ISM

Securing the Storage Infrastructure

Topic 1.

Storage Security Framework :-

1. Accountability Service
2. Confidentiality Service
3. Integrity Service
4. Availability Service

1. Accountability → Refers to accounting for all the events and operations that take place in the data center infrastructure. The accountability service maintain a log of events that ~~tat~~ can be audited or traced later for purpose of security.

2. Confidentiality :- Provides required ~~security~~ secrecy of information and ensures that only authorized user have access to data. It covers both data in transit and data at rest.
   - data in transit (data transmitted over cable)
   - data at rest (stored in storage device)

3. Integrity :- Ensures that information is unaltered. The objective of the service is to detect and protect against unauthorized updation and deletion of data. It typically covers both data in transit and data at rest.

④ Availability :- Ensures that authorised user has reliable and timely access to data. These services enables users to access the required computer system, data and applications residing on these system.

Availability services are also implemented on the common system ~~using~~ used to transmit information among computers that may reside at different location. This ensures availability of information if a failure in one particular location occurs. This service must be implemented for both electrical data & physical data.

Topic II.

Risk Triad :- → Threats → Assets → Vulnerability.

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

* Risk → Risk arises when an attact seeks to access assets by exploiting an existing vulnerability.

To manage risk, organisation primarily focus on vulnerability because they cannot eliminate threats that appear in various forms and sources to its assets.

Risk Assesment is the first step in determining the extent of potential threats and risks in an IT infrastructure. The process assess risk and helps to identify appropriate control to mitigate or eliminate risks.

① Assets :-

Information is one of the most important asset for any organisation. Other assets includes hardware, software and other infrastructure component required to access the information. To protect these assets, organisation must develop a set of parameters to ensure the availability of the resources to authorized users and trusted network.

Security method has 2 objective. First objective is to ensure that network is easily accessible to authorized user. Second objective is to make it difficult for potential attackers to access and compromise the system.

The effectiveness of a storage security methodology can be measured by two key criteria :-

(i) The cost of implementing the system should be fraction of value of protected data.

(ii) It should cost heavily to a potential attacker in terms of money, effort & time.

(2) Threats :-

Threats are potential attack that can be carried out on a IT infrastructure. Attack is Classified as :-

(a) Active attack :- Active attack includes data modification, denial of service (DoS), and repudiation attack. They pose threat to data integrity, availability and accountability.

(b) Passive attack :- Passive attack are attempt to gain unauthorized access into the system. They pose threat to confidentiality of information.

→ In data ~~modulation~~ modification attack, the unauthorized ~~attack~~ user attempt to modify information for malacious purposes. A modification attack can target the data at rest or data at transit. These attack pose threat to data integrity.

→ Denial of Service (DoS) attack prevent legitimate users from accessing resources and services. These attack generally do not involve access to or modification of information. They pose threat to data availability.

