Interested in learning more about security?

SANS Institute InfoSec Reading Room

Consolidating and Securing Enterprise Storage

In this paper, I will discuss how I plan on consolidating our enterprise storage using Sun's StorEdge 6960 SAN solution. I will start by defining what a SAN is and why has it become an essential part of a growing enterprise. I will briefly mention our current T3 SAN setup and its limitations. I will discuss the setup and configuration of SUN StorEdge 6960, the security features offered by SAN products in general and StorEdge 6960 in particular. I will describe how I plan on complementing these security features with ot...

Consolidating and Securing Enterprise Storage

GIAC Security Essentials Certification Practical
Version 1.4 (Option 1)

Abstract

In this paper, I will discuss how I plan on consolidating our enterprise storage using Sun's StorEdge 6960 SAN solution. I will start by defining what a SAN is and why has it become an essential part of a growing enterprise. I will briefly mention our current T3 SAN setup and its limitations. I will discuss the setup and configuration of SUN StorEdge 6960, the security features offered by SAN products in general and StorEdge 6960 in particular. I will describe how I plan on complementing these security features with other enterprise wide security measures already in place to achieve "defense in depth".

Storage Area Network

Recent industry research indicates that the storage requirement of an enterprise is growing at a staggering pace. IDC reports that the requirement for stored data is growing 80% annually [1]. In fact within our enterprise too, in the last 3-4 years we have outgrown our needs from a server attached RSM 2000 & T3 storage arrays. Unfortunately the IT staff qualified to manage these systems is only growing at only 5% per year[1]. The question then becomes how the IT managers are going to bridge this gap between high storage demand and shortage of human resources. The solution lies in utilizing the currently available Network Storage Technologies, namely NAS (Network Area Storage) and SAN (Storage Area Network). The distinction between the two is usually not very well understood as both achieve the objective of consolidating the enterprise storage requirement into one centralized storage. NAS and SAN represent two different storage technologies and they attach to the enterprise network in very different places. NAS is a defined product that sits between an application server and a file system. SAN is a defined architecture that sits between a file system and an underlying physical storage and is optimal for transferring storage blocks. A SAN is its own network, connecting all storage and all servers. SAN removes the storage from the servers so any server can gain access to any storage device regardless of the physical location of the storage or the user. In addition to offering any-to-any connections, SAN creates a scaleable environment. The number of nodes on a Fibre Channel-based SAN can grow and isn't limited like today's server-based DAS[2]. As a workgroup or Enterprise expands, its SAN can readily accommodate that growth. Fibre Channel-based SANs are frequently utilized to enhance data availability by increasing the speed at which data is shared. Creating an environment where any workstation has access to any

storage device leads to data being more readily available. The creation of an independent SAN further enhances the workflow of information among storage devices and other systems on the network. Additionally, moving storage-related functions and storage-to-storage data traffic to the SAN relieves the front end of the network, the Local Area Network (LAN), of time consuming burdens such as restore and backup. For all of the above mentioned reasons, inside a data center, SAN is often the preferred choice for addressing issues of bandwidth and data accessibility as well as for handling consolidations[3].

SAN Security

SAN is usually deployed in the enterprise's highly critical systems that require high availability (24x7), confidentiality and integrity. Workgroup SAN networks using Fibre Channel interface and protocol are physically isolated from the enterprise LAN and provide access to all of the storage to a "group" of users. As long as this "group" belongs to one department, the availability of data to all the users is not considered a major security threat. However this changes when multiple departments share SAN resources. Ability to identify the points of vulnerability and implement a reliable security solution is the key to securing a SAN fabric infrastructure. In order to get a better understanding of the SAN security issues, one should clearly understand the common SAN terminologies.[4]

There are no two opinions about securing the SAN. A 2002 InfoWorld Networked Survey indicated that 18% of those polled decided not to deploy SAN solution for their storage needs because of security concerns. For those who have already committed to a SAN solution, 56% still have security concerns. These concerns are multiplied many folds for IP-based SAN networks as these are vulnerable to many of the attacks made on corporate networks, such as spoofing and sniffing[5]. Since our enterprise SAN deployment is a fibre based physically isolated network, we will stick to deployment and security concerns of these only.

The primary security concern in SANs, also applicable to our environment, is the potential of un-authorized access. Since SAN provides any–to-any access, a hacker, after compromising an attached server has the ability to view confidential data. If they get the right permissions, the enterprise data can be destroyed or altered. The situation will be even worse if the SAN management host is compromised. A possible hacker in this case can even destroy the enterprise SAN architecture that may take lots of man-hours to rebuild. There are many different ways of dealing with the SAN security concerns.

Maintain data integrity by managing access to the data via software.

SAN management software or other software (e.g. OS and Volume Manager) can be used to limit access. Access can be limited by partitioning or segmenting storage resources so that only authorized users or enterprise groups can view

them. Storage administrators can separate sensitive information from less critical data on the SAN.

Using the SAN hardware components to limit access

There are several ways of limiting access to enterprise storage resources to specific users, servers and departments using the SAN hardware components. One such technique is called switch zoning. Switch zoning can be implemented on a single switch or multiple switches spread across the enterprise. The servers and the storage components can be part of single or multiple zones. These zones typically include components such as servers, storage devices, subsystems, and Host Bus Adapters (HBAs).

Switch zoning is further classified into two subcategories: hard zoning and soft zoning. In Hard zoning, also sometimes called a port zoning, members of individual zones are only allowed to communicate with other systems. Similar to what happens in a network switch, a SAN switch keeps a list of valid port addresses of a zone. Communication is allowed amongst port within the same zone. If a port tries to communicate with a port in a different zone, the frames from the non-authorized port are dropped. Since hard zoning is based on ports, it is more secure and efficient. However, this comes at the expense of less flexibility compared to soft zoning. Switch port numbers define whether a device is in a zone or not therefore moving of SAN components is not an easy task. It requires additional work by the network administrator to redo the zone assignments. This can become quite an hectic and repetitive task for a large enterprise with a dynamic environment.

Soft zoning is based on World Wide Number (WWN). Instead of looking at the port numbers, the switch in this case checks the WWNs of the source and destination. Frames are only forwarded if they belong to the same zones otherwise they are discarded. Since the switch in this case has to do additional work of checking the WWNs of both the source and destination, soft zoning is slower than hard zoning which results in a performance hit. A major benefit of soft zoning is flexibility. A device can be easily moved from one switch port to another without the need for zone assignment reconfiguration. This can save a lot of administrative time in SANs that have frequent configuration changes involving devices such as servers and storage subsystems. Soft zoning is also not as secure as its hardware counterpart (hard zoning). Though not very common in private Fibre Channel SANs, a hacker could pull off address spoofing by altering frame headers and making his or her way into a switch zone that's off limits.

Logical Unit Number (LUN) masking is another mechanism used by the SAN components. It serves the same goal of limiting access to storage resources to a set of servers and users, but in a different way. A LUN is defined as a SCSI logical unit number within a target. LUNs are physical storage components that

include disks and tape drives. In Fibre Channel SANs, LUNs are assigned based on the WWNs of the devices and components. LUN masking is the ability to exclusively assign each LUN to one or more connected host. The attached server can see only the LUNs that have been assigned to it. If multiple servers or departments are accessing a single storage device, LUN masking enables the network manager or administrator to limit the visibility of these servers or departments to a specific LUN (or LUNs) to help ensure security. LUN masking gives the added advantage of having a more granular control on the enterprise storage. For example, if switches hard zoning is used, all the LUNs on SUN T3 storage device would be available to all the hosts in the same zone as the T3. There is no way to limit the access to LUNs within a device. With LUN masking this can be easily done. LUN masking can be implemented at various locations within the SAN, including storage arrays, bridges and routers, and HBAs.

