International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 471-484
Published Online January 2020 in IJEAST (http://www.ijeast.com)

SECURITY EVALUATION AND PERFORMANCE ASSESSMENT OF STORAGE AREA NETWORK (SAN) - A CASE STUDY OF NATIONAL ASSEMBLY (NASS), ABUJA - NIGERIA

OKPE PETER BEN
Department of Computer Science,
Faculty of Science, University of Abuja –Nigeria

MUHAMMAD SANUSI
Department of Computer Science,
Faculty of Science, University of Abuja –Nigeria

Abstract - This paper is on the Security Evaluation and Performance Assessment of Storage Area Network (SAN); a Case Study of National Assembly (NASS), Abuja. SAN is a conglomerate of Storage system designated at various Data Centers using servers and other storage devices in a distributed system on a Network; it is an enterprise storage network with distributed storage technology that manages the data from several nodes in centralized place and secure network with the aid of Fibre Channel and iSCSI. SAN architecture in general, such as: SAN components, topology, and terminologies present an idea about SAN; the potential security threats, attacks and solutions available in SAN environments in terms of: network, implementation, and management. In this research work, the performance of SAN at NASS and associated security challenges and threats are evaluated. Several Protocols are employed in the simulation, Wireshark has been used to monitor the performance of the SAN system as well as the user's view and experiences that are gathered through the use of questionnaires and verbal interviews. The analysis of the captured packets/frames on the Network is based on the following filtering: DNS, FTP, UDP, HTTP, HTTPS, ICMP, SCTP, SSL, STP, TCP streams, in their respective statistical analysis in terms of: Input/Output graphs, Flow chart graphs, TCP and UDP stream graphs, and others. Necessary preventive measures were tested and established from several stimulations and collected experiences from users to address the security and performance challenges on the Network.

Keywords: SAN, IP, NASS, Network Protocol, Security

I. INTRODUCTION

The paper is on Security Evaluation and Performance Assessment of Storage Area Network (SAN); A Case Study of National Assembly, Abuja. Storage Area Network (SAN) is a conglomerate of Storage system designated at various Data Centers using servers and other storage devices in a distributed system on a Network as an enterprise storage network that have dedicated high-speed network which allows the establishment of direct connection between storage devices and processors (servers) centralized to the extent supported by the distance of Fibre Channel. The term SAN designates a new type of storage architecture in which the storage systems are attached to a high speed network dedicated exclusively to storage. It involves a whole new network totally distinct from existing communication networks with SAN Architecture(1). The application servers (usually UNIX or Windows NT based) access the storage resource through the SAN. Most of the local storage resources are off–loaded from the applications servers, are managed separately from them, and are consolidated at the data centre, site, or enterprise level(1). Being a high speed network infrastructure and the whole storage architecture, including servers, storage subsystems and management software, Fibre Channel is currently the preferred technology for implementing SAN architecture. To simplify the migration and integration of legacy equipment; hence, SAN infrastructures should be based on Fibre Channel technology to support multiple protocols(2). For example, the infrastructure can convey SCSI protocols that are widely used in UNIX and Intel based servers; ESCON (Enterprise System Connection) for IBM mainframes; and IP to offer networking capability. However, the purpose of SAN is not to replace LANs, all these protocols can simultaneously use the same cables. This new storage architecture is very different from traditional architectures, where each storage system is connected to a single or sometimes to a limited group of servers. That is why they are sometimes called private storage architectures. A Storage Area Network is obviously a specialized, high-speed network that provides block-level network access to storage; it typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. They may also span multiple sites[3]. SANs according to [4] are often used to:

- improve application availability (e.g., multiple data paths),
- enhance application performance (e.g.: off-load storage functions, segregate networks, etc.),
- increase storage utilization and effectiveness (e.g., consolidate storage resources, provide tiered storage, etc.), and
- improve data protection and security.

1.1 Research Question

The paper aimed at answering the following research questions to guide the study:

1. What are the security vulnerabilities and possible attacks on SAN?
2. How would the security vulnerabilities and the possible attacks on SAN be curtained?
3. What are the improvement methods to be adopted in the implementation of NASS SAN for effective performance assessment?
4. What are the significance of security evaluation and performance assessment of NASS SAN to enterprises, institutions and the society at large?
5. What are the security and performance loop holes that affects SAN on NASS Network?

II. METHODOLOGY

This study adopted a sample size of 150 questionnaires administered to ICT staff in National Assembly, the outcomes were analyzed and tabulated using simple percentage and frequency mean/mean deviation. It is obvious however, malicious insider and external intruders are threat to networks; hence, necessitated the network to be exploit for vulnerabilities using Wireshark as a tool to curtain the menace. Wireshark was installed, configuration, implemented on a computer system connected to the National Assembly SAN as a vulnerability tool that methodologically evaluate security and assessed performance of NASS SAN through a switch or Hub accessing SAN on the Fibre Channel and iSCIS platform to capture data-packets/frames. The analysis of the captured packets/frames on the Network is based on the following filtering: DNS, FTP, UDP, HTTP, HTTPS, ICMP, SCTP, SSL, STP, TCP streams, in their respective statistical analysis in terms of: I/O graphs, Flow graphs, TCP and UDP stream graphs, etc.; hence, necessary preventive measures were tested and established from several stimulations and collected experiences from users to addressed the security and performance challenges on the Network.

The study revealed the methods used in Security Evaluation and Performance Assessment of NASS SAN earlier; hence, investigating and evaluating NASS SAN to find out security solutions, vulnerabilities and attacks or threat on NASS SAN protocols, compare between the functionality of these protocols and find out the performance elements of NASS SAN on SAN protocols to improve the performance assessment; and as well adopt a model of iSCSI based SAN that simulated measures to the performance and find out some of the security vulnerabilities and the solutions to make NASS SAN secure in all ramifications, by using the practical experiment of vulnerability test with the aid of Wireshark for deeper understanding of functionality and security risks on SAN, with the results depicted in this paper. The Wireshark Vulnerability Scanner was used for port scanning of devices on the network to identify software vulnerabilities. It detects and identifies software bugs, open patches and vulnerabilities on NASS SAN; this is possible with aid of an open source tool in them that determines security threats and vulnerability. The central client manages the entire network and controls all the serves at remote storage stations. The scanner find open ports, recognize the services running on those ports, and find vulnerabilities associated with these services with the aid of a vulnerability assessment to perform critical data and infrastructure check to safeguard them; thereby taking into consideration the flaw or weakness in a system's design, implementation, or management exploited which tend to violate the SAN system's security policy, such as: recognizing, measuring, and prioritizing vulnerabilities in a system.

III. ANALYSIS AND RESULTS

The analysis in this paper is based on the administered questionnaire and Wireshark simulations**.**

3.1 Administered Questionnaire Analysis

Research Question One: What are the security vulnerabilities and possible attacks on SAN?