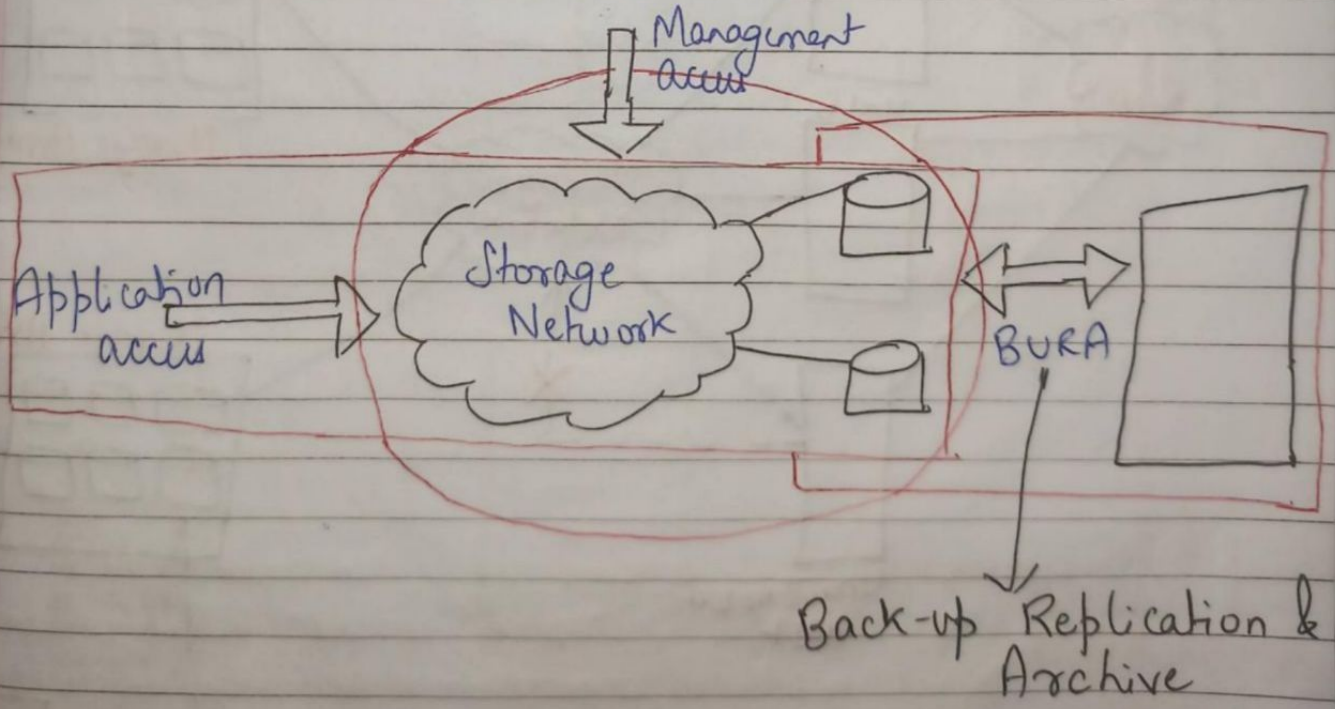
→ Repudiation is an attack against the accountability of information. It attempt to provide false information by either impersonating someone or denying that an event or a transaction has taken place.

③ Vulnerability :-

The paths that provide access to information are often vulnerable to potential attack. Each of the path may contain various access points which provide different level of access to storage resource.

It is important to implement adequate security controls at all the access points on an access path. Implementing security controls at each access points of every access path is known as defense in depth.

