1. Storage Security Framework

→ The basic information security framework is built to achieve four security goals :-

(I) Confidentiality

(II) Integerity

(III) Availability

(IV) Accountability

- Storage security framework incorperates all security standards, procedures and controls required to mitigate threats in the storage infrastructure environment.

(I) confidentiality :-

→ Provides required hiding of information & ensures that only authorized users have access to data.

→ this requires authentication of users who need to access information.

(II) Integerity :-

→ Ensures information is unaltered.

→ Ensuring interity requires detection & protection against unautherized deletion of information

→ Provides measures such as error detection and correction for both data & system.

(III) Availability :-

→ Ensures that authorized users have reliable & timely access to system, data & application.

→ Also implies that sufficient resources are available to provide a service.

(iv) Accountability :-

→ Refers to responsibility for all events & operations that take place in data center infrastructure.

→ ~~To~~ Maintains a log of events that can be traced later for purpose of security.

2. Risk Triad

→ Risk Triad defines risk in terms of threats, assets and vulnerabilities.

→ Risk arises when a threat agent uses an existing vulnerabilities to compromise the security services of an asset.

→ To manage risks organizations primarily focuses on vulnerabilities..

• Assets :-

→ e.g, information, hardware, software and other components required to access the information.

→ To protect these assets, organizations must develop a set of parameters to ensure the availability of the resources to authorized users and trusted networks.

→ Security methods have two objective

(i) ensure network is easily accessible to the authorized users.

(ii) To make it difficult for potential attackers to access & compromise the systems

→ the security methods should provide adequate protection against unauthorized access, viruses or

- threats :-

→ threats are potential attacks. ~~that~~

→ these attacks can be active or passive

→ Active attacks :- include data modification, denial of service (DoS). They pose threat to data integrity, availability and accountability

→ Passive attacks :- are attemps to gain unauthorized access into the system.

- Vulnerability :-

→ the path that provides access to information are often vulnerable to potential attacks.

→ Each of these path contain various access points which provides different level of access to the storage resources

→ Implementing security controls at each access ~~point~~ path is known as "Defence in Depth"

→ Defence in Depth ~~uses~~ recommends using multiple security measures to ↓ the risk of threats

→ Defence in Depth is also known as "layered approach to security", because there are multiple measures for security at different levels, defence in depth gives additional time to detect & respond to an attack.

→ Attack surface
Attack vector
work factor
} 3- factors to consider when assessing the extent to which an environment is vulnerable to security threats

5. Storage Security Domain:

Ans → To identify the threats that apply to a storage network, access path to data storage can be categorized into 3- security domains

① Application access

② Management access

③ Backup, Replication and Archive

① Application access Domain :-

→ includes only these applications that access the data through file system or ~~at~~ database interface.

→ Controlling User access to data :-

- Access control services regulate user access to data
- these services. reduces the threates of stealing host identity & elevating host privileges.
- Both threats affect data integrity and confidentiality.
- Access control mechanisms used in the application access domain are user and host authentication (technical control) & authorization (administrative control).

→ Zoning is a control mechanism on the switches that segments the network into specific paths to be used for data traffic.

→ LUN masking determines which hosts can access which storage device.

(ii) Management Access Domain :-

→ Providing management access through an external network ↑ the potential for an unauthorized host or switch to connect to that network.

→ In such circumstances, implementing appropriate security measures prevents certain types of remote communication from occurring.

→ Using secure communication channel such as Secure Shell (SSH) or Secure Socket Layer (SSL).

(iii) Backup, Replication and Archive :-

→ Organization must esure that the disaster recovery (DR) site maintains the same level of security for the backed up data.

→ Protecting Backup, replication & achive infrastructure requires addressing several threats/attacks, DOS attacks & media theft.

→ Such threat represents violation of integrity, confidentiality & availability.

4. SAN Security Architecture

Ans → Storage ~~archi~~ networking environments are a potential target for unauthorized access, theft and misuse because of vastness & complexity of these environments.

→ ∴ security ~~strag~~ strategies are based on the "Defence in Depth" concept.

→ this ensures that the failure of one security control will not compromise the assets under protection.