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 471-484
Published Online January 2020 in IJEAST (http://www.ijeast.com)

Table 3.1: The Security Vulnerabilities and possible attacks on SAN. **(N = 150)**

S/N	Statement	SA	A	D	SD	Mean
1.	SNMP vulnerability recorded low performance of SAN and immensely affected its security on Network.	72	51	19	8	3.25
2.	Unauthorized access, bandwidth abuse session hijacking are the major reasons for low performance of SAN and its security on NASS Network	58	73	13	6	3.22
3.	Insider Threats posed a great setback to the entire NASS Network and consequently affecting SAN performance as well as discouragement to its security	81	60	9	0	3.48
4.	The performance of SAN and its Security is usually affected by Man-in-the Middle Attack and Name Server Pollution Attack respectively on NASS Network	15	48	62	25	2.35
5.	Address Weakness attack due misconfigured IP address/switches affects SAN security/performance	60	68	18	4	3.23
	Overall Mean					**3.12**

From table 3.1 above, the research question was to find the security vulnerabilities and possible attacks on SAN. The overall mean indicated a positive response. This is because it was in line with the decision rule which states 2.5 and above response as considered positive. This shows that the respondent affirmed from item 1, 2, 3, 4 and 5 attested for the security vulnerabilities and possible attacks on SAN.

Research Question Two: How would the security vulnerabilities and the possible attacks on SAN be curtained?

Table 3.2: Ways curtained the security vulnerabilities and the possible attacks on SAN be curtained (**N = 150)**

S/N	Statement	SA	A	D	SD	Mean
6.	Proper configuration of IP Addresses to avoid spanning-tree protocols and placement of the right ICT/Network personnel in the ICT unit would boost the performance and security of SAN tremendously.	83	62	3	2	3.51
7.	Motivation and incentive to the ICT personnel and Network Administration to encourages effective security and efficient utilization of SAN	80	65	4	1	3.49
8.	Proper supervision and monitoring of NASS Network to checkmate threats that are detrimental to SAN performance and Security.	82	67	1	0	3.54
	Overall Mean					**3.51**

From table 3.2 above, the research question was to find out how would the security vulnerabilities and the possible attacks on SAN be curtained. The overall mean indicated a positive response. This is because it was in line with the decision rule which states 2.5 and above response as considered positive. This shows that the respondent affirmed from item 6, 7and 8 reflects how the security vulnerabilities and the possible attacks on SAN can be curtained.

Research Question Three: What are the improvement methods to be adopted in the implementation of NASS SAN for effective performance assessment?

Table 3.3: The improvement methods to be adopted in the implementation of NASS SAN for effective performance assessment. (**N = 150)**

S/N	Statement	SA	A	D	SD	Mean
9.	Access Authentication should be implemented on SAN to prevent unauthorized access.	80	60	10	0	3.47
10.	Special IP should be configured with Host and Subnets for	84	58	7	1	3.50

	effective broadcast dedicated exclusively for SAN on the NASS Network.					
11.	National Assembly should establish policy that would guide against Insider Threats.	90	58	2	0	3.97
12.	SSID authentication should be properly configured for both LAN and Wireless Network Connection.	87	60	3	0	3.96
13.	Network Administrators, ICT Staff and alike should be periodically sent on training to update their skills and knowledge in order to meet up with the current advancement in ICT.	60	83	5	2	3.34
	Overall Mean					**3.65**

From table 3.3 above, the research question was to find out what are the improvement methods to be adopted in the implementation of NASS SAN for effective performance assessment. The overall mean indicated a positive response. This is because it was in line with the decision rule which states 2.5 and above response as considered positive. This shows that the respondent affirmed from item 9, 10, 11, 12 and 13 indicated the improvement methods to be adopted in the implementation of NASS SAN for effective performance assessment

Research Question Four: What are the significance of security evaluation and performance assessment of NASS SAN to enterprises, institutions and the society at large**?**

Table 3.4: **T**he significance of security evaluation and performance assessment of NASS SAN to enterprises, institutions and the society at large. **(N = 150)**

S/N	Statement	SA	A	D	SD	Mean
14.	Security evaluation and performance assessment of NASS SAN would to a greater extent exposed vulnerabilities on the network.	60	58	31	1	3.18
15.	Security evaluation and performance assessment of NASS SAN would ensure availability, confidentiality and integrity of data and information; and, offer insight into network communication to identify performance problem, locate security breaches, analyze application behaviours and performance capacity planning so as to: locate faulty network devices, measure high delays along a path and locate the point of packets lost.	74	65	11	0	3.42
	Overall Mean					**3.30**

From table 3.4 above, the research question was to find out what are the significance of security evaluation and performance assessment of NASS SAN to enterprises, institutions and the society at large. The overall mean indicated a positive response. This is because it was in line with the decision rule which states 2.5 and above response as considered positive. This shows that the respondent affirmed from item 14 and 15 indicated the significance of security evaluation and performance assessment of NASS SAN to enterprises, institutions and the society at large.

Research Question Five: What are the security and performance loop holes that affects SAN on NASS Network?

Table 3.5: The security and performance loop holes that affects SAN on NASS Network (**N= 150)**

S/N	Statement	SA	A	D	SD	Mean
16.	Lack of proper Adhoc and infrastructural network knowledge has been detrimental to SAN security and its performances on NASS Network	81	69	0	0	3.54
17.	NASS Management and Network Administrators' ignorance have tremendous effects on SAN performance in terms of storage utilization and security on NASS Network.	68	82	0	0	3.45
18.	The ICT Staff and Network Administrators' attitude toward SAN usage and security have a great effect on its performance on NASS Network.	52	78	13	7	3.25

19.	National Assembly policies sometimes impacted changes that affect system upgrades and SAN security positively on NASS Network.	62	82	5	1	3.36
20.	Ignorance of the benefits accrued from SAN affects its performance and Security on NASS	77	69	3	1	3.48
	Overall Mean					**3.42**

From table 3.7 above, the research question was to find out what are the security and performance loop holes that affects SAN on NASS Network. The overall mean indicated a positive response. This is because it was in line with the decision rule which states 2.5 and above response as considered positive. This shows that the respondent affirmed from item 16, 17, 18, 19 and 20 shows the security and performance loop holes that affects SAN on NASS Network.