Topic III: Storage Security Domain :-

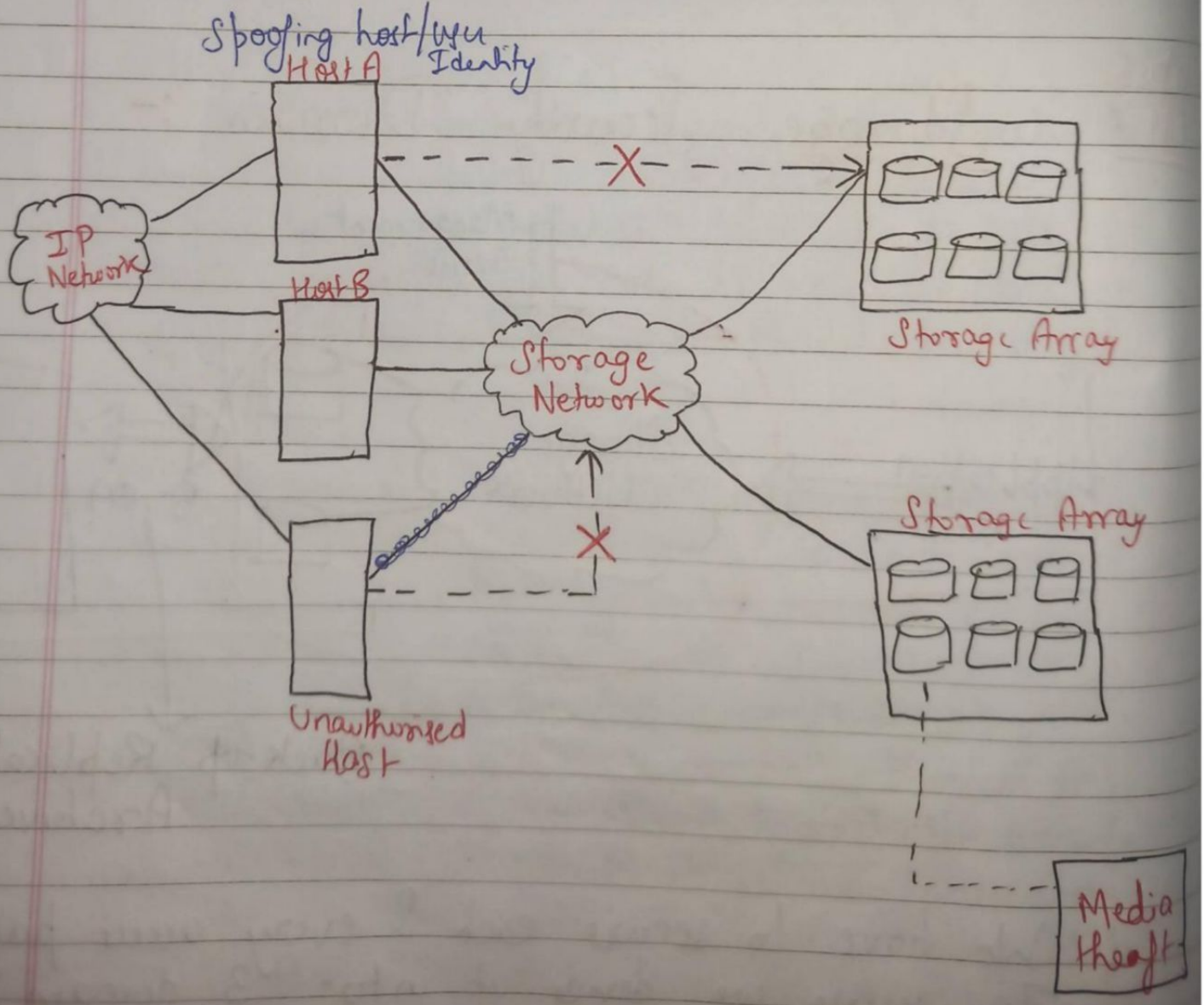


We have to secure each & every access path. To secure we devide it into 3 domain :-