Our current SAN setup

In our current environment we have Sun StorEdge T3 [6,7] arrays connected in a SAN environment via a redundant switch fabric. These powerful SAN solutions can be configured either as a single controller unit "workgroup" model the T3WG or a dual controller unit "enterprise" model the T3ES (see FIGURE 1). The dual controller T3ES is fundamentally two T3WGs cabled together to act as one storage device. The T3ES is also referred to as a "partner group," as it has two controller units that act as one. T3ES configuration contains fully redundant components; a pair of dual 16-port redundant fail-over switches and a pair (or pairs) of redundant fail-over drive controller trays. In our T3WG configuration, the controller is the single point-of-failure. To ensure that this would not cause a disruption in enterprise data availability, host based software (using a volume manager like Veritas Volume Manager) mirroring is used. As storage needs grow, a pair of T3 bricks is simply added to the switch ports.

The SunStorEdge T3 are out-of-band devices. This means that configuration and enterprise data travel on separate links. This helps in improving the performance on the Fibre data link, while device monitoring and trouble-shooting is carried out using their Ethernet interface. A management host is used to administer, configure, and monitor these arrays. Telnet is used to connect to the T3s from this management host. To avoid transmitting the T3 admin passwords in plain on our public network, we configured a private 10.X.X.X network.

While the above setup has performed well, it has its limitations:

- Setup and configuration has to be done on individual T3. For a small number of devices this may not be an issue. but as we scale to large number of T3, this will result in large management overhead.

- There is a limited number of LUNs that each T3 can be divided into and depends on the RAID controller hardware in these storage devices.

- T3 are visible to all the servers connected to the SAN switches. The servers belong to different groups in the enterprise. Ownership of these devices is configured in Veritas Volume Manager. A compromised server can forcibly import devices containing confidential enterprise data.

- Since the communication between the management station and the T3 is not encrypted, the possibility of compromising admin password exists.

Sun StorEdge 6960

When it was time to consolidate our enterprise storage requirements, we decided to look for a solution that will not only provide us with more space but will also overcome these T3 limitations. The Sun StorEdge 6960 [8,9] system targets the enterprise SAN environment and has features that overcome the limitations with our current setup. The Architecture of 6960 is shown in Figure 2. Some of 6960 features are described as follows:

- A Storage Service Processor is included in each subsystem. This centralized SAN management server provides support for monitoring and configuration of all the attached T3s, including upgrades of firmware. It is connected internally on a private LAN with all the T3 and provides out-of-band storage management. It is a SUN workstation running Solaris 8 and it provides software and diagnostic tools to support effective isolation. It is also connected to our private LAN on another interface. Since it is a Solaris server, for added security it can be hardened like any other server system in the enterprise by running SUN JASS scripts. We connect to this from our private LAN using ssh, thus ensuring that administrative passwords can not be snooped as an added measure of security, even though the SSP is on a private network.

- Logical unit number (LUN) segmenting, slicing, or carving for storage consolidation gives us much granular control over the usage of the enterprise storage, thus providing better utilization.

- LUN security access (masking) for the storage consolidation models. We have already discussed this in detail in the previous section.

- Support for cascading switches. This provides scalability needed to accommodate our increasing storage requirements.

- Data Path Redundancy. All of the storage subsystems provide full data path redundancy with no data path component as a single point of failure, offering 24x7 data availability. Redundant components include the FC switches, Sun StorEdge T3+ arrays, virtualization engines and dual power distribution units (PDUs).

Figure 3 shows the Sun StorEdge 6960 system. The system uses two Sun StorEdge network FC 16 port switches for host connections. A maximum of 14 hosts (Solaris, NT/Windows2000 and Linux) can be connected, even though 14 ports are available for hosts per switch. For redundancy purposes the second switch has connections to a second HBA on these hosts. The system can support up to three Sun StorEdge T3+ arrays in one cabinet. By adding a Sun StorEdge 6960 expansion cabinet, the system supports up to eight Sun StorEdge T3+ arrays. The total configured capacity of 6960 storage is between 472GB and 20.16 TB.

Configuration and Setup

We currently have a one rack 6960 with two T3 partner-pair. The space will be shared by two departments of the enterprise. Using the virtualization, we carved the LUN into 5 VLUNs. For LUN masking we had, couple of options:

- Create two zones for the two departments and associate the VLUNS and the HBA of the servers to their respective zones. This provided us the security we needed, however we would have lost the HBA fail over capability using Veritas's Dynamic Multipathing. For that to work the two HBAs have to be in different zones.

- Create zones for each of the HBAs and then associate VLUNs to those.

For fail over capabilities to work using DMP we choose option 2.

Virtualization LUN summary for LUNs seen by virtualization engine v1 is shown below. This was collected using the showvemap command on the storage service processor. As you can see the each LUN is divided into 5 VLUNS. In this setup we can freely assign VLUNs to any number of zones. Zones are defined per HBA. Thus we control what VLUNs a server can see.

VIRTUAL LUN SUMMARY

Diskpool	VLUN Serial Number	MP Drive Target	VLUN Target	VLUN Name	Size GB	Slic	Zones
t3b00	6257483330303038	T49152	T16384	1_t3b00	100.0		
t3b00	6257483330303039	T49152	T16385	2_t3b00	100.0		
t3b00	6257483330303041	T49152	T16386	3_t3b00	100.0		
t3b00	6257483330303042	T49152	T16387	4_t3b00	100.0		
t3b00	6257483330303050	T49152	T16392	VLUN1	77.0	FL_Unix_h2s	
t3b01	6257483330303043	T49153	T16388	1_t3b01	100.0		
t3b01	6257483330303044	T49153	T16389	2_t3b01	100.0		
t3b01	6257483330303045	T49153	T16390	3_t3b01	100.0		
t3b01	6257483330303046	T49153	T16391	4_t3b01	100.0		
t3b01	6257483330303051	T49153	T16393	VLUN2	77.0		

ZONE SUMMARY

Zone Name	HBA WWN	HBA Name VLUNs	Initiator	Online	Number of VLUNs
FL_Unix_h1s	210000E08B072945	FL_Unix_h1s	I00002	Yes	0
FL_Unix_h2s	210000E08B075243	FL_Unix_h2s	I00002	Yes	1
Undefined	210000E08B072945	FL_Unix_h1s	I00001	Yes	0
Undefined	210000E08B075243	FL_Unix_h2s	I00001	Yes	0

Defense in depth

In previous sections, we looked at the primary issues of concern for SAN security and some of the possible solutions in general. The technique used in Sun StorEdge for restricting access is LUN masking. There are additional and more complex approaches that can be used, such as employing Brocade's Secure Fabric OS (SFOS)[10]. However, these are expensive and complex solutions which are usually used in large SAN environments that may spread across multiple geographical locations and connected over IP networks. For a relatively secure environment like ours, a Medium Security level can be achieved by complementing the SAN security features with enterprise security and using third party tools. Our Multi-layered SAN security comprises of the following layers:

- Layer One: These are the organization wide security measures (Firewalls and IDS) from the outside world.

- Layer Two: This comprises of the servers that are attached to the SAN. These servers are secured by

  - Installing the latest SUN recommended and security patches[11] and installing, configuring and running the SUN JASS (Jumpstart Architecture and Security Scripts) toolkit[12]. This kit hardens and secures the Solaris Operating Systems. It does this by disabling unnecessary internet services and daemons that are started by default. Once this is done, on per server basic we re-enable the services and daemons that are required for the server to function.
  - Using Secure Shell (ssh)[13] for remote sessions. Ssh is a program for logging into and executing commands on remote machines. It is primarily used to provide secure encrypted communications between two untrusted hosts over a public network. It has various other features including X11 and TCP/IP port forwarding over the secure channel. On most sites it is being used as a replacement for its old insecure counterparts, rlogin, rsh and rcp.