3.2 SAN Analysis and Results using Wireshark Protocol Analyzer Simulation

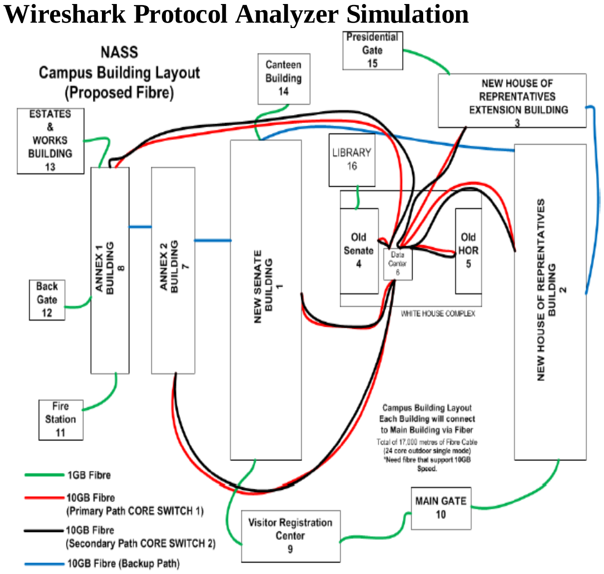


Figure 3.1: **NASS SAN Fibre Channels Architectural Layout** *that was analyzed (Source: NASS Field Survey of Adhoc/ Infrastructural Network Design, 2011)*

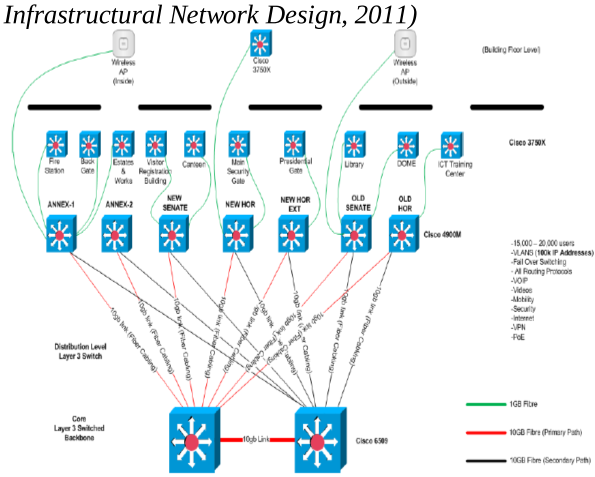


Figure3.2: Showing NASS Campus Enterprise and Data Center Network Distribution & Core (Source: NASS Field Survey of Adhoc/Infrastructural Network Design, 2011)

3.3 Result of the IP Configuration in Preparation of Packet Capturing and Analysis using: *ipconfig/all* in the command(cmd) prompt on NASS Network

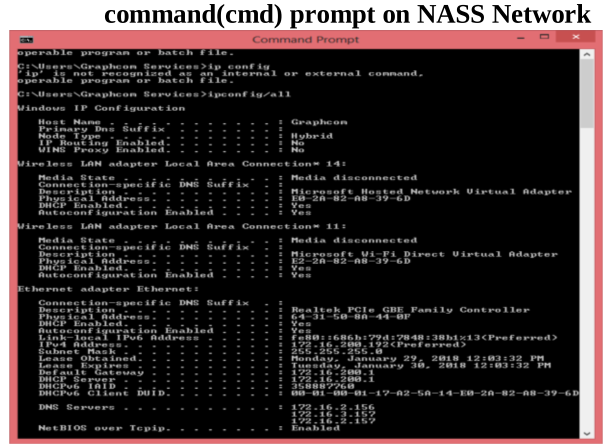


Figure 3.3 The ***ipconfig/all***above is to obtain the interface with the Default Gateway connection *(Source: Portscan Analysis on NASS Network using wireshark, 2018)*

3.4 Packet Frame Capture and Analysis of NASS SAN using Wire Shark

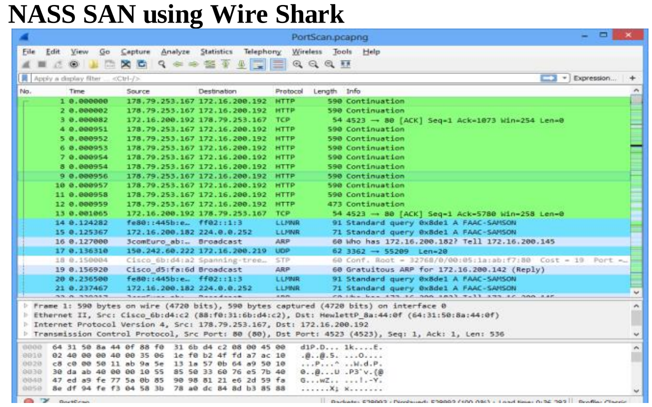


Figure 3.4: Captured packets/frames on National Assembly Network (Source: Portscan Analysis on NASS Network using wireshark, 2018)

Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 471-484
Published Online January 2020 in IJEAST (http://www.ijeast.com)

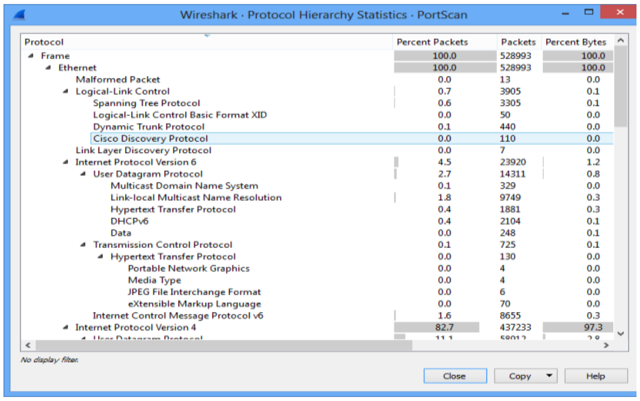


Figure 3.5: Showing Protocol Hierarchy Statistics of the PortScan (Source: Portscan Analysis on NASS Network using wireshark, 2018)

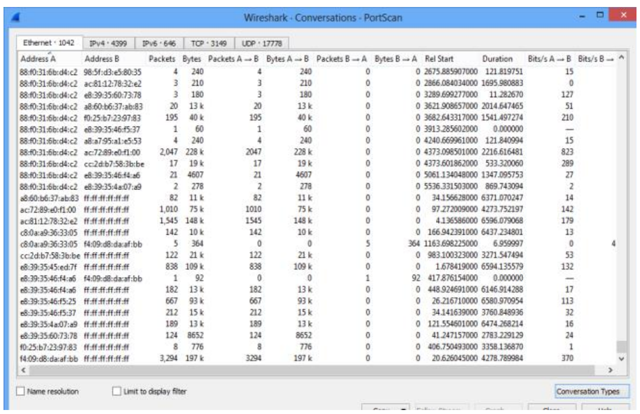
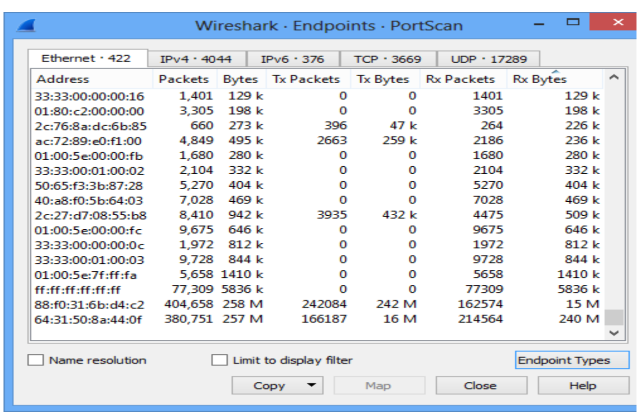
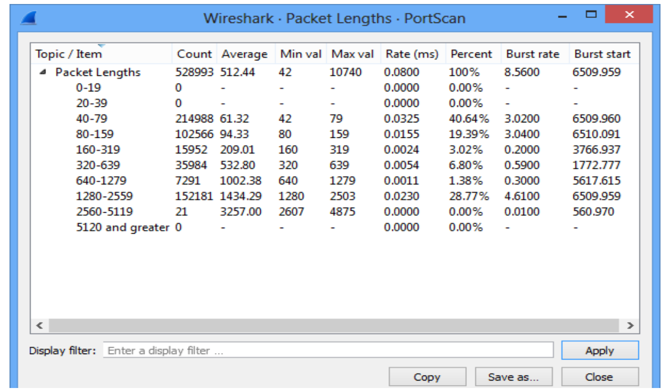