(i) Application Domain
(ii) Management Domain
(iii) BURA

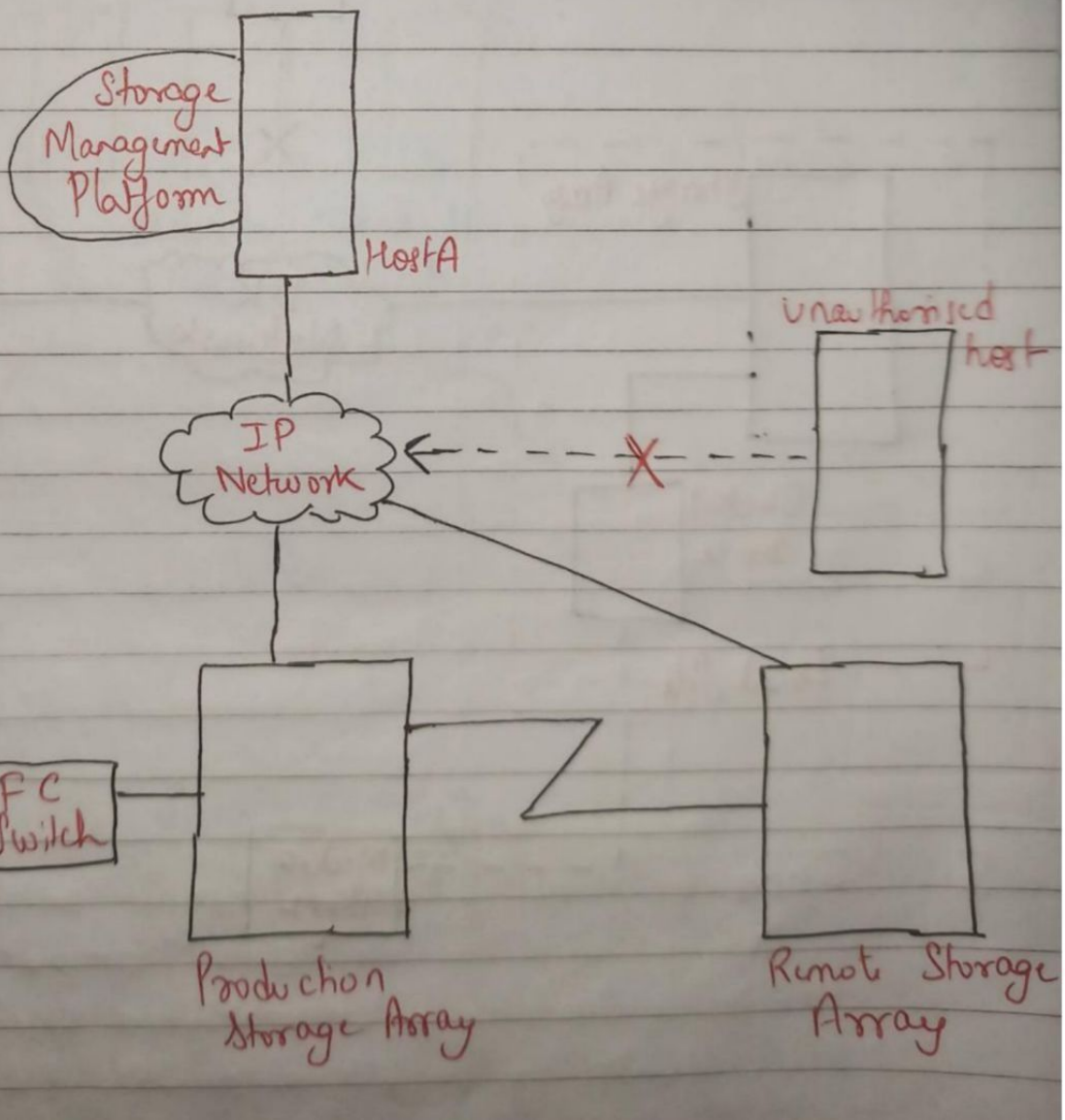
(i) Securing the Application Access Domain :-