- Enforcing strict passwords. Expiring passwords and checking for weak passwords on a routine basis using tools like John the Ripper[14]. John the Ripper is a fast password cracker, currently available for many flavors on multiple platforms. Its primary purpose is to detect weak Unix passwords.
- Monitoring the network traffic, using MRTG[15] for DOS attacks and other irregular network traffic patterns. Figure 4a & 4b show the network traffic on one of the production servers attached to the SAN. Looking at these 48 hrs (a) and Weekly (b) graphs one can easily notice a DOS (Denial of Service) or other suspicious activities. The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing graphical images which provide a LIVE visual representation of this traffic. MRTG is based on Perl and C and works under UNIX and Windows NT.
- Monitoring the system and status of its daemons, services and processes using the Big Brother[16] system and network monitor. A screen shot of what our Big Brother web page looks like is shown in Figure 5. Big Brother and its extensions are discussed in detail later in other sections.

- Layer Three: This is the SAN security layer. As we have already discussed, SAN is secured by
  - Protecting the devices on SAN from un-authorized access. This is done by employing LUN masking capabilities of SUN StorEdge 6960.
  - Protecting access to SAN component configuration. This is dealt with again by 6960 by having a private network connecting the storage devices, switches and virtualization configuration ports.

- Layer Four: Backup and Recovery. In order to ensure availability and integrity of enterprise data in case of its loss or compromise, backups are done daily. Our backup architecture is shown in Figure 6. The data is backed up using a Legato Networker[17] 6.1 server, to two ADIC [18] Scalar 100 tape libraries. The backup clients comprise of Sun & NT servers. We have divided the servers that are backed up into two groups, A & B. The production servers are placed in Group B. These servers are configured with an additional network interface and form a separate private backup network. This avoids putting the backup traffic on the public LAN, which can then be fully utilized for the enterprise data traffic. The backups are run on a daily basis. One set of full backups are run on the weekends, while incremental sets are run daily. These full weekly backups save data from all the save sets except a few that quite large and pretty static. Another set of full backups are run every month that do a full backup for all the servers.

- Layer Five: The physical access to SAN is controlled in this layer by allowing only authorized personel in the data center, locking the cabinets of SAN components (SUN StorEdge 6960, T3 Rack) and removing the power keys from the servers and locking them in a safe.

Big Brother

Big Brother is a web based system and network monitoring tool. It displays its output on web pages that are refreshed every 5 minutes (default setting), thus enabling enterprise system, network and database administrators to see how their servers are working in near real-time, from any web browser, anywhere. As can be seen from sample shot of Big Brother display page (Figure 5), it has systems monitored listed in the rows on the left hand side while the the tests for each system in columns across the top of the page. The monitored systems and tests form a matrix of different colored dots on the web page. Green being good, yellow being a warning and red being an indication of trouble. The background color of the status pages is always the color of the most serious condition of any element being monitored at that time.

Big Brother uses a client-server architecture combined with methods which both push and pull data. Network testing is done by polling all monitored services from a single machine, and reporting these results to a central location. This centralized location is defined by a configuration variable BBDISPLAY on each client host. To gather local system information, a BB client needs to be installed on the local machine. With a default install this will send CPU, process, disk space, and logfile (/var/adm/messages for unix servers) status reports in periodically. Each report is time stamped with an expiration date. This lets one know when a report is no longer valid. When this happens the system admin needs look at the reasons for causing this. One of the most common reasons in my experience is that the BB client on the server being monitored dies. Why it dies needs to be investigated further. The Big Brother servers and BBNET functions run on Unix/Linux and NT/Win2K. Clients are available for Unix/Linux, NT (works on Win2K), Novell, and the Mac.

Big Brother includes support for testing ftp, http, https, smtp, pop3, dns, telnet, imap, nntp, and ssh servers. Support for additional tests can be easily added by making some configuration changes. When a BB client is installed on a local machine, it will monitor disk space, CPU usage, messages file, and can check that important processes are up and running.

Big Brother also provides notification using e-mail and pager alerts. The notifications are easily customized so that one can notify based on time-of-day, machine, or the test that failed. In addition, it supports an initial delay before paging (to avoid late night false alarms), page-only-every defined amount of time, paging groups, acknowledgement, and escalation.

Big Brother also provides reporting based on the server names. In addition, it provides access to historical status information so one can see what the problem was at any given time. Big Brother supports external scripts /plug-ins[19] to monitor everything from Sybase Databases to CPU temperature on Solaris machines. Big Brother is very flexible. Warning and alarm levels are all easily re-definable. The Web Display can be easily customized. BB has hooks into other products, like MRTG for bandwidth monitoring. One can easily adapt the source code to suite specific needs.

Big Brother Extensions

In addition to the default configuration, more tests and monitors can be easily added using external scripts. We have added several extensions to our Big Brother monitoring server. This has greatly increased our system availability and security and helped us reduce, and in some cases eliminate production system downtime. Some of these external monitors are:

larrd ™

One of the most important plug-in for Big Brother is larrd[20]. It lets us take the important data from Big Brother logs and plots them over multiple time durations (hourly, daily, weekly & monthly). Default install lets us generate plots for system's load average, CPU utilization, disk utilization, TCP connect times, processes & users, and vmstat. Figure 7 shows some of the useful larrd plots. We have modified it to generate graphs for our several customized plug-ins. Some important ones are

- Connection counts to our production JRun.
- Connection counts to our production Sybase.
- Web response time from our production iPlanet webservers.

A.I.D.E. (Advanced Intrusion Detection Environment)

Aide[21] is exactly what its name implies, an intrusion detection tool. It creates a database from the regular expression rules that it finds from the config file. Once this database is initialized it is used to verify the integrity of the files. Figure 8 shows an alert that occurred when changes were being made on the monitored server. In this case it was an administrator who made the change, however had it been a real attacker, modification of these files would have resulted in notifications (e-mails/pages) being sent out with-in 5 minutes.

Nmap ("Network Mapper") Extension.

Nmap[22] is a security scanner used for network exploration and security auditing. It can rapidly do ping sweep, port scans and OS detection on large networks.

Nmap runs on most types of computers and has both command line and graphical versions. "Nmap is a classic example of a reconnaissance tool. Reconnaissance tools are used to gather information about a site before actually launching an attack. If an attacker can gather enough information during reconnaissance, ultimate compromise of network is trivial[23]". Nmap external script monitors what ports are open on our servers and compares them with a list of what should be open on these servers and alerts us in case of a mismatch. One such alert is shown in Figure 9.

Another important monitor script is one that scans the system logs to find if some one has tried accessing the open ports of web servers and sendmail to gain access. Two such events are shown in Figures 10 & 11, where intruders ran malicious commands.

Conclusion

SAN consolidation helps an enterprise better manage its resources. Since it is a relatively newer architecture than DAS (direct attached storage), IT managers have their apprehensions about implementing it. One of the primary concerns is the security in such storage networks. Though these features are still maturing, there exists enough (LUN masking and zoning) that Fibre Channel SAN can be deployed with relative confidence in an enterprise. "Defense in depth" can be achieved by complementing the SAN security with enterprise security measures and forming multi-layers of protection using security and monitoring tools. These almost guarantee earlier detection, if not absolute protection from malicious intruders.