Figure3.6: Showing Statistical Analysis of Conversation on the National Assembly Network (Source: Portscan Analysis on NASS Network using wireshark, 2018)



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
33:33:00:00:00:16	1,401	129 k	0	0	1401	129 k
01:80:c2:00:00:00	3,305	198 k	0	0	3305	198 k
2c:76:8a:dc:6b:85	660	273 k	396	47 k	264	226 k
ac:72:89:e0:f1:00	4,849	495 k	2663	259 k	2186	236 k
01:00:5e:00:00:fb	1,680	280 k	0	0	1680	280 k
33:33:00:01:00:02	2,104	332 k	0	0	2104	332 k
50:65:f3:3b:87:28	5,270	404 k	0	0	5270	404 k
40:a8:f0:5b:64:03	7,028	469 k	0	0	7028	469 k
2c:27:d7:08:55:b8	8,410	942 k	3935	432 k	4475	509 k
01:00:5e:00:00:fc	9,675	646 k	0	0	9675	646 k
33:33:00:00:00:0c	1,972	812 k	0	0	1972	812 k
33:33:00:01:00:03	9,728	844 k	0	0	9728	844 k
01:00:5e:7f:ff:fa	5,658	1410 k	0	0	5658	1410 k
ff:ff:ff:ff:ff:ff	77,309	5836 k	0	0	77309	5836 k
88:f0:31:6b:d4:c2	404,658	258 M	242084	242 M	162574	15 M
64:31:50:8a:44:0f	380,751	257 M	166187	16 M	214564	240 M

Figure 3.7: Showing Endpoints in the PortScan on NASS Networking using Wireshark (Source: Portscan Analysis on NASS Network using wireshark, 2018)



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	528993	512.44	42	10740	0.0800	100%	8.5600	6509.959
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	214988	61.32	42	79	0.0325	40.64%	3.0200	6509.960
80-159	102566	94.33	80	159	0.0155	19.39%	3.0400	6510.091
160-319	15952	209.01	160	319	0.0024	3.02%	0.2000	3766.937
320-639	35984	532.80	320	639	0.0054	6.80%	0.5900	1772.777
640-1279	7291	1002.38	640	1279	0.0011	1.38%	0.3000	5617.615
1280-2559	152181	1434.29	1280	2503	0.0230	28.77%	4.6100	6509.959
2560-5119	21	3257.00	2607	4875	0.0000	0.00%	0.0100	560.970
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Figure4.12: Showing the HTTP packets counter analysis (Source: Portscan Analysis on NASS Network using wireshark, 2018)

4.5 Analysis of Captured Packets using DNS Filtering

This entails typing the Syntax: ***dns*** at the filter command segment and press the enter key to capture only DNS related packets for Analysis. Hence, **Results:**

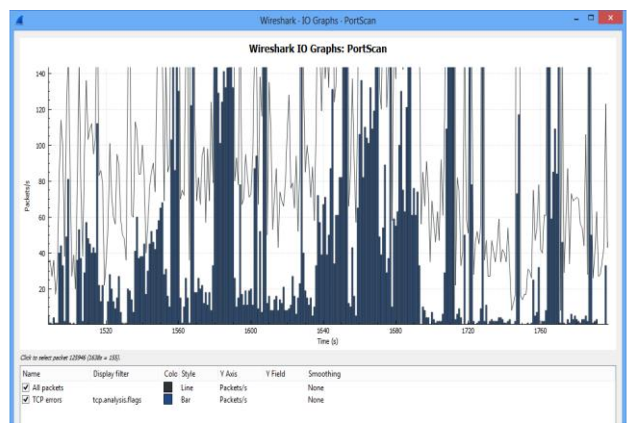
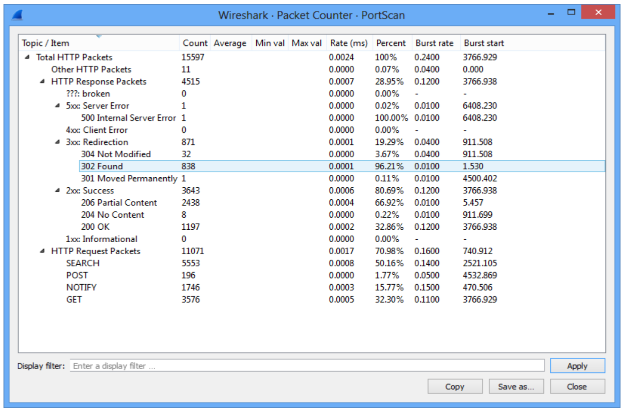


Figure 4.9: Showing the The I/O graph of the filtered DNS (Source: Portscan Analysis on NASS Network using wireshark, 2018)



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	15597				0.0024	100%	0.2400	3766.929
Other HTTP Packets	11				0.0000	0.07%	0.0400	0.000
HTTP Response Packets	4515				0.0007	28.95%	0.1200	3766.938
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	1				0.0000	0.02%	0.0100	6408.230
500 Internal Server Error	1				0.0000	100.00%	0.0100	6408.230
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	871				0.0001	19.29%	0.0400	911.508
304 Not Modified	32				0.0000	3.67%	0.0400	911.508
302 Found	838				0.0001	96.21%	0.0100	1.530
301 Moved Permanently	1				0.0000	0.11%	0.0100	4500.402
2xx: Success	3643				0.0006	80.69%	0.1200	3766.938
206 Partial Content	2438				0.0004	66.92%	0.0100	5.457
204 No Content	8				0.0000	0.22%	0.0100	911.699
200 OK	1197				0.0002	32.86%	0.1200	3766.938
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	11071				0.0017	70.98%	0.1600	740.912
SEARCH	5553				0.0008	50.16%	0.1400	2521.105
POST	196				0.0000	1.77%	0.0500	4532.869
NOTIFY	1746				0.0003	15.77%	0.1500	470.506
GET	3576				0.0005	32.30%	0.1100	3766.929