The application access domain may include only those application that access the data through the file system or a database interface.



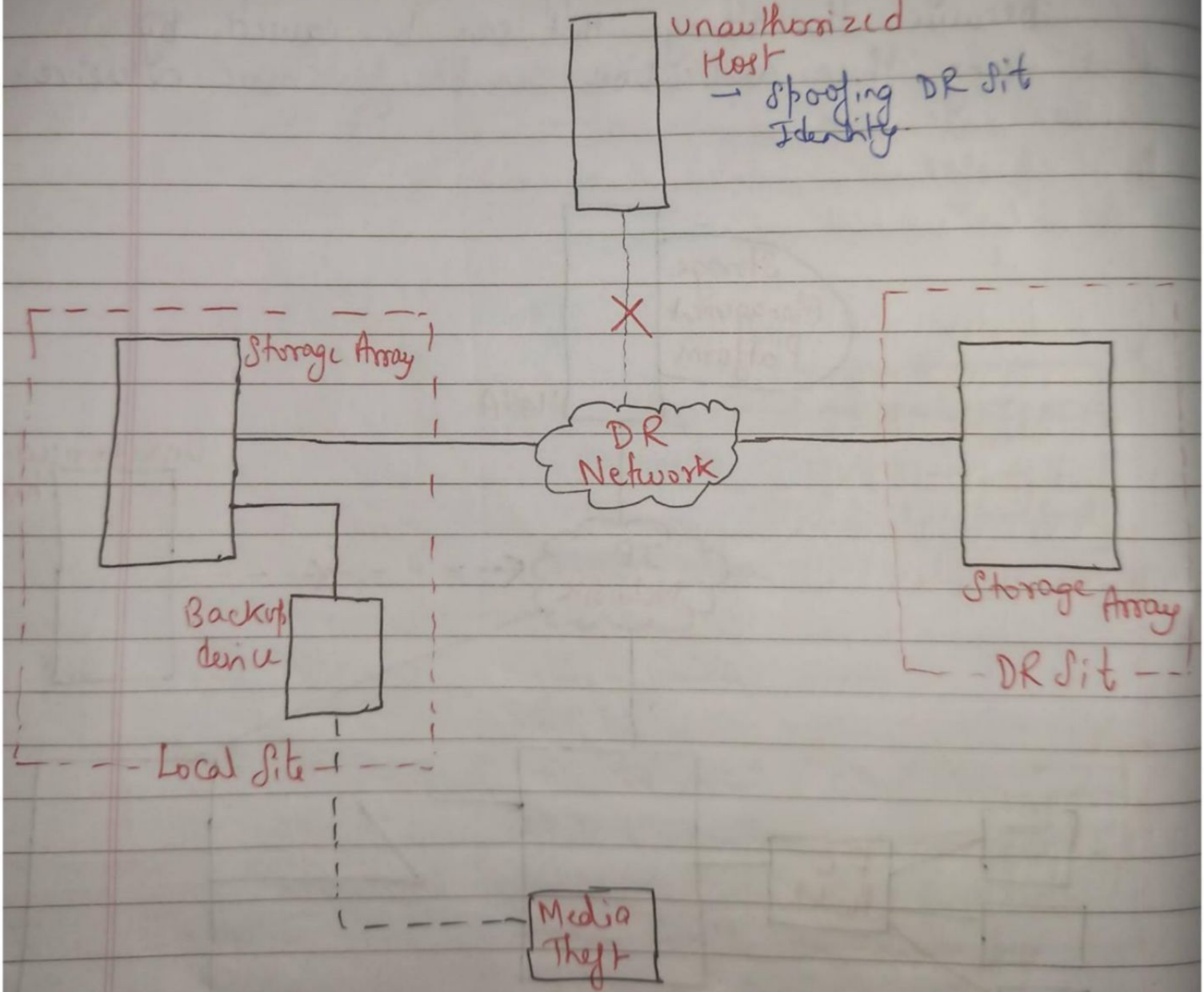
(ii) Securing the Management Access Data :-

