Security Analysis and Improvisation in Storage Area Network

Vishwesh M S[1], Nikhil D K[2], Vikas S B[3]

[1,2,3]*Student, Department of Computer Science, JSS Academy of Technical Education, Karnataka, India*

Abstract- *In an era of digital world, individuals and organization look to private and public cloud services for storage and retrieval of data in a secure and timely manner. Consequently, the demand for organizations to collect and retrieve data remotely is growing exponentially. Current storage technologies like Direct attached storage are facing important potential data storage challenge. As a result, new technologies would need to be imported. SAN is a distributed storage technology that regroups data in many private nodes and stores it in a secured location. From the perspective of security, the implementation of physical security in all geographically far-flung locations is not sufficient to ensure complete security. As a result, the SAN security framework should be designed and developed. This paper examines the functioning of the various SAN protocols. It also looks at other storage technologies such as direct storage (DAS), network storage (NAS) including various indicators such as: Storage capacity metrics, Throughput and read/write storage metrics, IOPS and latency storage metrics, MTBF and TBW, Form factors and connectivity. This paper concentrates on the security vulnerabilities in Storage Area Network, listing the different attacks in the Storage Area Network protocols and comparing them to other technologies mentioned above. Another aspect of this work involves highlighting performance factors in the Storage Area Network that will help in improving performance-based security solutions.*

Key Words: Storage Area Network, Direct Attached Storage, input/output operations per second. Network Attached Storage.

1.INTRODUCTION

SAN is a high-speed computer network that gives block-level access to data container. Storage area network generally consists of storage elements, switches, hosts, storage devices that are connected with each other using different technologies, protocols and topologies. Storage Area Network are mainly used to improve the accessibility of storage devices. Storage Area Network features container devices to a host so the data container appears to be attached locally. This simplified layout of host data storage is achieved by using different types of virtualizations.

Storage Area Network is often used for Improving the efficiency of applications (e.g., off-load data container functions, separating networks), Improving the availability of applications (e.g., multiple data paths), SANs also generally play an huge role in an industry BCM activities, improve storage efficiency and utilization (for example, consolidate storage resources, provide tiered storage, etc.) and improve data protection and security. SANs are typically based on Fiber Channel methods, which uses a variant of the Fiber CP for open systems and proprietary for mainframes.

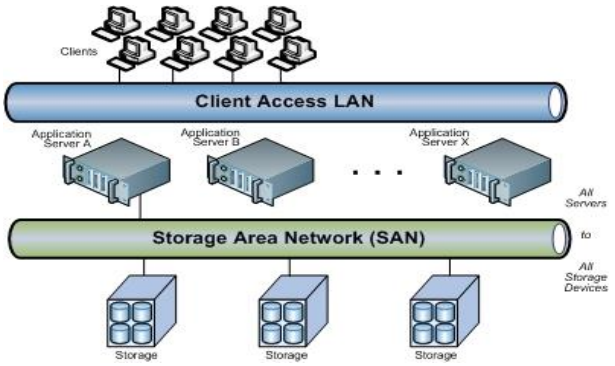

Fig-1: SAN and LAN

Because a Storage area network is a dedicated network of storage devices, typically accessed by other devices over a local area network, it avoids interference with LAN traffic in data transmission. Storage Area Network can be defined as a special speed network that provides a communication networks between servers and storage devices. The Storage Area Network has changed the storage structure that was a special connection between the networks and the data container devices, and the server efficiently controls and manages the storage device. Introducing a flexible network that allows one server or multiple servers to share a common storage utility.

There are several protocols for producing the SAN, the most common are:

- iSCSI
- Fibre Channel Protocol

1.1 Internet Small Computer System Interface

The transportation of Small Computer System Interface packets in the internet Small Computer System Interface is done over IP or TCP. The iSCSI is made up of several components such as:

1.The SCSI request is sent to sent to the target storage by the iSCSI Initiator, which acts as the host in this process.

2.The iSCSI is one of the cheapest and easiest option available for the connectivity, the only requirement for this process is the software initiator. The iSCSI also looks over the process of encapsulation and decapsulation.

3.The burden placed on the host CPU is reduced by TCP offload engine NIC. The TOE card receives the iSCSI information from the host and then the target receives the data from TOE card using IP or TCP.