Figure 3.8: showing the Statistical Analysis of Packet Lengths on National Assembly Network (Source: Portscan Analysis on NASS Network using wireshark, 2018)

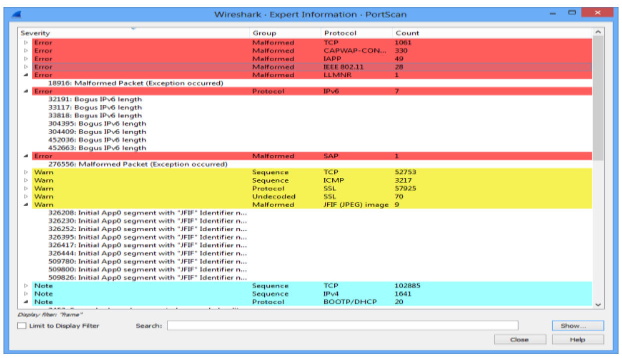


Figure4.13: Showing the Expert information of the PortSan using Wireshark (Source: Portscan Analysis on NASS Network using wireshark, 2018)

4.6 Analysis of Captured Packets using UDP Filtering

This entails typing the Syntax: ***udp*** *and* ***frame*** at the filter command segment and press the enter key to capture only DNS related packets for Analysis. Hence, Results:

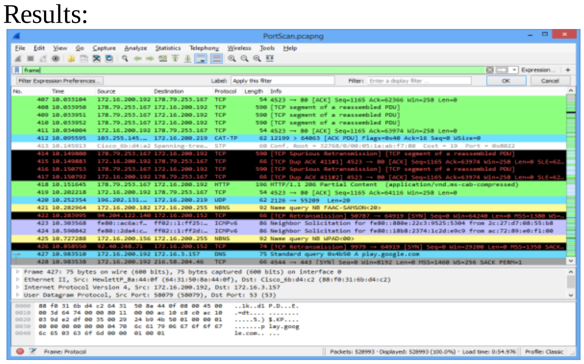
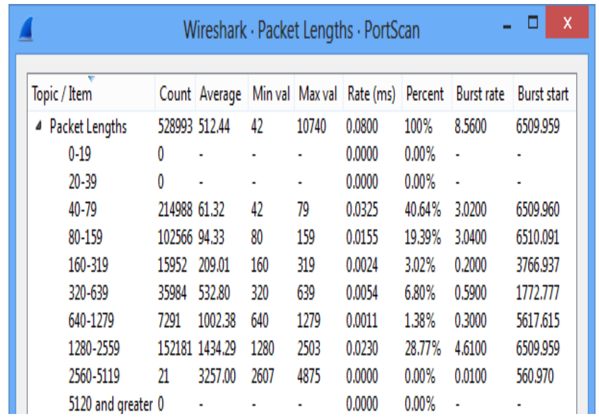


Figure4.14: Showing the result of the UDP and FRAME filtering (Source: Portscan Analysis on NASS Network using wireshark, 2018)



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	528993	512.44	42	10740	0.0800	100%	8.5600	6509.959
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	214988	61.32	42	79	0.0325	40.64%	3.0200	6509.960
80-159	102566	94.33	80	159	0.0155	19.39%	3.0400	6510.091
160-319	15952	209.01	160	319	0.0024	3.02%	0.2000	3766.937
320-639	35984	532.80	320	639	0.0054	6.80%	0.5900	1772.777
640-1279	7291	1002.38	640	1279	0.0011	1.38%	0.3000	5617.615
1280-2559	152181	1434.29	1280	2503	0.0230	28.77%	4.6100	6509.959
2560-5119	21	3257.00	2607	4875	0.0000	0.00%	0.0100	560.970
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Figure4.21: Showing Packet Length in filtered UDP(Source: Portscan Analysis on NASS Network using wireshark, 2018)

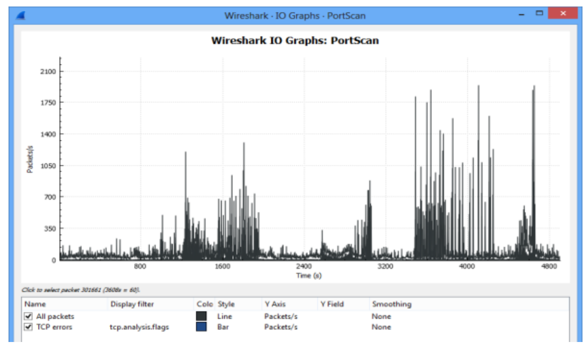


Figure 4.22: Showing I/O Graph for the filtered UDP stream (Source: Portscan Analysis on NASS Network using wireshark, 2018)

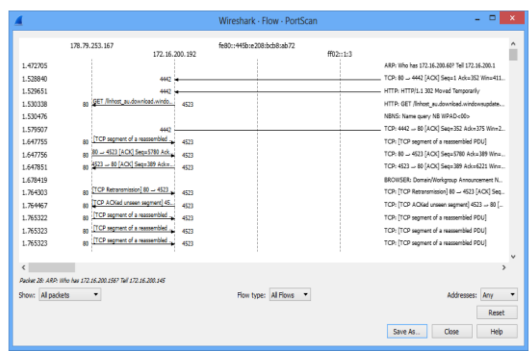


Figure 4.23 Showing filtered UDP stream when followed Source: Portscan Analysis on NASS Network using wireshark, 2018)

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 471-484
Published Online January 2020 in IJEAST (http://www.ijeast.com)

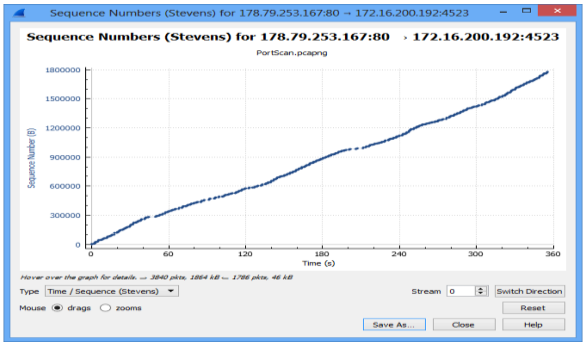


Figure 4.24: Showing Time SequenceStevens) Analysis of TCPGraph Stream of NASS etworkSource: Portscan Analysis on NASS Network using wireshark, 2018)