Management access whether monitoring, provisioning, or managing storage resource, is associated with every device within the storage network. Implementing appropriate controls for securing storage management application is important because the damage that can be caused by using these application can be far more extensive.

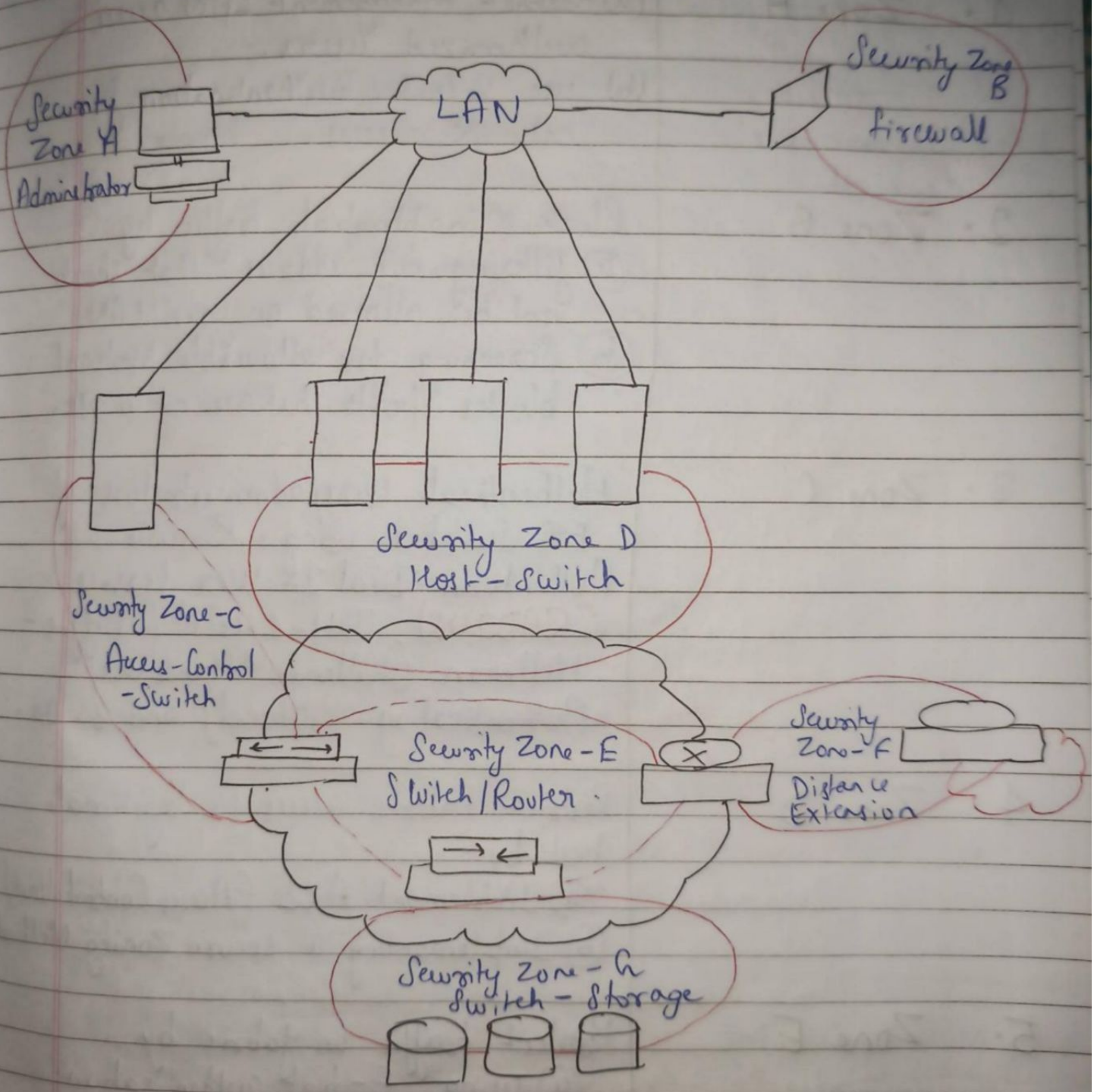


(iii) Securing Backup, Replication & Archive (BURA) :-

Backup, Replication and Archive is the third domain that needs to be secured against an attack.



Topic IV. Security Implementations in Storage Network :-



↳ SAN Security Architecture.

S.No.	Security Zones	Protection Strategies
1.	Zone A	(a) Restrict management LAN access to authorized users. (b) use-2-factor authentication for network access.
2.	Zone B	Block of inappropiate traffic by (a) filtering out address that should not be allowed on your LAN. (b) Screening for allowable protocol blocks ports that are not in use.
3.	Zone C	Authenticate users/administrators of FC Switches using Remote Authentican Dial In User Service (RADIUS), DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol) and so on.
4.	Zone D	Restrict Fabric access to legitimate host by (a) Implement ACL (Access Control Unit) (b) Implementing a secure Zoning Method
5.	Zone E	Protect traffic on fabric by (a) using E-port authentication (b) encrypting the traffic in transit (c) implementing FC switch control and port Controls

6. Zone F	Implementing encryption for in-flight data (a) FC-SP for long distance FC extension (b) IPSec for SAN extension via FCIP.
7. Zone G	Protect the Storage Array on your SAN via (a) WWPN-based LUN masking (b) SPI locking

Topic

Monitoring the Storage Infrastructure :-

- Parameters Monitoring
  - Accessibility
  - Capacity
  - Performance
  - Security
- Component Monitoring
  - Host
  - Storage Network
  - Storage

* Monitoring helps to analyze the utilization and consumption of various storage infrastructure resources. This analysis facilitates capacity planning, forecasting, and optimal use of these resources

* Monitoring Parameters :- Storage infrastructure components should be monitored for accessibility, capacity, performance and security.

→ Accessibility refers to availability of a component to perform its desired operation during a specified time period. A component is said to be accessible when it is functioning without any fault at any given point in time.

Monitoring hardware and software component for accessibility involves checking their availability status by reviewing the alerts generated by the system.

→ Capacity :- Capacity refers to the amount of storage infrastructure resource available. Example of capacity monitoring includes examing the free space available on a file system or a RAID group, or the number of ports available on a switch.

Inadequate storage capacity leads to degraded performance or effect accessibility. Capacity monitoring ensures uninterrupted data availability and scalability.

→ Performance :- Performance monitoring evaluates how efficiently different storage infrastructure component are performing and helps to identify bottlenecks.

Performance monitoring usually measures and analyze behaviour in terms of response time or ability to perform at certain predefined level.