→ Security zones	Perotection Strategies
Zone A [Authentication at management console]	• Restricts management LAN access to authorised users • implement tunelling for secure remote access to the management LAN • use of two-factor authentication.
Zone B (Firewall)	Block inappropriate traffic by (a) filtering out addresses (b) screening for allowed perotocols.
Zone C (Access-Control-Switch)	Authenticate users of FC Switches ~~us~~ using RADIUS, DH-CHAP & so on.
Zone D (Host-to-switch)	Restricts Fabric access to ~~do~~ legitimate hosts by implementing a secure zoning method such as port.
Zone E [Switch~~to~~ to switch / switch to Router]	Perotect traffic on Fabric by using E-Port authentication, encrypting the traffic in transit

Zone F (Distance Extension)	Implement encryption for in-flight data.
Zone G (Switch to Storage)	Protect the storage arrays on your SAN

5 Monitoring the Storage Infrastructure.

→ Monitoring is one of the most important aspects that forms the basis for managing storage infrastructure resources.

→ Provides the performance & accessibility status of various components.

→ Helps to analyze the utilization & consumption of various storage infrastructure resources.

* Monitoring Parameters :-

→ Storage infrastructure components should be monitored for :-

(I) Accessibility

(II) Capacity

(III) Performance

(IV) Security

(I) Accessibility :-

→ Monitoring the accessibility of h/w components or s/w components involves checking their availability status by reviewing the alerts generated ~~by~~ from the system.

→ For ex. a port failure might result in a chain of availability alerts

(ii) capacity :-

→ capacity monitoring ensures uninterrupted data availability and scalability by preventing outages before they occur.

→ Inadequate capacity leads to degraded performance.

→ For ex :- if 90% of ports are utilized in a particular SAN fabric, this could indicate a new switch might be required if more arrays & servers ~~are~~ needs to be installed on the same fabric.

(iii) Performance :-

→ Performance monitoring evaluates how efficiently different storage infrastructure components are performing.

→ also deals with utilization of resources

→ Performance measurement is a complex task that involves various components on several interrelated parameters.

(iv) Security :-

→ Helps to check ~~[illegible]~~ or track unauthorized configuration changes to storage infrastructure resources.

→ physical security of a storage infrastructure can also be continuously monitored using badge readers, biometric scans or video cameras.

~~6. Storage Management Activities~~

7. Authentication, Authorization & Kerberos in NAS environment:

→ NAS is open to multiple exploits, including viruses, unauthorized access & data tampering.

→ Permissions and ACLs (access control lists) ~~are deployed over~~ form the 1st level of protection to NAS resources by restricting accessibility and sharing.

* NAS File Sharing : Authentication and Authorization

→ In a file sharing environment, NAS devices use standard file-sharing protocols NFS & CIFS.

→ Therefore, authentication & authorization are implemented & supported on NAS devices same as in a UNIX or Windows File sharing environment.

→ Authentication :

- Authentication requires verifying the identity of a network user and therefore involves a login credential lookup on a Network Information System (NIS) server in a UNIX environment.
- Similarly, a windows client is authenticated by a windows domain controller that houses the Active Directory.
- NAS devices uses same authentication technique to validate network user credentials.

→ Authorization :-

- Defines user privileges in a network
- UNIX files uses mode bits to define access rights granted to owners, groups & other users
- Windows uses an ACL (access control list) to allow or deny specific rights to a particular user for a particular file.

* KERBEROS :

→ Kerberos is a network authentication protocol, which is designed to provide strong authentication for client / server applications by using secret-key cryptography.

→ It uses cryptography so that a client and server can prove their identity to each other across an insecure network connection.

→ In Kerberos, authentication occurs bet^{n} clients & servers.

→ The client gets a ticket for a service and the server decrypts this ticket by using its secret key.

→ An user, or host that gets a service ticket for a kerberos service is called a kerberos client.

→ The term kerberos generally refers to the key Distribution Center (KDC).

→ The KDC implements the authentication service (AS) and the Ticket Granting Service (TGS).

→ KDC has a copy of every password associated with every principal, so it is absolutely vital that KDC remains secure.