References

1. Security for the SAN Workgroup by Jeffrey D. Coffed
http://www.attotech.com/pdfs/SANSecure.pdf

2. Network Storage – The Basics by Drew Bird
http://www.enterprisestorageforum.com/technology/features/article/0,,1064_947551,00.html

3. Network-Attached Storage, White Paper by Sun Microsysterms
http://www.sun.com/storage/white-papers/nas.html

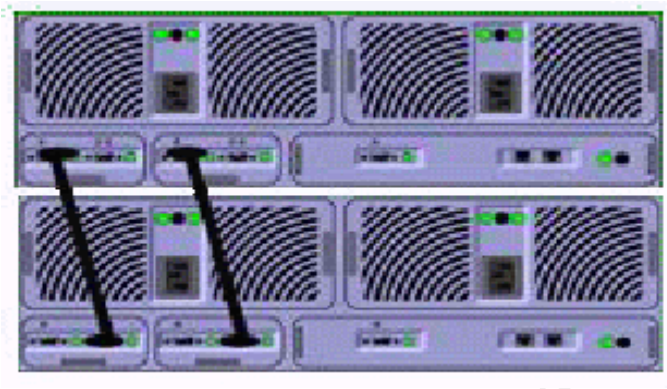
4. SAN Security Glossary
http://www.computerworld.com/printthis/2002/0,4814,75203,00.html

5. SAN security goes IP, Mandy Andres, May 10 2002, InfoWorld
http://www.infoworld.com/article/02/05/10/020513fesecurity1_1.html

6. SUN STOREDGE T3 ARRAY FOR THE ENTERPRISE Features, Functions & benefits
http://www.sun.com/storage/t3es/features.html
7. The Sun StorEdge™ T3 Array: Installation, Configuration, and Monitoring Best Practices *By Ted Gregg*
http://www.sun.com/solutions/blueprints/1001/t3bp.pdf

8. Sun StoreEdge ™ 6900 Series
http://www.sun.com/storage/midrange/6900/index.html
9. Sun StorEdge™3900 and 6900 Series 1.1 Reference and Service Manual Part No. 816-5253-10, July 2002, Revision A
10. SAN Security: A best Practices Guide
http://www.brocadekorea.com/download/resource/SAN_Security_Practices_Guide.pdf
11. Sun Solaris Patches
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
12. Solaris Security Tools : Jumpstart Architecture Solaris Scripts (JASS)
http://wwws.sun.com/software/security/jass/
13. Openssh http://www.openssh.com/
14. John the Ripper http://www.openwall.com/john/
15. Multi Router Traffic Grapher (MRTG)
http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
16. Big Brother System and Network Monitor http://bb4.com
17. Legato Networker: http://portal2.legato.com/products/networker/
18. ADIC Scalar 100 Tape Library
http://www.adic.com/ibeCCtpItmDspRte.jsp?minisite=10000&respid=22372&item=43102&section=10058
19. Big Brother External Scripts and Plug-ins. http://www.deadcat.net
20. larrd : Tool for plotting vital system parameters.
http://www.packetpushers.com/projects.htm
21. Advanced Intrusion Detection Environment (AIDE)
http://www.cs.tut.fi/~rammer/aide.html
22. Nmap (Network Mapper) http://www.insecure.org/nmap/
23. GSEC Security Essentials ToolKit by Eric Cole.

T3WG (Single Brick)



T3ES (Partner Group)

Figure 1. T3 Configurations [7]

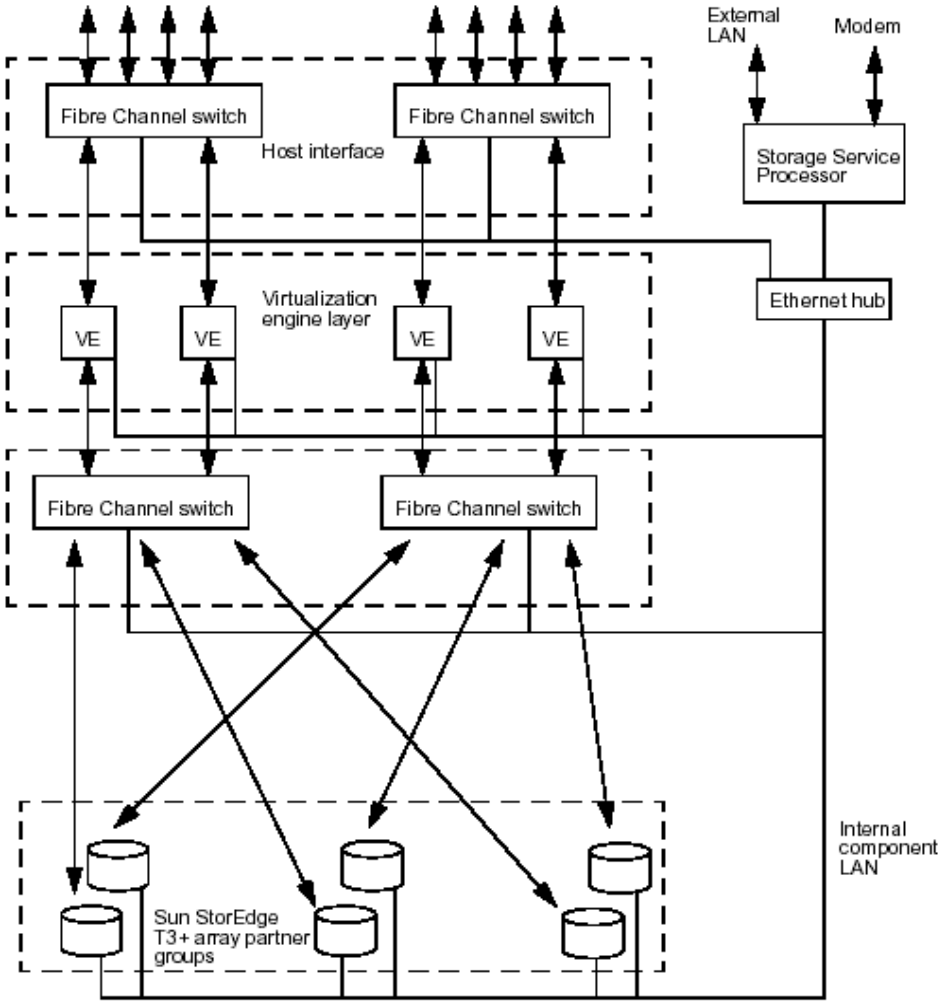


FIGURE 2. Sun StorEdge 6960 Series Architecture[9]