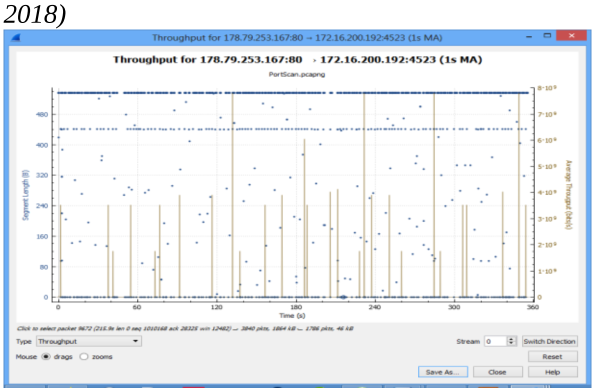


Figure 4.25: Showing Throughput Analysis of TCP Graph Stream of National Assembly Network Source: Portscan Analysis on NASS Network using wireshark, 2018)

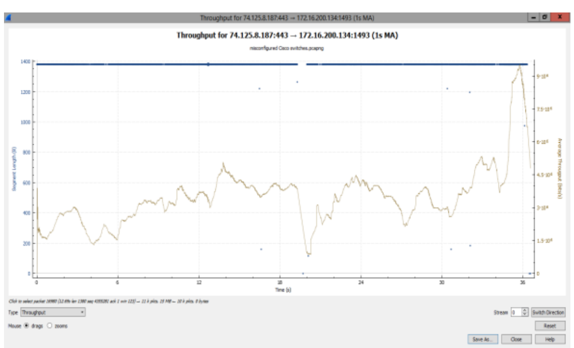


Figure 4.26: Showing Throughput Graph Analysis of for a Source to Destination IP Source: Portscan Analysis on NASS Network using wireshark, 2018)

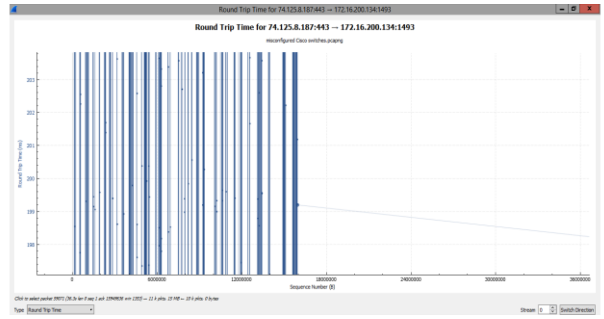


Figure4.27: Showing Round Trip Time Analysis of for a Source to Destination IPSource: Portscan Analysis on NASS Network using wireshark, 2018)

4.8 Performance Metric of Storage Area Network (SAN) on NASS Network

The performance metric is usually in consideration of the following: Bandwidth, Bit Rate, Burst Rate, Packet Length, Throughput, Latency (Delay) and Response Time. Thus, the two Network Metrics for evaluating performance are:

1. Throughput: The actual measure of how fast data can be sent through a network.
2. Latency (Delay): how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

In justification of the Result analysis above, the following were deducted:

(i) **Throughput:** At the point in the network when the bandwidth of 20Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 20,000 bits; the Throughput was evaluated thus; ***Throughput*** = 12,000 x 20,000 = **4 Mbps**
60

The throughput is almost one-tenth of the bandwidth in this case.

(ii) **Latency (Delay)** = Propagation Time + Transmission Time + Queuing Time +Processing Delay

Propagation Time: the measures of the time required for a bit to travel from the source to the destination. ***Propagation Time*** = Distance
Propagation Speed

The propagation speed of packet depends on the medium and on the frequency of the signal. Considering a packet propagated with a speed of 3 $x10^8$ mfs. It is lower in air; it is much lower in cable.

The propagation time of a distance between two points (Source - Destination) of 12,000km with a propagation speed of 2.4 x 108 mls in cable is thus estimated thus:

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 9, ISSN No. 2455-2143, Pages 471-484
Published Online January 2020 in IJEAST (http://www.ijeast.com)

Propagation Time = $\frac{12,000 \times 2000}{2.4 \times 10^8}$ = **100ms**

The above estimation show that due to effective cable links/connection, a bit from a source A reaches its destination B in 100ms.

This proved that the propagation time and element of throughput of the Network is OKAY

Transmission Time: Due to variation in leaving and arriving time of individual bits (which make up a Message) from source to destination, the time required for transmission of a message depends on the size of the message and the Bandwidth of the channel.

Transmission Time: = $\frac{\text{Message Size}}{\text{Bandwidth}}$

Thus; the propagation time and transmission time for a 3.5kbyte message (an e-mail) with network bandwidth of 1Gbps; have a distance of 12,000km between the sender and the receiver at 2.4 x 108mls light travels speed; hence, Propagation and transmission time thus;

Propagation Time = $\frac{12000 \times 2000}{2.4 \times 10^8}$ = **100ms**

Transmission Time = $\frac{4500 \times 8}{10^2}$

= **0.036ms**

In this case, the Transmission Time can be ignored because the message is short with high bandwidth; hence, the dominant factor is the Propagation Time not the transmission time.

In a similar scenario, with the propagation time and transmission time for a 5Mbyte message (an image) with network bandwidth of 1Mbps; have a distance of 12,000km between the sender and the receiver at 2.4 x 108mls light travels speed; hence, Propagation and transmission time estimated as: Propagation Time

= $\frac{12000 \times 2000}{2.4 \times 10^8}$ **=100ms**

Transmission Time = $9,000,000 \times 8 / 10^6$ = **72s**

In this case, the Propagation time can be ignored because the message is very long with bandwidth not very high; hence, the dominant factor is the Transmission Time not the Propagation time.

IV. PREVENTIVE MEASURES

Summary of Threat/Attacks and Security Measures on Storage Area Network and Fibre Channel on the National Assembly Network

The Implementation and deployments of Fibre Channel which is the back bone of SAN is confronted by some major threats such as the following table:

SN	ATTACK	Capacity, Acts and Effects	PREVENTIVE MEASURES
1.	***Insider threats***	The source of most attacks in SAN are insiders, insider known as the people who work with SAN management console and storage devices, most of the attackers from outside target these management consoles because the majority of management consoles are working over TCP/IP protocol and attackers are familiar with IP networks and their security holes. Insider attacker usually Spy the network causing a computer security breach in which a malicious user intercepts- and possibly alters – data traveling along a network." Due to the fact that insiders pose the greatest threat to data security, this type of inside attack is far more dangerous than outside attacks and should not be overlooked by any organizations.	The most common attacks in NASS-SAN are internal attacks, the first step of improving SAN security is begun with insiders. Vulnerabilities from insiders are related to the contractors and authorized person who has access to work with SAN. Control and defence of these types of attacks need to limit the responsibilities and access of the person who works with management devices and divide their responsibilities into different groups with different level of access. Using different username and password for each one of members with different level of access to the management console and devices, isolating the physical devices and servers if it is possible to separate them with other network devices and use access card and finger print at entrance. Control the system logs and activities of the administrators to verify changes and why changes happened to the system and by whom [5].
2.	***SNMP vulnerabilities***	Even though Simple Network Management Protocol (SNMP) has been considered by security experts as insecure for a long time, the CERT Coordination Center (CERT/CC), a computer security consortium,	Fortunately, while some SAN software vendors use SNMP for some basic storage-management operations, they more often implement higher-level functions using proprietary technology. Several strategies have been proposed by CERT/CC to counter the vulnerabilities in