4.The iSCSI Host Bus Adapter is the hardware component of iSCSI which has the capability of providing the performance gain to the process as it offloads the whole iSCSI and TCP/IP processing from the host processor

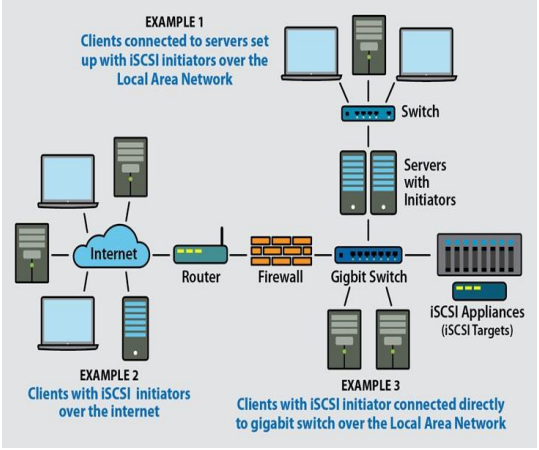

Fig -2: iSCSI

1.2 Fibre Channel protocol (FC)

Fibre Channel is a network technology used mainly in storage area networks, for loss-free transfer, high-speed of raw block data between server devices and computer data storage. Fibre Channel networks connect to dedicated high-speed, low-latency storage networks that support bandwidth rates of 2, 4, 6, 8, and 16 Gbps.

Input/Output protocol and network, like SCS are attached with the FC, embedded and carried within the FC Channel networks. The architecture of the FC is built in such a way that for the fundamentals for FC SAN framework. In FC machinery in the first instance it develops to connect the request for greater speeds of data moving between servers and cloud storage networks; it provides data moving at 32Gbps or even much more data. FC overcome some limitations like input/output speed, distance limitations and flexibility. In SAN all users have access to SAN like local disks to system. The compatible of a large range of devices that hold up FC is because of the different types of FC are in charge. FC uses the serial transfer technique instead of parallel one to overcome the speed and distance limitation.

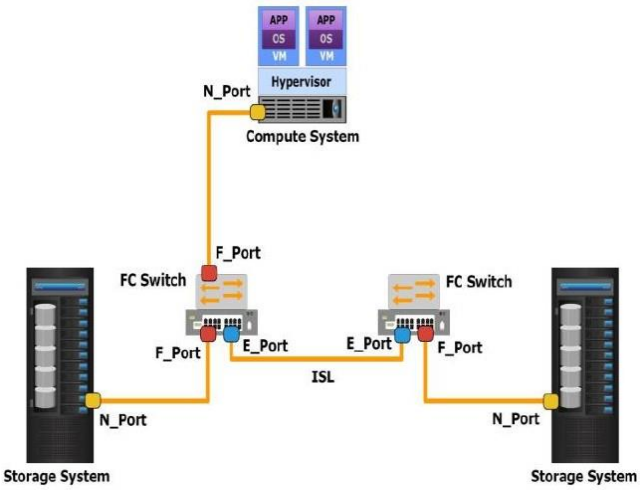

Fig -3: Fibre Channel Protocol

2. STORAGE AREA SECURITY

A **Storage Area Network** (SAN) operates on FC or Ethernet (Gigabit), a switched system with point-to-point architecture that is more of impractical to hijack or snoop packets except you have physical access to the system or access to the switches; therefore, we required to secure the storage area network. Key for this case is the Configuration; this is the prime part of building a firm SAN. We call to test and check the system configuration with the network analysis device to discover security holes and weak points and overcome with the proper methods and better configurations. The administrators of SAN should make use of the security configuration for IP SAN in which it enables the mutual CHAP rather than single or one-way CHAP, use the encoded practice such as IPSec and iSCSI methodology if it possible. As for the zoning and masking, in the FC port, fabric and switch-wide access control, are the common technique used. As we raised before the most recent attacks that is when you the direct access to the system. Insiders are the reason for most of the attacks, as in IT they have the direct contact to the system/network. The initial step to avoid the attacks is that to improve the security in networks with the insiders, we should give limited access to the people who works within this management. By the using the different levels of access to network system we can avoid the internal attacks. This also helps us to review the persons that made access to the networks and what are the changes made by them. Also, by isolating the physical item (SAN, servers and networks) and uses access authentication cards or biometrics like finger scanning while entering the network.

2.1 Storage Area Network Attacks

FC (fibre Channel) transmission is text-clear, that allows the good security menacing to be real. In fact, there is no any encoded-on level called frame that is a bad thing, by taking the performance into consideration the network will have all frames was encoded.

