Bangalore Institute Of Technology

Department of Information Science & Engineering

Storage Area Network Assignment

Security Enhancement in Storage Area Network

Guide:
Mrs. Shilpa M
Asst. Prof. ISE

By:
R.Vaibhav -1BI16IS063
Prajwal B.R. -1BI16IS036
Raushan Sah -1BI16IS043
Md Asif Ali-1BI16IS030

Abstract:

Living in the age of digital transformation, companies and individuals are moving to public and private clouds to store and retrieve information, hence the need to store and retrieve data is exponentially increasing. Existing storage technologies such as DAS are facing a big challenge to deal with these huge amount of data. Hence, newer technologies should be adopted. Storage Area Network (SAN) is a distributed storage technology that aggregates data from several private nodes into a centralized secure place. Looking at SAN from a security perspective, clearly physical security over multiple geographical remote locations is not adequate to ensure a full security solution. A SAN security framework needs to be developed and designed. This work investigates how SAN protocols work (FC, ISCSI, FCOE). It also investigates about other storages technologies such as Network Attached Storage (NAS) and Direct Attached Storage (DAS) including different metrics such as: IOPS (input output per second), Throughput, Bandwidths, latency, cashing technologies. This research work is focusing on the security vulnerabilities in SAN listing different attacks in SAN protocols and compare it to other such as NAS and DAS. Another aspect of this work is to highlight performance factors in SAN in order to find a way to improve the performance focusing security solutions aimed to enhance the security level in SAN.

Index Terms—SAN, Information Security, Storage Technologies, SAN Performance factors

INTRODUCTION:

A storage area network (SAN) or storage network is a Computer network which provides access to consolidated, block level data storage. SANs are primarily used to enhance accessibility of storage devices, such as disk arrays and tape libraries, to servers so that the devices appear to the operating system as locally attached devices. A SAN typically is a dedicated network of storage devices not accessible through the local area network (LAN) by other devices, thereby preventing interference of LAN traffic in data transfer. We can define a SAN as a specialized, high-speed network that provides transport channel between servers and storage devices. Sometime we refer to it as the network located behind the servers. It allows any-to-any connection across the network, it uses interconnected elements such as switches and directors (a Fiber Channel (FC) director is a modular, chassis-based networking device that provides connectivity between host servers, switches and storage systems in a dedicated FC SAN).

SAN changed the way that there is a dedicated connection between a server and storage, and that the server effectively manages and controls the storage devices. Moreover, SAN roles eliminates any restriction to the amount of data that a server can have access to, currently, the number limited by the number of storage devices that are attached to the individual server. Instead, it introduces a flexible network that enables one server or many heterogeneous servers to share a common storage utility. The network can have many storage devices such as disks, tapes, and optical storage. Moreover, the storage utility might be located at a far distant location from the servers that it uses.

There are several protocols for implementation of SAN, the most common are:

- internet Small Computer Interface (iSCSI)
- Fiber Channel (FC)

RELATED WORK:

Prior FC SAN implementation shows that communication between devices was any to any, there was no management and access control mechanism to protect storage that was used by one host from being accessed by another. Current ISCSI SAN implementations dont take into consideration authentication, authorization and encryption. Storage area network (SAN) management system for discovering SAN components using a SAN management server [1] embodiments of a LUN security utility which provides LUN security operations including, but not limited to, searching for and locating one or more LUNs, LUN selection, LUN to disk array port binding, LUN masking and fabric zoning operations in one utility. Embodiments may provide a central user interface that guides a user through configuring LUN security operations and allows the user to execute the configured LUN security operations with a single operation. Embodiments may provide a central point from which to perform LUN security operations including one or more of, but not limited to, LUN binding, LUN masking and fabric zoning.