		announcement that the Oulu University Secure Programming Group in Finland had discovered that SNMP is riddled with security holes that are more damaging than were first perceived. SNMP is a standard protocol that let network devices communicate information about their operational state to a central system, and has been used since this protocol appeared in 1989. This become a serious security issue because SAN vendors and storage-management software vendors has been supporting this protocol in their products all along. Oulu University researchers found SNMP to be vulnerable to Denial of Service (DoS) attacks, service interruptions in which an attacker can gain access to an affected device. This is viewed as serious compromise to ***integrity, availability and confidentiality*** of SAN fabric and the data being stored(6).	SNMP, but none is ideal. First is to determine whether the specific device vendor has developed a patch or workaround. CERT/CC has provided a list of vendors' responses to the SNMP alert on CERT Web site (7). Another recommendation is to disable or disconnect SNMP devices that are not essential to the operation of the SAN. If this is not viable, then ingress filtering can be used to block SNMP traffic from entering into network, because external hosts seldom need to initiate inbound traffic to machines that provide no external services. Other ideas include configuring SNMP agents to refuse messages from unauthorized systems, or segregating SNMP traffic onto a separate management network. CERT/CC has advised all companies to take action immediately because the SNMP vulnerabilities are real and dangerous to their network (8).
3.	***Session hijacking attack***	The is very dangerous because it is an act of taking over a whole session of the network. It makes both data/packets at rest or motion vulnerable.	Every session code created must have an equivalent code that destroys the session when operation is done; and as well to help log out unauthorized user
4.	***Address Weakness attack***	This usually occur from the misconfigured IP addresses and switches; which eventually form a spanning tree protocol and hence, giving room for eavesdropping on the network.	**Authorization**: authorization is used for verifying level of access to devices in a SAN and it's provided by the WWN address of the node or port that known as WWNN and WWPN (8).
5.	***Name Server Pollution attack***	It is a deliberate act by an intruder to compromise server name in order to have access to the network and storage resources	Servers should be authenticated with user and passwords to grant access to only authorized users. SAN fabric nameserver responses to queries based on the assumption that hosts will not contact storage devices that are not discovered via the nameserver.
6.	***ISCSI attacks***	iSCSI SAN faced with some other problems as well such as performance of devices that works with Ethernet base servers and switches, in general these devices do not need high performance for sharing their facilities with others but if we want to implement a SAN in a larger scale networks these devices cannot handle traffic and over load of the networks and we should switch to high performance ones. The other factor that effects on the performance of the iSCSI SAN is the initiator software type and version that used in our network for communication between storage devices, choosing the right software or hardware initiator can also effects on the	The following can improve the iSCSI SAN performance. Hence, iSCSI should not be used for applications that require using high speed network bandwidth, it is a good idea to possibly assigns the dedicate LAN just for traffic that related to iSCSI devices and always use upgrade and update version of the iSCSI initiator, using the devices that supports the higher bandwidth such as 1 to 10 GB/Sec network devices in the network architecture. Using CAT 6 cabling has better effect on speed of the network and performance. Separating subnet range of the network users from iSCSI traffic can be effective to improve performance on iSCSI SAN. Another useful issue for performance improvement is using balanced network

		performance of SAN. The current built in initiator software that used in operating systems are working well in general use but if the traffic overload goes higher and the network becomes larger with higher bandwidths and work load that is better to change the software initiator with the hardware one [(10)].	bandwidth, which means that use of equal or higher bandwidth between host initiators and targets and only assigns one or two storages to any NIC or HBA and put one of them as active and the other as standby. Using jumbo frame also can be a good idea for increasing the performance of the system, the normal frame size in IP networks is 1500 bytes with using jumbo frame can be increased up to 9000 bytes in size and improve the throughput and performance of iSCSI network up to 50% more so it contains more iSCSI commands and frame payload than normal frame size also jumbo frame is a convenient solution for longer distance [(9)].
7.	***Man-in-the-middle Attack***	There are several possible man-in-the-middle types of attacks to SAN such as: 1. World Wide Name (WWN) attack on the HBA. WWN attack happens when a machine with different HBA and WWN id assigned is accessing unauthorized storage resources through the SAN fabric. Whether it happens intentionally or accidentally, it can compromise the *confidentiality*, *availability* and *integrity* of the data. This attack can possibly be achieved by using a compromised dual-home host with a Host Bus Adapter (HBA) to read, store, or distribute SAN files. **2.** Management Admin attack – admin password unencrypted via telnet. Management attack can occur when unauthorized individuals in the network is able to obtain elements of management communications such as Administrator password using some type of sniffer software such as sniff, that can be used to grab passwords in the network.	1. As a solution, Device Connection Controls can be used to bind a particular WWN to a specific switch port or set of ports and preventing ports in another physical location from assuming the identity of an actual WWN. SAN **2.** Solution to use isolated subnet for management or do local management only. Several steps can be taken as protection against this type of attack, such as using SAN management software that encrypts password from some interfaces like Management Console, to a switch fabric. Management Console can also be placed in an isolated, dedicated network to protect it from 'Man-in-the-middle' type attack [(8)].
8.	***Internet Simple Name Server Domain Hopping Authentication Attack***	Most of the people who works with server storages thought that security is exist somewhere else in the network and there is no need to be worried about security features in storages and new technologies such as SAN	**Authentication**: help to identify the person, software or hardware to have permission for using system. Authentication doesn't exist by default in SAN.. Authentication is not inherently exist in SAN but through some other applications we can provide it to SAN such as SAN management software's and applications that have access to control SAN devices, some authentication models such as Diffie-Hellman-Challenge Handshake Protocol (DH-CHAP), Fibre Channel Authentication Protocol (FCAP) and Fibre Channel Security Protocol (FC-SP) provide security for different connection type