Text-Clear will please the all the performance and cover enormous issues, but it is also visible to unknown entities with the valuable information, that includes the sensitive information. The kind for information that non authorized uses or hackers try to obtain from the SAN are mentioned:

- FC name
- 32-bit IP-address
- WWN
- Information about Routing
- Layer-3 information i.e., frame
- Sequence Ids
- Sequence control number
- Domain name
- Management information

Hack on SAN means an unauthorized access to gain the sensible information and data that is stored in SAN. Some common types of attacks on SAN FC:

- Zone attacks
- LUN attacks
- MITM
- Server name attacks
- Session hijack

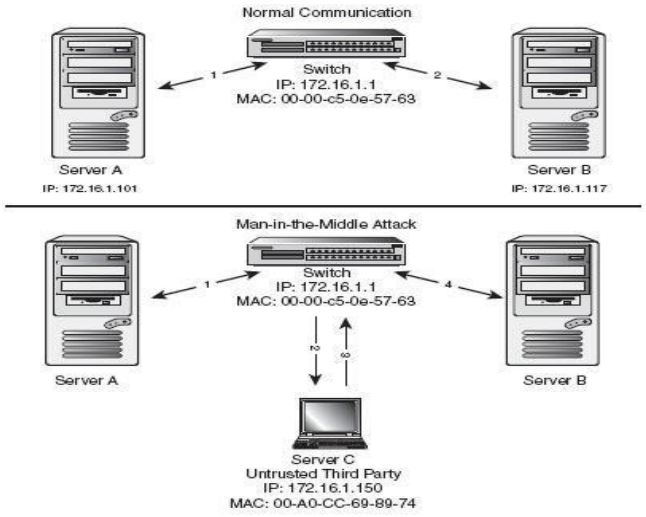

Fig -4: Man in the Middle Attack

2.2 Security Solution for FC SAN

Data in SAN is grouped into two parts:

- Data in flight: data is encoded at the transmission period from the original area to its destination
- Data in rest: data protection on stored medium, tapes or disks is done by encryption of available data.

Security of data contains the data integrity and data confidentiality, when we talk about both data at rest or data in flight. Data confidentiality was to make sure that data is not visible or give access to the unauthorized users. Data integrity gives guarantee that the available is not altered, destroyed or lost in an unauthorized hand. In FC uses a good method such as Switch Link Authentication protocol, which gives a secured establishment between 2 channels. For end-to-end it uses a next level generation in implementing the Switch Link Authentication protocol is developed and called as Fibre Channel Authentication protocol, is a Public Key Infrastructure (PKI) which is based on the mechanism called cryptographic authentication which provides the establishment for same region in the various entities in the SAN.

- FC Zoning
- LUN (Logical Unit Number) masking
- Binding Ports
- VSAN

2.3 iSCSI SAN attacks

iSCSI protocol is used to establish the connections by the IP SAN. The connection between storage and host can be managed by the iSCSI protocol. An IP packet contains data and SCSI commands which are encapsulated and transported using the TCP/IP. Because it is very inexpensive and simple to build, iSCSI is extensively used to link servers to storage, especially in circumstances where an FC SAN is not available. Some of the security risks that are possessed on IP SAN are:

- iSNS Domain Hopping
- ARP Poisoning attack
- Brute Force Attack
- Man-in-the-middle Attack

2.4 iSCSI SAN security solutions

Protecting the IP SAN can done in several different ways, in which the Encryption will be provided by the SSL and IPSec. Next the IQNs will provide the authorization. At last CHAP will secure the authentication, by addressing the username and the password. A connection will be established from initiators to LUN on targets