→ Security :- Monitoring a storage infrastructure for security helps to track and prevent unauthorised access and login failures, whether accidental or malicious.

Security monitoring helps to track unauthorized configuration changes to storage infrastructure resource.

* Components Monitored :-

Host, network, and storage are components within the storage environment that should be monitored for accessibility, capacity, performance and security.

Host :-

The accessibility of a host depends on the availability status of hardware components and software process running on it. For example, a host's NIC failure might cause inaccessibility of host to its user.

File system utilization of host also needs to be monitored. Monitoring helps estimate the file system's growth rate and predict when it will reach 100%.

Accordingly, the administrator can extend the file system space proactively to prevent application outtage.

Server performance mainly depend on Input/Output profile, utilization of CPU and memory. For example, if a server running an application is experiencing 80% of CPU utilization continously. it indicate that server may be running out of processing power which can lead to degraded performance and slower response time.

Administrator can take several action to correct the problem such as upgrading or adding more processor and shifting the workload to different servers.

Security monitoring on server involves tracking of login failures and execution of ~~out~~ unauthorized application or software process.

Storage Network :-

Storage Network need to be monitored to ensure uninterrupted communication between the server and the storage array. Uninterrupted access to data over the Storage network depend on the accessibility of the physical and logical component of the storage network.

The physical component of storage ~~comp~~ network includes switches, ports and cables. Logical component includes constructs such as zones. Any failure in physical & logical component may cause data unavailability.

Capacity monitoring in storage network involves monitoring the availability of ports in the switch, the no. of available port in entire fabric, individual ports and each interconnect device in fabric.

Monitoring the performance of storage network enables assessing individual component performance and helps to identify network bottleneck. For example, heavily used ports can cause queing delays on the server.

Security in Storage Network provides information for any unauthorized change to the configuration of a fabric. Login failures, and unauthorized access to switches for performing administrative changes should be logged and monitored continously.

Storage :-

The accessibility of the storage array should be monitored for its hardware components and its various process. For example, failure of a replication task affect disaster recovery capability.

Capacity monitoring of a storage array enables the administrator to respond to storage needs as they occur.

A storage array can be monitored using a number of performance metrics such as utilization rate of various storage array components, I/O response time, and cache utilization.

Monitoring security helps to track unauthorized configuration of the storage array and ensures that only authorized users are allowed to access it.

Topic VI.

Storage Infrastructure Management Activities

The key storage infrastructure management activities performed in a data center can be broadly classified as :-

(i) Availability Management
(ii) Capacity Management
(iii) Performance Management
(iv) Security Management
(v) Reporting.

(i) Availability Management :- A critical task in availability management is establishing a proper guidelines based on defined service levels to ensure availability.

Availability management involves all availability related issue for component or service to ensure that service levels are met.
A key activity in activity management is to provision redundancy at all levels, including component, data, or even site.

(ii) Capacity Management :-

→ Goal :- ensure adequate availability of resources based on their service level requirements.
→ involves optimization of capacity based on cost & future needs.
→ provide capacity analysis that compare allocated space to forecast space.
→ provide trend analysis based on rate of consumption.

(iii) Performance Management :- Ensures the optimal operational efficiency of all components. Performance analysis is an important activity that helps to identify the performance of storage infrastructure components.

(iv) Security Management :- Key objective is to ensure confidentiality, integrity and availability of information in both virtualized and non-virtualized environments. Prevent unauthorized access.

(v) Reporting :- involves keeping track and gathering information from various component and process.
This information is compiled to form a reports for trend analysis, capacity planning, chargeback, and performance.

Capacity planning reports contain current & historic information about utilization of storage, file system, database tablespace, ports, etc.

Chargeback reports contain information about allocation or utilization of storage infrastructure components.

Performance reports provide details about the performance of various storage infrastructure components.

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 ever 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 techniques to validate network user credentials.

→ Authorization :-

- defines user privileges in a network
- UNIX system 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 between 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.

14.6 Concepts in Practice: RSA and VMware Security Products

RSA, the security division of EMC, is the premier provider of security, risk, and compliance solutions, helping organizations to solve their most complex and sensitive security challenges.