			such as switch-to-switch, node-to-node, node to switch connections [5].
9.	***Storage Theft***	Theft of storage media or storage devices can be used to access data as well as to deny legitimate use of the data	**LUN masking:** A storage device can be divided into logical units that are identified by logical unit numbers (LUNs10). LUN masking refers to making a LUN visible to some hosts while remaining invisible to others.
10.	***Sniffing Storage Traffic***	Storage traffic on dedicated storage networks or shared networks can be sniffed via passive network taps or traffic monitoring revealing data, metadata, and storage protocol signaling. If the sniffed traffic includes authentication details, it may be possible for the attacker to replay (retransmit) this information in an attempt to escalate the attack.	**Authentication:** For SANs it is important for a switch to verify the identity of other switches in the SAN with which it communicates to prevent rogue switches from joining a SAN. Likewise, the nodes in a SAN (e.g., storage devices and hosts) need to employ authentication to guard against unauthorized access to data.
11.	***Network Disruption***	Regardless of the underlying network technology, any software or congestion disruption to the network between the user and the storage system can degrade or disable storage.	**Access Control:** Access control on a SAN is implemented through application of zoning, Logical Unit (LUN) masking, and port binding mechanisms. In a SAN, Access control is based on machine identities rather than on the more familiar user and group identity types.
12.	***WWN Spoofing***	An attacker gains access to a storage system in order to access/modify/deny data or metadata	**Port Binding:** World Wide Names (WWN) are used for identification in a SAN. Port binding is a SAN security mechanism that specifies which WWNs are permitted to connect through that physical port. This association can mitigate snooping or spoofing attempts by an adversary and should be used whenever possible.
13.	***Storage Masquerading***	**An** attacker inserts a rogue storage device in order to access/modify/deny data or metadata supplied by a host	**Zoning:** A SAN fabric can be segmented into separate zones to restrict the visibility of portions of a SAN to specific hosts and storage devices. Soft zoning is based on limiting SAN fabric nameserver responses to queries based on the assumption that hosts will not contact storage devices that are not discovered via the nameserver. Some modern switches allow “hard” (switch ASIC) zoning based on WWN that uses physical port numbers on SAN switches to restrict traffic forwarding and is a more secure zoning method because it does not rely on correct host behavior and in particular is not vulnerable to spoofing of host identity.
14.	***Corruption of Data***	Accidental or intentional corruption of data can occur when the wrong hosts gain access to storage.	**Encryption:** There are two major use cases for encryption in assuring data confidentiality on a SAN: 1) data in motion and 2) data at rest. Sensitive and high-value data11 needs to be cryptographically protected in SANs when it is in motion as well as when it is at rest on a storage device.
15.	***Rogue Switch***	An attacker inserts a rogue switch in order to perform reconnaissance on the	**Zoning:** A SAN fabric can be segmented into separate zones to restrict the visibility of

		fabric (e.g., configurations, policies, security parameters, etc.) or facilitate other attacks.	portions of a SAN to specific hosts and storage devices. Soft zoning is based on limiting SAN fabric nameserver responses to queries based on the assumption that hosts will not contact storage devices that are not discovered via the nameserver. Some modern switches allow “hard” (switch ASIC) zoning based on WWN that uses physical port numbers on SAN switches to restrict traffic forwarding and is a more secure zoning method because it does not rely on correct host behavior and in particular is not vulnerable to spoofing of host identity.
16.	***Switch, Denial of Service (DoS).***	An attacker can disrupt, block or slow down access to data in a variety of ways by flooding storage networks with error messages or other approaches in an attempt to overload specific systems within the network.	**Availability**: checking the availability of devices is same as QOS and exists in layer 2 of FC that known as error control on frames. Availability and ability of detecting and controlling errors is one of the essential tasks on implementing a SAN [11].

V. CONCLUSION

This paper evaluates security and assessed the performance of Storage Area Network (SAN) on NASS Network. In this evaluation, it has been identified that the current configuration and resources at NASS are being threaten constantly due to misconfigured switches, internal and external threats, with the most dangerous threats to the network considered to be ***insider threat***.

In this research work, the performance of SAN at NASS and associated security challenges and threats are evaluated. Several internet protocol (IP) network and protocols are employed in the simulation. The analysis of the captured packets/frames on the Network is based on the following filtering: DNS, FTP, UDP, HTTP, HTTPS, ICMP, SCTP, SSL, STP, TCP streams, in their respective statistical analysis in terms of: I/O graphs, Flow graphs, TCP and UDP stream graphs, etc.; necessary preventive measures were tested and established from several stimulations and collected experiences from users to address the security and performance challenges on the Network. The results of this investigation as evaluated indicates that SAN is a convenient data storing solution when availability, data sharing, speed of transferring data and security are main goals. Hence, to achieve effective security on the network with optimum efficiency on the performance of SAN, it is proposed that the following measures be adopted:

- implementation of security best practices for installation/configuration; monitoring environment for unauthorized changes/activity;
- promote strong authentication and access control for administrative/operations access;
- enforce SLAs for patching and vulnerability remediation;

The security and performance features of SAN protocols can help the storage administrators to have better configuration on their network with respect to performance.

VI. REFERENCES

1. Prigges M. (2010),"Fibre Channel vs. iSCSI: The war continues",(http://www.infoworld.com)
2. Tate J., Beck P., Hecto I., Hugo R., Shunmugarathan K., Miklas L. (2012), Introduction to Storage Area Networks and System Networking, Fifth edition, IBM, United States (Pg 33-75).
3. Xubin He., Qing Y., and Ming Z. (2012), A Caching Strategy to Improve iSCSI Performance, University of Rhode Island, National Science Foundation under grants, ISBN: 0-7695-1591-6.
4. Chris L. (2012)," Fibre Channel Industry Association, Fibre Channel Features", San Francisco, USA, http://www.fibrechannel.org/.
5. Dwivedi H. (2005): ISCSI Security (InsecureSCSI),*https://www.blackhat.com/.*
6. SNI A. (2015), "*Storage Security: Encryption and Key Management*, August 2015", (pg 25-100).
7. *http://www.cert.org/advisories/ca-2002-03.html*.
8. Taylor M. (2012)," iSCSI Security: Networking and Security Options",*(www.computerweekly.com)*
9. Whitepaper (2011), "EMC best practice for performance and availability of storages, Corporate Headquarters",*http://www.emc.com.*

10. S.John. (2007), "iSCSI vs. Fibre Channel explained, Fibre Channel takes rightful place beside Fibre Channel", *http://www.cuttedge.com*.
11. SAN security (2010)," Storage area network (SAN) security FAQ, Network System Architects, Inc.", *(http://www.sansecurity.com)*
12. Akanksha V., Shrijee B. (2013), "performance Analysis of Internet protocol storage Area network and its usage in clustered database", International journal of Computer science Vol 10 issue4 No2 ISSN 1694-0784
13. Vishvanah R., Azra N. (2014), "Survey on Recent Technology of storage Area Network Attached Storage Protocols", Intertional Journal of Innovative Research in Electrical Electronic Instrumentation and Control engineering", Vol 2 Issue 8 August ISSN 2321-2004.
14. Brothers T., mandagare N. (2008),"Microsoft Exchange implementation and distributed Storage Area network", International Journal of computer and Applications, Vol 30 Issue 3)pg 251-264).
15. Priyaka M. (2016), " A study paper on Storage Area network problem solving issues", International journal of Computer Science Trends and Technology, Vol 4 ISSN 2347-8578.