In this research we present a detailed description and elaboration for best security practices, mitigation techniques for SAN technology will be explored. Regarding FC SAN technology, zoning was invented to address this security risk, by providing an access control mechanism which allowed only the members of the same zone to communicate within that zone; all other attempts from outside are rejected, categorized into three types: port zoning, WWN zoning, mixed zoning. Speaking of the ISCSI SAN technology, authentication is secured and satisfied when using Challenge Handshake Authentication Protocol (CHAP), authorization is obtained by adapting IQNs, in addition encryption is provided by IPSec or SSL.

STORAGE AREA SECURITY ISSUES:

A SAN uses Gigabit Ethernet or FC, a switched network with point-to-point architecture that makes it nearly impossible to snoop or hijack packets unless you have physical access to the network or to administrative access to the switches. This is more or less true, therefore we need to secure the SAN as much as possible. Configuration is key in this case, it is the most important part of building a secure SAN. We need to test and check the network configuration with network analysis tools to find security holes and weaknesses and apply proper policies and security configuration. SAN administrators should apply security configurations for the IP SAN such as enabling and using mutual CHAP instead of one-way CHAP, use encryption methods like IPSec for iSNS server and iSCSI devices wherever it is possible. As for FC SAN, LUN masking and zoning, security in FC switch port, switch-wide and fabric-wide access control, and logical partitioning of a fabric (Virtual SAN) are the most commonly used SAN security methods. As mentioned in the saying before most of the attacks are when you have physical access to the network. Most of the attacks on SAN are from insiders, as in employees or IT personal, who have access to the SAN Management console and storage devices.

The first step to improve SAN security is to begin with the insiders, we need to control, limit the responsibilities and access of the personal who works with these Management devices. We have to use different accounts for each person and have different level of access to the management console and devices. This will also help to review the logs and audit who logged in and what changes were made. We need to isolate the physical devices (SAN, switches and servers) if possible and use access cards and finger print at the entrance.Most Outside attackers targets the management consoles since they all work over TCP/IP, they try to gain access so they can access the SAN data.

SAN SECURITY EVALUATION:

In this chapter we are going to provide simulation of the iSCSI connection between Servers and IP SAN that uses iSCSI protocol, to check security risks and to evaluate different security measures (practices) in order to identify the best practice.

A. Configuration Setup- In this experiment we used an IBM Workstation with the below specs: CPU:Intel Xeon 1.87 GHz E5502 RAM:16 GB DISK:1 x 140 GB 1 x 2 TB NIC:1 x 1 GB. The environment consists of one ESXi 6.0 U1 host installed on IBM Workstation. The ESXi itself will be installed on the local disks. We will manage the ESX using VMware vSphere client and connect to the ESXi server via the Management IP address. Domain Controller Server. The active directory domain is: name.co and it will be installed on a virtual machine on the ESXi server. This file server will be installed on a virtual machine on the ESXi server. We will do the following to promote it: - Create the virtual machine. - Install windows 2012 R2 server. - Name the server. Configure the IP addresses and here configures the domain controller as primary DNS server. - Join this server to the domain.

FreeNas FreeNAS is an operating system that can be installed on virtually any hardware platform to share computer data storage over a computer network. Free as in free and open source and NAS as in network-attached storage, FreeNAS is the simplest way to create a centralized and easily-accessible home for your data. FreeNAS can also be installed on a virtual VM, it supports Windows, OS X and Unix clients and various virtualization hosts such as XenServer and VMware using the CIFS, AFP, NFS, iSCSI, SSH, rsync and FTP/TFTP protocols. FreeNAS can be configured to be used as NAS by supporting the following file level protocols CIFS and NFS or as SAN by supporting block level access protocols as iSCSI. Workstation This workstation is used to do the attacks on the IP SAN, it has the following software installed: 1- Wireshark 2- Cain and Able 3- Nmap

B. First config, least secure- Since the Target connects the Portal 10.0.0.23 and the initiator group ID 3 to the extents VMware and VMware1, which mean any Host initiator can connect to those LUNs, view and edit the data.