VMware offers secure and robust virtualization solutions for virtualized and cloud environments. This section provides a brief introduction to RSA SecureID, RSA Identity and Access Management, RSA Data Protection Manager, and VMware vShield.

14.6.1 RSA SecureID

RSA SecurID two-factor authentication provides an added layer of security to ensure that only valid users have access to systems and data. RSA SecurID is based on something a user knows (a password or PIN) and something a user has (an authenticator device). It provides a much more reliable level of user authentication than reusable passwords. It generates a new one-time password code every 60 seconds, making it difficult for anyone other than the genuine user to input the correct token code at any given time. To access their resources, users combine their secret Personal Identification Number (PIN) with the token code that appears on their SecurID authenticator display at that given time. The result is a unique, one-time password to assure a user's identity.

14.6.2 RSA Identity and Access Management

The RSA Identity and Access Management product provides identity, security, and access-controls management for physical, virtual, and cloud-based environments through access management. It enables trusted identities to freely and securely interact with systems and access. The RSA Identity and Access Management family has two products: *RSA Access Manager* and *RSA Federated Identity Manager*. RSA Access Manager enables organizations to centrally manage authentication and authorization policies for a large number of users, online web portals, and application resources. Access Manager provides seamless user access with single sign-on (SSO) and preserves identity context for greater security. RSA Federated Identity Manager enables end users to collaborate with business partners, outsourced service providers, and supply-chain partners or across multiple offices or agencies all with a single identity and logon.

14.6.3 RSA Data Protection Manager

RSA Data Protection Manager enables deployment of encryption, tokenization, and enterprise key management simply and affordably. The RSA Data Protection Manager family is composed of two products: *Application Encryption and Tokenization* and *Enterprise Key Management*.

- Application Encryption and Tokenization with RSA Data Protection Manager helps to achieve compliance with regulations related to PII by quickly embedding the encryption and tokenization of sensitive data and helping to prevent data loss. It works at the point of creation, ensuring that the data stays encrypted as it is transmitted and stored.
- Enterprise key management is an easy-to-use management tool for encrypting keys at the database, file server, and storage layers. It is designed to simplify the deployment of encryption throughout the enterprise. It also helps to ensure that information is properly secured and fully accessible when needed at any point in its life cycle.

14.6.4 VMware vShield

The VMware vShield family includes three products: *vShield App*, *vShield Edge*, and *vShield Endpoint*.

VMware vShield App is a hypervisor-based application-aware firewall solution. It protects applications in a virtualized environment from network-based threats by providing visibility into network communications and enforcing granular policies with security groups. VMware vShield App observes network activity between virtual machines to define and refine firewall policies and secure business processes through detailed reporting of application traffic.

VMware vShield Edge provides comprehensive perimeter network security for a virtualized environment. It is deployed as a virtual appliance and serves as a network security gateway for all the hosts within the virtualized environment. It provides many services including firewall, VPN, and Dynamic Host Configuration Protocol (DHCP) services.

VMware vShield Endpoint consists of a hardened special security VM with a third party antivirus software. VMware vShield Endpoint streamlines and accelerates antivirus and antimalware deployment because antivirus engine and signature files are updated only within the special security VM. VMware vShield Endpoint improves VM performance by offloading file scanning and other tasks from VMs to the security VM. It prevents antivirus storms and bottlenecks associated with multiple simultaneous antivirus and antimalware scans and updates. It also satisfies audit requirements with detailed logging of antivirus and antimalware activities.

Summary

The continuing expansion of the storage network has exposed data center resources and storage infrastructures to new vulnerabilities. IP-based storage networking has exposed storage resources to traditional network vulnerabilities. Data aggregation has also increased the potential impact of a security breach. In addition to these security challenges, compliance regulations continue to expand and have become more complex. Data center managers are faced with addressing the threat of security breaches from both within and outside the organization.

Organizations are adopting virtualization and cloud as their new IT model. However, the key concern preventing faster adoption is security. The cloud has more vulnerabilities compared to a traditional or virtualized data center. This is because cloud resources are shared among multiple consumers. Also the consumers have limited control over the cloud resources. Cloud service providers and consumers are facing threat of security breaches in the cloud environment.

This chapter detailed a framework for storage security and provided mitigation methods that can be deployed against identified threats in a storage networking