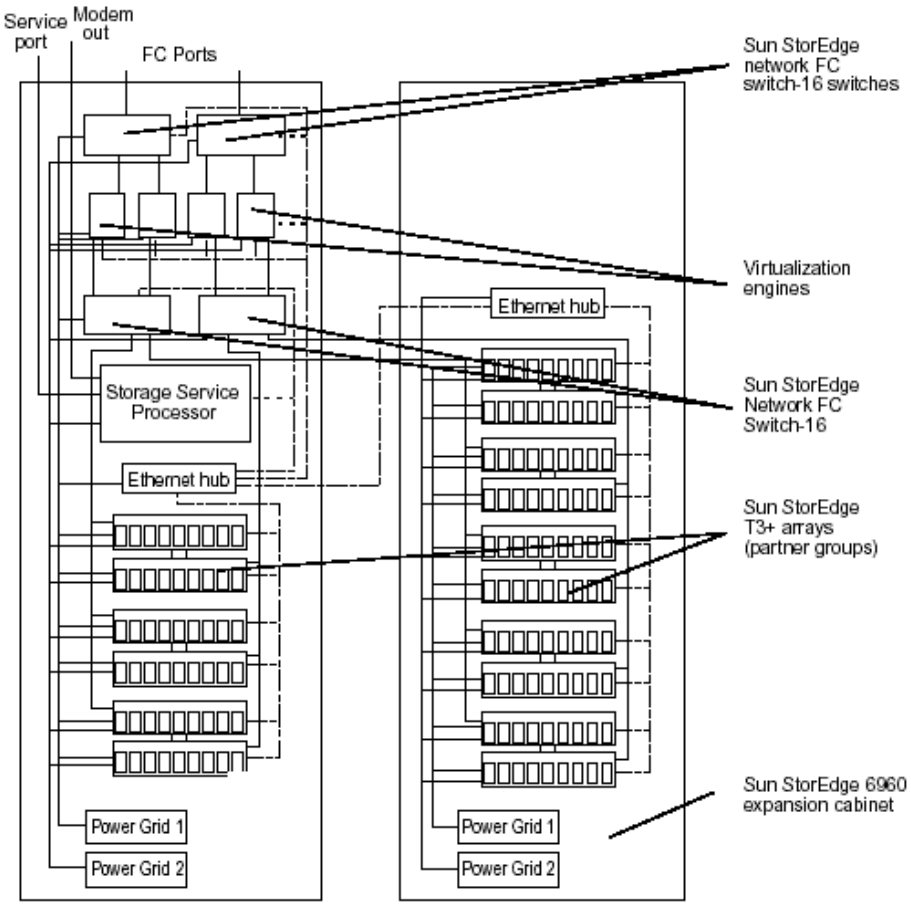
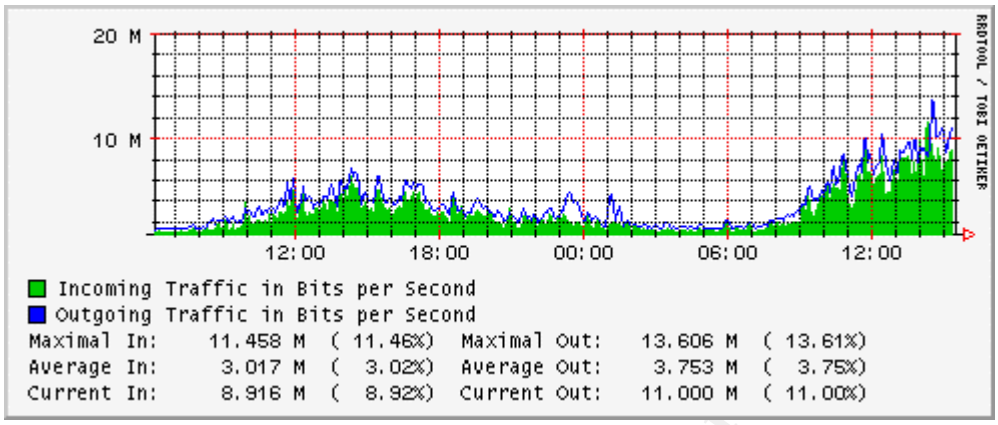
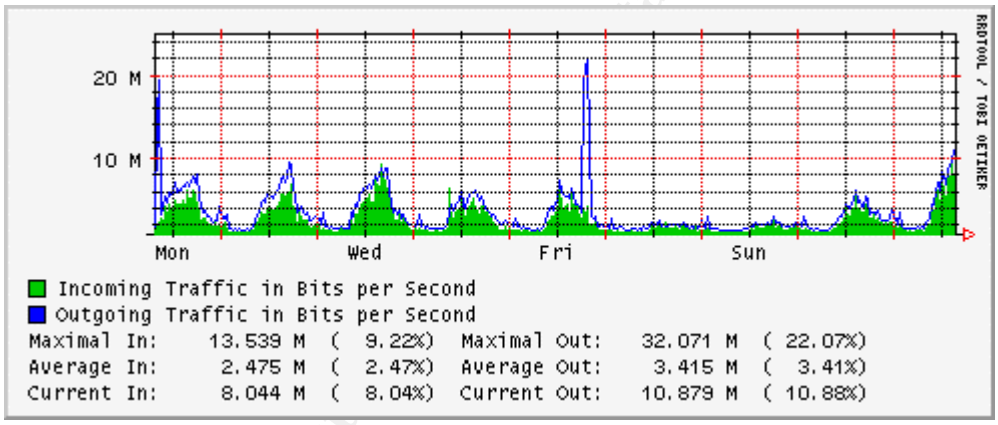


Figure 3. Sun StorEdge 6960 System[9]



a) Daily Graphs



b) Weekly Graphs

Figure 4 a & b show an MRTG graph of the network traffic on one of our production servers.

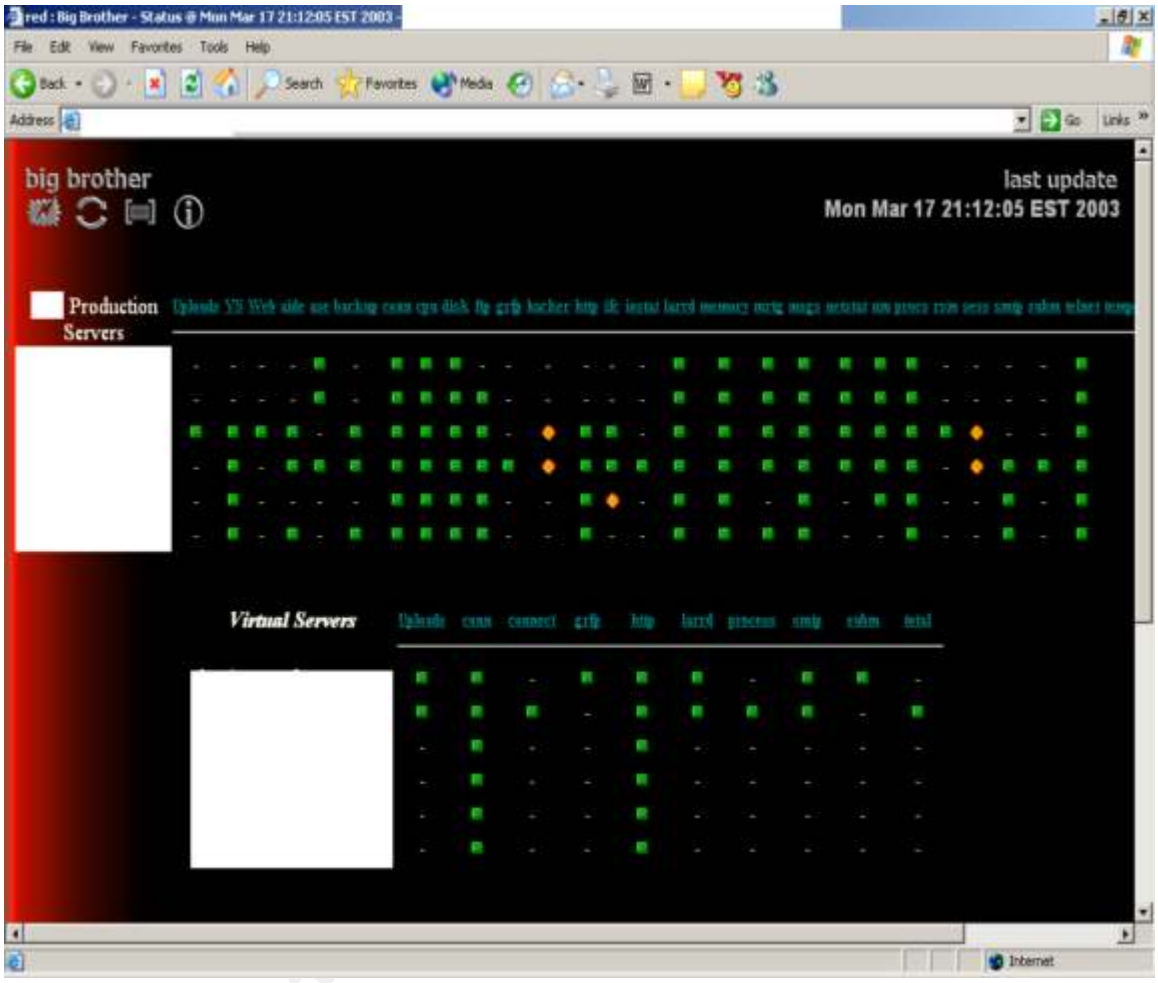


Figure 5. Screen Shot from Big Brother Server.