C. Second config, more secure- To avoid this from happening, login to the IP SAN (FreeNAS) under block (iSCSI) initiators. Create a new initiator and select the Host(s) IQN that have access to this LUNs and which network. This is good but still we can get around it easily. All we need to know is the IQN of the file server, this can be done by doing an ARP poisoning between the file and IP SAN, and from that we can detect the file server IQN and use that to connect to the LUN.

iSCSI traffic is clear text. On a windows 7 that is connected to the iSCSI switches, run ARP poisoning between 10.0.0.23 IP SAN and the File server 10.0.0.19. Then run wireshark and check the traffic as we can see in the picture below the source and destination of the traffic is between the file server and the IP SAN, filter by iSCSI word and look for Login command, you can see the file server IQN: iqn.1991-05.com.microsoft:file.name.co And the IP SAN iqn for this target: iqn.2005-10.org.freenas.ctl:freenasfile1 This also shows that there is not any authentication method.

D. Third config, most secure To solve the issue, we had before we need to enable mutual chap on the IP SAN and on the Servers. Under the Portal tab select the portal group required and for discovery authentication select mutual chap, and select the authentication group. On the windows 7 start the ARP poisoning and run Wireshark, we will be able to get the IQN information and we will notice that the authentication is enabled. To decrypt the mutual chap we will need the ID and the message challenge and the hash, this is a lot harder than it was at the beginning of CHAP authentication, nowadays it is harder to decrypt the password, since the ID (CHAPI) and Message Challenge (CHAPC) changes randomly and frequently as show in the pictures below.

CONCLUSION:

With the increased amount of data collected, businesses are relentlessly trying to manage the high volumes of data on overburdened LANs. As the Saying goes every coin has two sides, same goes for SAN technology, although the first side was positive and helped reduce cost and maintain high availability, there is another side that falls in a gray area where SAN has some security risks. Companies and clients needs to be assured that the data (information) that travels through the SAN is safe and secure. We discussed in this work about the architecture of SAN which is any high-performance network whose primary purpose is to enable storage devices to communicate with computer systems and with each other. Also, we talked about the networking component, a SAN can be based on Fiber Optic or Gigabit Ethernet, depending on the architecture and required speed and performance. A SAN component includes hubs, switches, directors and routers from a networking point of view. SAN also uses clustered file system to allow access to the same data by the different hosts or nodes. We compared the functionality and security feature of the most commonly used protocols by SAN, iSCSI and Fibre Channel. Security and performance was a big part of this work, in which we identified the attack types in SAN such as ARP poisoning, man in the middle, session hijacking, address weakness, name server pollution, iSNS domain hopping, sniffing and spoofing the data to which we discussed the solutions to improve security without having a big impact on performance.

To ensure the security of SAN we need to use the combination of authentication, authorization and encryption which will make it harder for attackers to use malicious code to take advantage of functionality errors or protocol faults within the storage networks. In FC we used LUN masking, zoning, port binding and VSANs, as for IP SAN we used mutual CHAP, Radius server, IPSec and others. A storage area network is only as secure as its weakest link. Therefore, every element of the SAN must be considered when addressing security needs, including the most dangerous threats to SAN which are insiders, people who work in the company and have access to the SAN devices and their management console. As for performance on iSCSI or FC, it is recommended to use the latest firmware and Operating systems available to the SAN devices, using NIC TOE (in IP SAN) will help offload operations from the CPU and increase performance when using encryption like IPSec, using dedicated switches for iSCSI traffic will help secure and increase the performance of the system, changing the MTU on the Hosts, switches and Storage will increase the performance of the system. We implemented the IP SAN model to get more familiar with this technology and what issues we might face during implementations. SAN technology allowed IT Managers to do more with less and as result, reduce administrative and equipment costs while adhering to high availability requirements for mission-critical application, which ultimately helps save the company money.

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/ [Accessed 2 Apr. 2018].

[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 [Accessed 2 Apr. 2018].

[6] Education.emc.com. (2018). Information Storage and Management V3 - EMC Education. [online] Available at: https://education.emc.com/guest/campaign/InformationStorageandManagement.aspx [Accessed 2 Apr. 2018].

THANK YOU