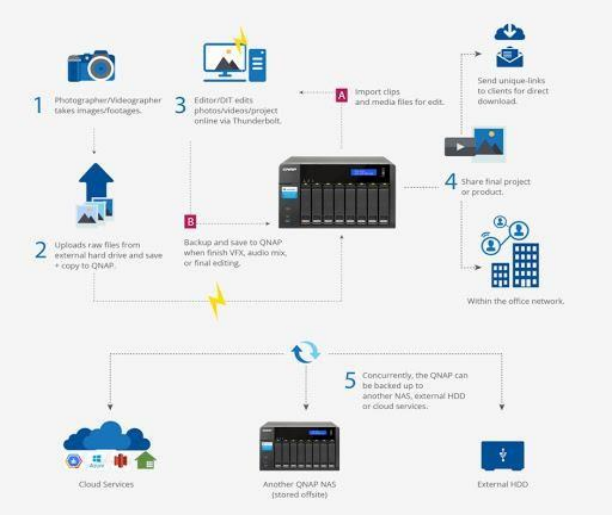

Fig -5: iSCSI Attack

3. SAN SECURITY EVALUATION

3.1 Configuration Setup

In the proposed paper we have used the IBM with the unique specification, like CPU: Intel with 1.86GHz to 2.3GHz RAM: 32GB HARD DISK: 2TB. There are some pre-installed workstations like one ESXi 6.0 user interface which is also later installed on disks. The connection between V Mare client and ESXi server is done via Management IP address, the ESX will be managed by V Mare. The server will then be installed in the V Machine on the EXSi. To promote we do have to follow some steps: Virtual Machine should be created with some specs, windows should we installed on R2 server. Join server to domain. NAS is an OS (operating system) which is installed on the virtual machine by any platform to interchange the data available in the computer. Free NAS is a best way to group up centralized and it is a easy way to access the data. Free NAS is also install in VM, the supported operating systems are Windows, OS x and Unix, also in various virtual hots like V Mare and Xen servers with the AFP, iSCSI, NFS protocols. Free NAS is used as NAS with support of the following file protocols NFS and CIFS by support block access protocols as in workstation. This workstation will attack the IP SAN, following software to be installed: step 1- Wireshark step 2- Cain step 3- Nmap

3.2 Least secure, First configuration

Target that is connected to the portal 10.0.0.24 and with the ID 4 to VMware 1 and VMware that says any initiator host that can connect to this LUN and can change the data in it.

3.3 More secure, Second configuration

To prevent this, initially we need to login to IP SAN which is free NAS that comes under the iSCSI initiators. Then a new set of initiators is created and by selected the Host(s) that gives access to visible LUNs and those networks. The one thing we need to know that IQN is of the file server, this is done by APN poisoning between the files and SAN IP.

4. CONCLUSION

When the collected data is increasing, people in business will try to manage huge amount the data on the LANs. It has two sides, SAN tech the initial side which is a positive side and helps in reducing the cost and good availability, the second side that will be the grey location in that is safe. We have to be assured that information which moves in San is secure and safe. As we know about the architecture in which the purpose is to give space to interchange the information with the system, also the component in the SAN is based Optic and Gigabyte, based on the type of architecture used. Components like Hubs directors and switches are also included. Cluster system is used in the SAN to ensure the secure access to the information by the various nodes. Security type and functionality is compared in order to use protocols like iSCSI and channels like Fibre. Performance and security play's huge role in this system, where we come to know the attacks and its types in SAN, one like poisoning (ARP), MITM, hijacking, address hacking, server error, domain hop, spoofing of data(information). This problem has to overcome by advancing the security without effecting the system performance. To the greater performance and security SAN should be combined with authorization, encoded and authentication which great difficulty in attacking. Where as in FC SAN uses LUN masking, VSANs as IP SAN mutual Chap, the data collection area is secured as weakest link. So, we need to include the address, much prevent from the serious threat to SAN system that is insiders, people like who got access to system information and data storage area. Latest OS and firm ware are used in the SAN devices to get better performance in iSCSI. We can improve the system performance by offload some commands from the system or CPU also by using switches in iSCSI will enhance the security and performance in SAN, by frequent change in the hosts, switches may also help in improving the performance in the system. The proposed system is implemented the SAN system to get know about the technology and type problem that we face while developing the model. SAN include IT's to perform the tasks with less information, as a result it minimizes the cost where it saves the revenue of the company.

REFERENCES

[1] Patents.google.com. (2018). US7194538B1 - Storage area network (SAN) management system for discovering SAN components using a SAN management server - Google Patents. [online] Available at: https://patents.google.com/patent/US7194538B1/en

[2] Patents.google.com. (2018). US7599360B2 - Methods and apparatus for encapsulating a frame for transmission in a storage area network – Google Patents. [online] Available at: https://patents.google.com/patent/US7599360B2/.

[3] Snia.org. (2018). SNIA — Advancing Storage and Information Technology. [online] Available at: https://www.snia.org/

[4] Bing.com. (2018). [online] Available at: https://www.emc.com/collateral/hardware/white-papers/h4173- approaches-encryption-data-at-rest-enterprise-wp.pdf

[5] Redbooks, I. and Networking, S. (2018). IBM Redbooks - Introduction to Storage Area Networks. [online] Redbooks.ibm.com. Available at: http://www.redbooks.ibm.com/abstracts/sg245470.html

[6] Education.emc.com. (2018). Information Storage and Management V3-EMC Education. [online] Available at: https://education.emc.com/guest/campaign/InformationStoragea ndManagement.aspx

[7] Chukry, Souheil & Sbeyti, Hassan. (2019). Security Enhancement in Storage Area Network. 1-5. 10.1109/ISDFS.2019.8757492.