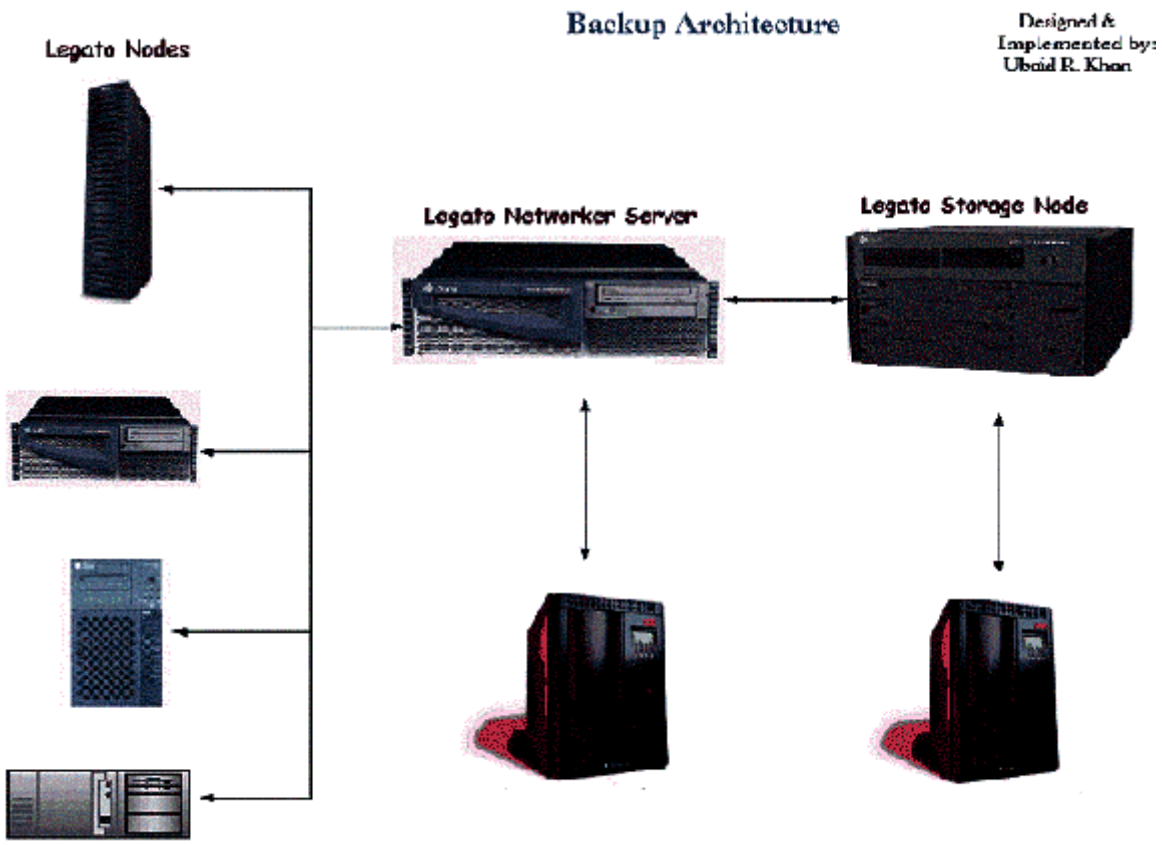


Figure 6: Backup Architecture

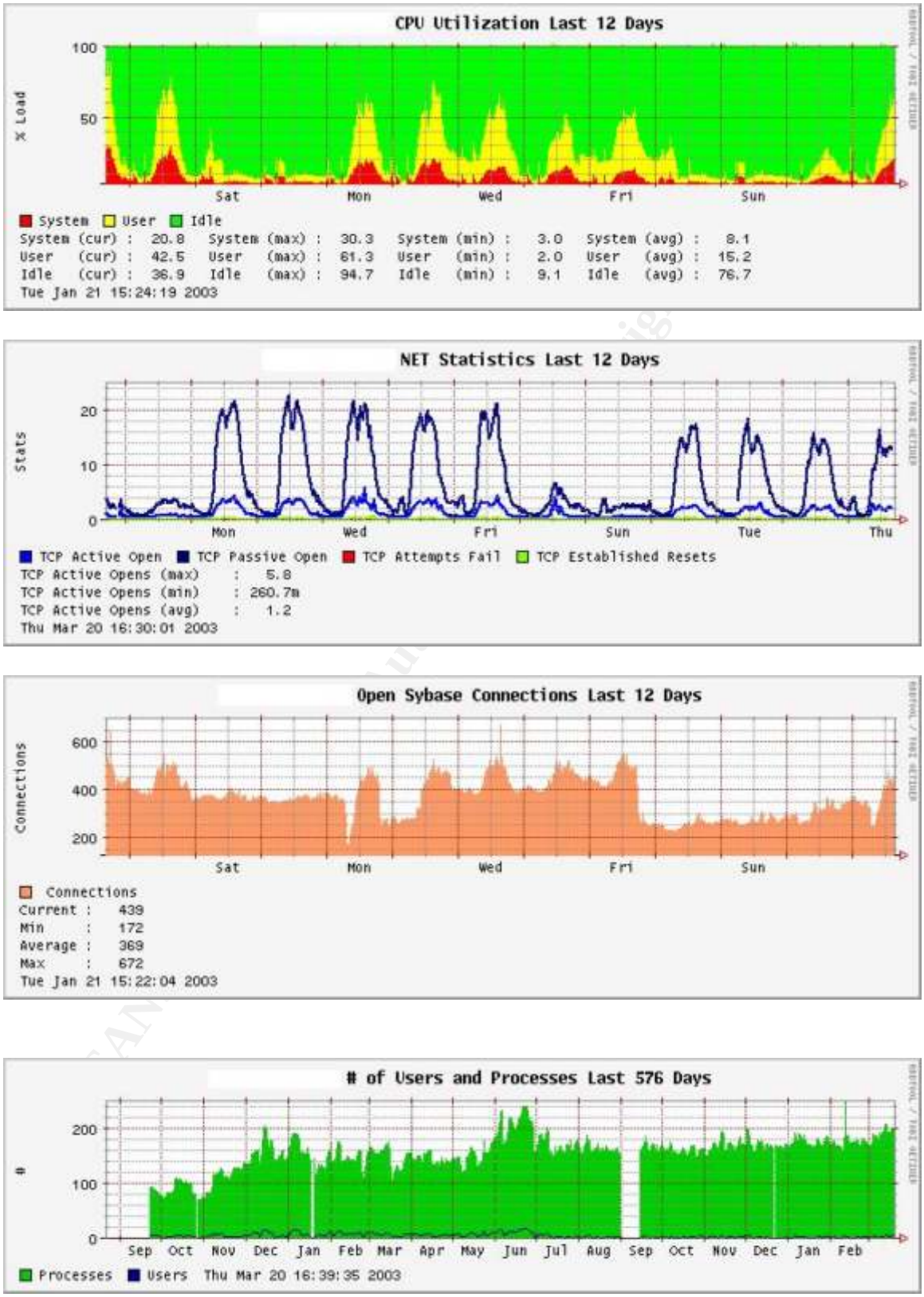


Figure 7. Some useful larrd plots.

