specific events.
* Reviewing logs is mundane and reactive, and many server administrators devote their time to performing duties that they consider more important or urgent. However, log files are often the only record of suspicious behavior.
* Enabling the mechanisms to log information allows the logs to be used to detect failed and successful intrusion attempts and to initiate alert mechanisms when further investigation is needed.
* Procedures and tools need to be in place to process and analyze the log files and to review alert notifications.

Server logs provide— ­

* Alerts to suspicious activities that require further investigation ­
* Tracking of an attacker’s activities ­
* Assistance in the recovery of the server ­
* Assistance in post-event investigation ­
* Required information for legal proceedings.

**Server Backup Procedures:**

* One of the most important functions of a server administrator is to maintain the integrity of the data on the server. This is important because servers are often some of the most exposed and vital hosts on an organization’s network.
* The server administrator needs to perform backups of the server on a regular basis for several reasons. A server could fail as a result of a malicious or unintentional act or a hardware or software failure.
* In addition, Federal agencies and many other organizations are governed by regulations on the backup and archiving of server data.
* Server data should also be backed up regularly for legal and financial reasons.

**Recovering From a Security Compromise:**

* Most organizations eventually face a successful compromise of one or more hosts on their network. Organizations should create and document the required policies and procedures for responding to successful intrusions.
* The response procedures should outline the actions that are required to respond to a successful compromise of the server and the appropriate sequence of these actions (sequence can be critical).
* Most organizations already have a dedicated incident response team in place, which should be contacted immediately when there is suspicion or confirmation of a compromise.
* In addition, the organization may wish to ensure that some of its staff are knowledgeable in the fields of computer and network forensics.
* A server administrator should follow the organization’s policies and procedures for incident handling, and the incident response team should be contacted for guidance before the organization takes any action after a suspected or confirmed security compromise.

**Security Testing Servers:**

* Periodic security testing of servers is critical. Without periodic testing, there is no assurance that current protective measures are working or that the security patch applied by the server administrator is functioning as advertised.
* Although a variety of security testing techniques exists, vulnerability scanning is the most common.
* Vulnerability scanning assists a server administrator in identifying vulnerabilities and verifying whether the existing security measures are effective.
* Penetration testing is also used, but it is used less frequently and usually only as part of an overall penetration test of the organization’s network.

**Remotely Administering a Server:**

* Remote administration of a server should be allowed only after careful consideration of the risks. The risk of enabling remote administration varies considerably depending on the location of the server on the network.
* For a server that is located behind a firewall, remote administration can be implemented relatively securely from the internal network, but not without added risk.
* Remote administration should generally not be allowed from a host located outside the organization’s network unless it is performed from an organization-controlled computer through the organization’s remote access solution, such as a VPN.