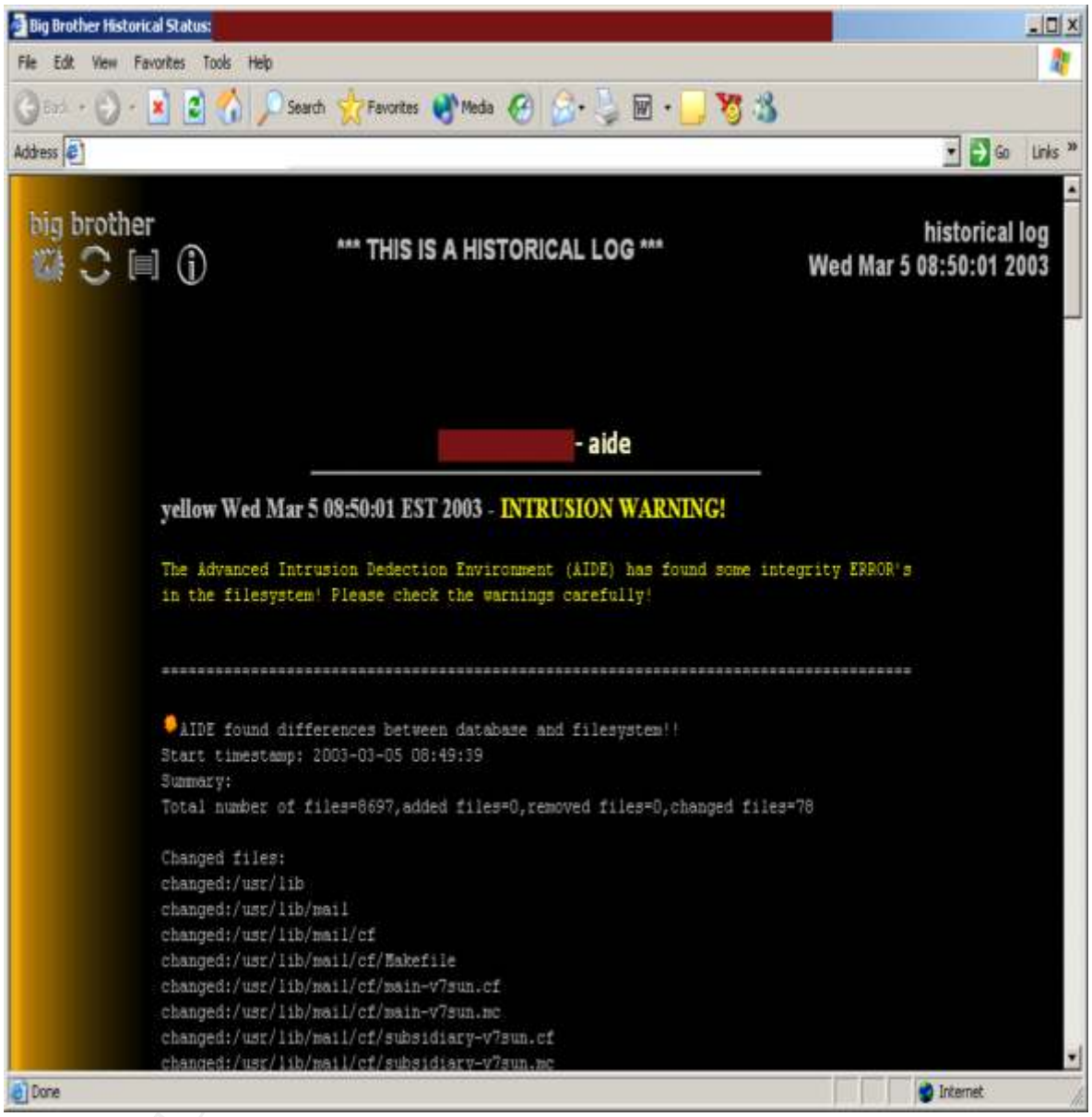


Figure 8. Shows a Big Brother alert for AIDE integrity check on one of our servers.

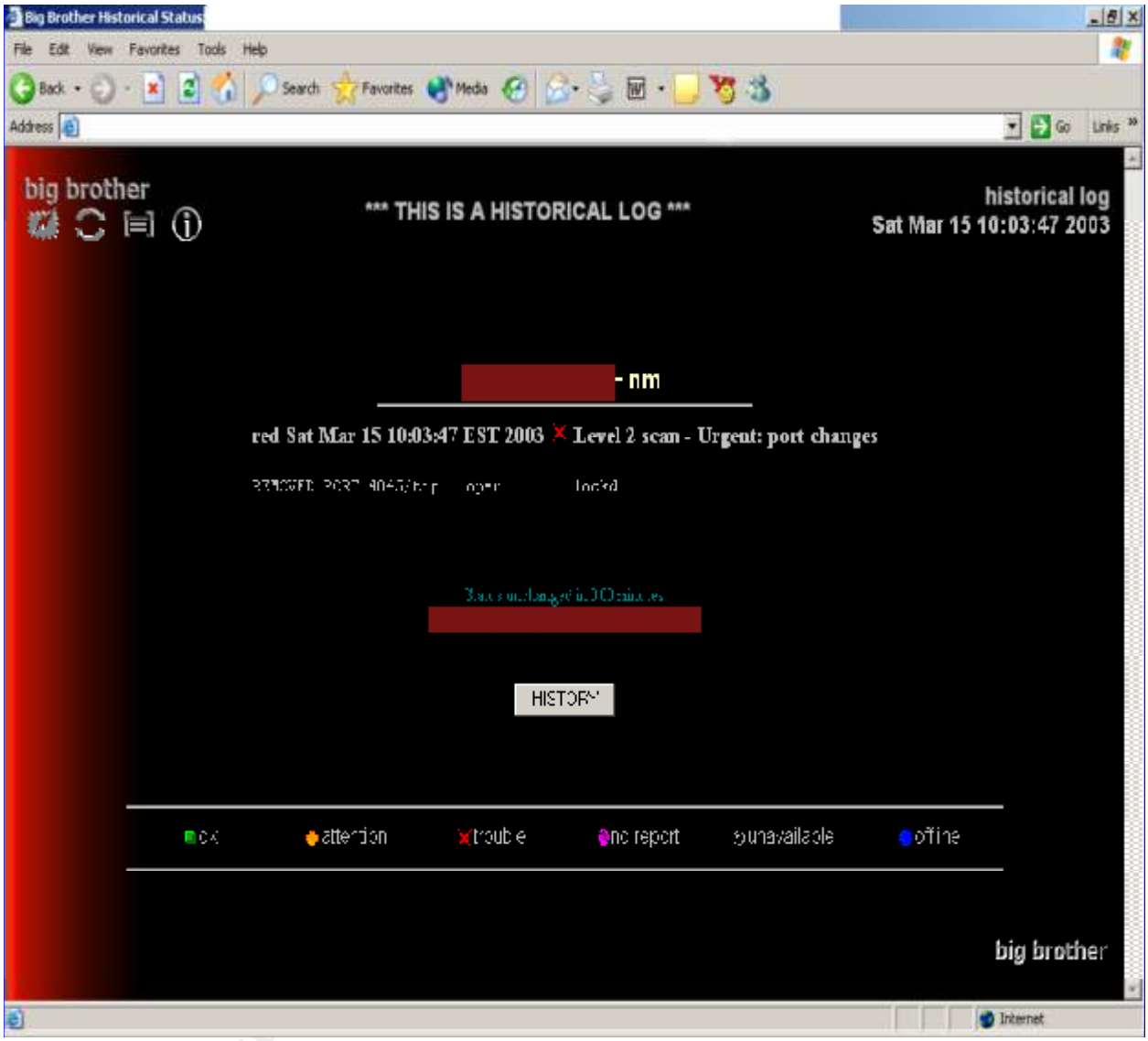


Figure 9. Shows a Big Brother Nmap monitor

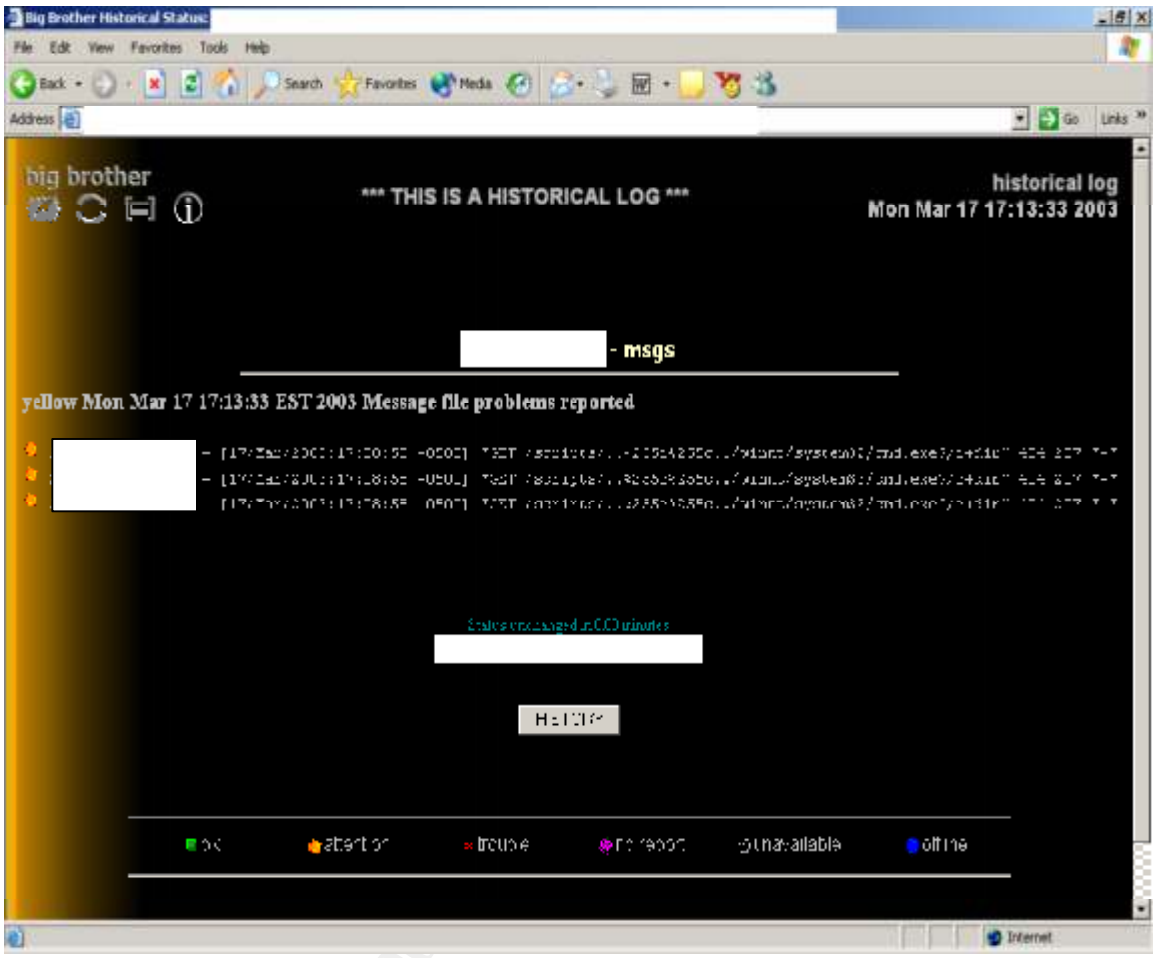


Figure 10. An attack against our web servers.

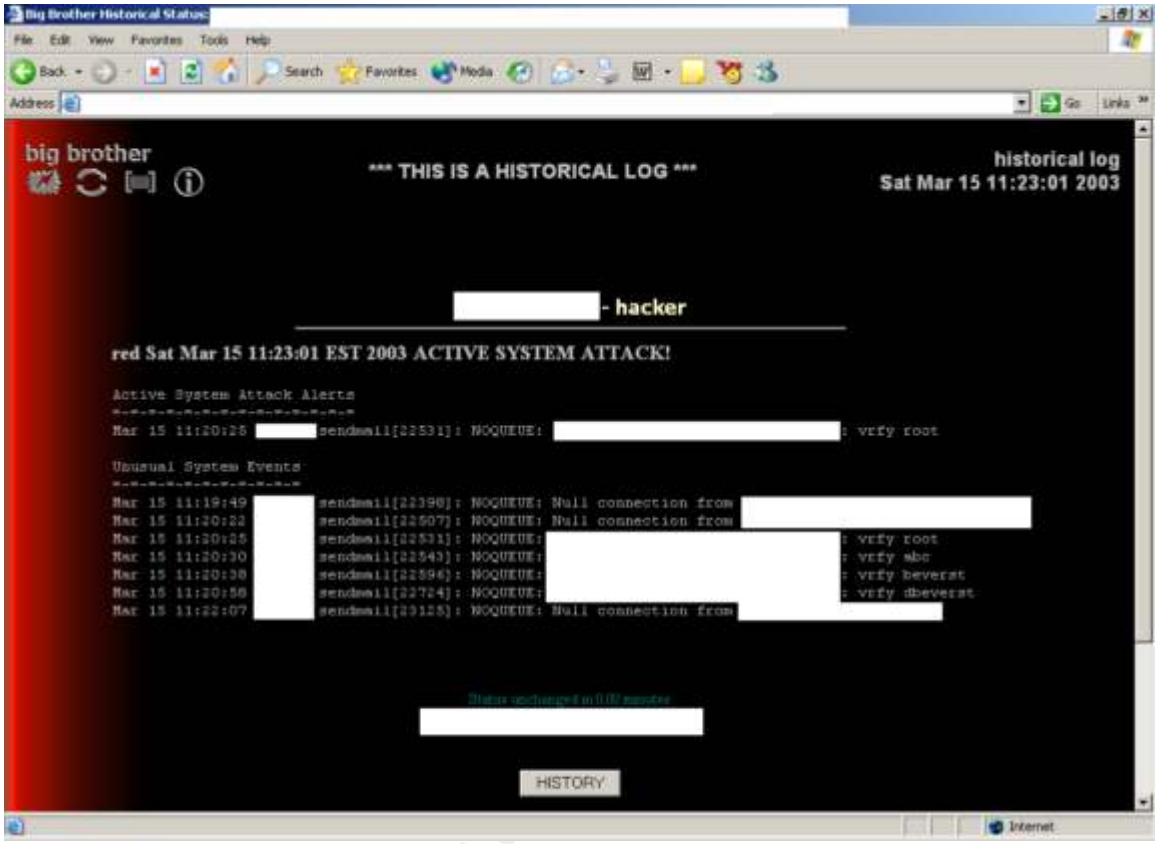


Figure 11: An attempt to compromise our servers via a sendmail attack.

Last Updated: March 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Boston Spring 2018	OnlineMAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced