GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Todd Chapman

GSNA Practical Assignment 2.0

Security Risk Assessment and Audit of an EMC SAN

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Research in EMC SAN Security Risk Assessment, Audit, Measurement Practice, and Control

System to be audited

Data are the most valuable assets of our company. The consolidation of our storage infrastructure, expansion of e-business initiatives, and increased access to corporate information and systems by business partners has made the confidentiality, integrity, and availability of those information assets an important area of concern. As internal corporate auditors we have been asked to audit the security of our organization's EMC SAN (Storage Area Network).

Audit Scope

The scope of this audit is information security risks and controls of the corporate EMC SAN. This includes physical access, administrative controls, and connections to other systems, logging, monitoring, and administrative procedures. We have no specific knowledge of SAN technology, so a great deal of research will be required to properly understand EMC SANs and the associated security issues.

The audit scope does NOT include security access to information on authorized hosts connected to the SAN; such as Unix or NT file permissions, NFS, or other types of application level information security controls. Operating system security hardening of management stations, service processors, and other systems connected to the SAN is not covered. Information security related to backup, recovery, and disaster recovery are also not within the audit scope.

The system is an EMC SAN comprised of two main components:

- 1 - EMC Symmetrix 8730 Enterprise Information Storage Solution, currently with 16.9 terabytes of disk space (maximum 24.8TB) and at microcode level 5567.

- 1 - EMC Connectrix DS-32M Fiber Channel (FC) switch with 32 universal Fiber Channel ports. Firmware version 3.02

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The following software packages are used to manage the SAN:

- EMC Control Center 4.3
  - Symmetrix Manager
  - ESN Manager
  - Connectrix Manager
- SymmIP 2.06
- SymmRemote 2.06

The role of the EMC SAN within the client organization is to provide enterprise-wide storage services, employing the following features of Storage Area Networks:

- ***Centralized/Consolidated*** storage allowing easier management of data and flexible provisioning of disk space to disparate computer systems.
- ***Scalable*** storage systems requiring less floor space, less power and cooling, and lower maintenance costs than distributed, host attached storage architectures.
- A ***highly redundant*** architecture guaranteeing data availability during hardware failures, component upgrades, and systems backups.
- ***Higher throughput*** than can be economically achieved on host attached storage devices.

The planning stage of the audit process revealed that the EMC SAN houses all types of corporate information including, human resources data, customer databases, and company financials. As an enterprise system, any department or project team can request SAN storage space. The SAN is expanded when needed through an enterprise budget, similar to a network infrastructure.

Although availability, confidentiality, and integrity of SAN information is critical, it is currently assumed that this will be achieved through SAN architectural features (redundancy, pre-emptive maintenance). Because there is currently no focus on security as a SAN requirement, no documented security processes or controls exist for the SAN to be audited against. Therefore the audit will concentrate on auditing existing system configuration and controls, using security principles and industry best practices as a benchmark. The audit report will concentrate on recommendations for implementation and documentation of SAN security policies, access controls and administrative procedures.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk Evaluation

There are three primary types of security risk associated with an EMC SAN, all of which have potentially serious financial consequences.

1. Information Theft

   Hackers, corporate employees, contractors, or vendors with server access may gain access to confidential information. This includes violation of the principle of least privilege for users who have legitimate access to limited areas of confidential information.

2. Denial of Service

   Hackers, corporate employees, contractors, or vendors may maliciously disrupt part or all SAN functionality.

3. Data Corruption

   Hackers, corporate employees, contractors, or vendors may maliciously corrupt data stored on the SAN.

There are four points of access, which might be exploited. Can you spot the potential attackers? (Figure 1):

1. Modem connections to Symmetrix and Connectrix service processors

   The service processor modem allows EMC support to remotely control the service processor, similar to PC Anywhere. While the modem is a distinct point of access, connections to the service processor through a modem are operationally equivalent to being physically located at the service processor. Thus the types of risks to information are the same for both modem connection to, and physical access to the service processors.

2. Network connections to Connectrix switch, Connectrix service processor, or SAN management station

   The Connectrix switch has an IP interface for some configuration functions, such as zoning. The Connectrix service processor uses an Ethernet IP interface to connect to the Connectrix switch. The SAN management station has both Fiber Channel and Ethernet connectivity to the SAN.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Symmetrix/Connectrix service processors (consoles)

   The service processors are laptops connected to the EMC devices. The Connectrix switch service processor allows zoning, as well as availability of the switch to be managed, SNMP configured, and devices added, modified, and deleted. The Symmetrix service processor allows EMC support engineers to monitor device errors and statistics.

4. Direct attach (via Fiber Channel) hosts

   Some SAN management, such as LUN masking is performed over Fiber Channel by a host directly attached to the SAN.

retains full rights

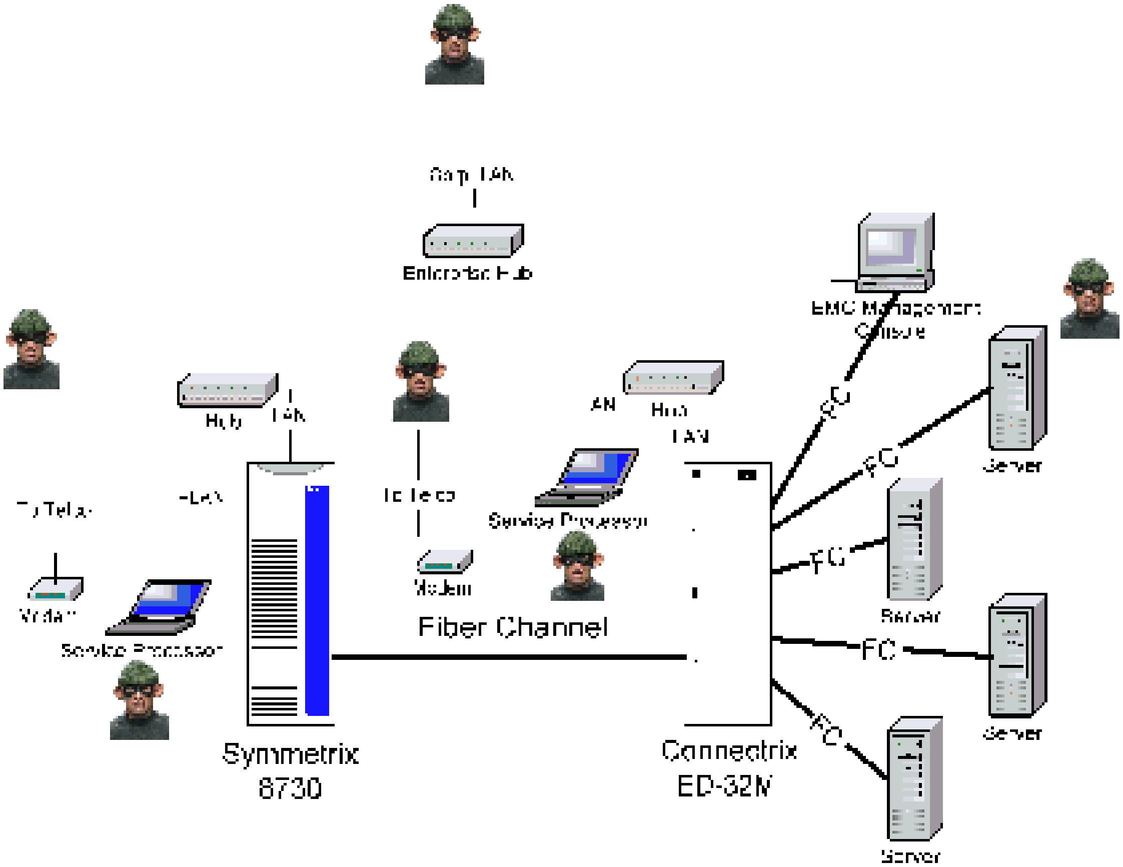


Figure 1 - EMC SAN Points of Access

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table 1 illustrates which types of risk are associated with which points of access.

		Information Theft	Denial of Service	Data Corruption
Service Processor	What Can Go Wrong?	Information cannot be stolen solely through compromise of the Symmetrix and Connectrix service processors.	Operation of the EMC can be interrupted from the system consoles.	Can data be written to specific disk areas?
	How Likely Is It?	Not possible.	Medium	Medium
	What are the consequences?	N/A	Loss of system access with likely financial impact.	Possibly undetected data tampering with possible financial impacts.
Network	What Can Go Wrong?	The SAN network connections cannot be used to transfer data from the SAN.	Operation of the EMC can be interrupted through the network using management software. For example, zoning changes.	Can data be written to specific disk areas?
	How Likely Is It?	Not possible.	High	Medium
	What are the consequences?	N/A	Loss of system access with likely financial impact.	Possibly undetected data tampering with possible financial impacts.
Direct attach	What Can Go Wrong?	Hosts directly attached to the SAN may be able to read secret data if zoning and controls are not in place.	Operation of the EMC can be interrupted through Fiber Channel connections. For example, changes in LUN masking.	Hosts directly attached to the SAN may be able to modify secret data if zoning and controls are not in place.
	How Likely Is It?	High	Low	High
	What are the consequences?	Unauthorized access to confidential data with possible financial impacts.	Loss of system access with likely financial impact.	Possibly undetected data tampering with possible financial impacts.

Table 1 - Risks and Points of Entry Matrix

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Current State of the Practice

A thorough research process was used to find resources to apply to the identification of risks and development of the audit checklists. Three specific types of resources were sought (in order of preference):

1. Existing audit procedures and checklists for EMC SANs.
2. Other information addressing security issues and controls of EMC SANs.
3. Information addressing SAN security issues in general, or information specific to other vendors SAN products whose concepts could be applied to the case of an EMC SAN.

No information specific to auditing EMC Storage Area Network security, or auditing SANs for any other vendors was found during the research process. Most documents of value addressed SAN security from an administrator's perspective, and a few addressed best practices of SAN security. All valuable sources that were found are documented below in the context of the method used to find them.

The following sources were used to find information to be applied in the creation of the audit checklists:

- **Internet Search Engines:**

  Google Web and Google Groups searches for the keywords, SAN and security turned up mostly documents describing security issues with Internet Protocol based SANs that are not addressed by this paper. A number of short articles discussing SAN security were found at searchstorage.com [17,18, 19], one including a reference to a Fiber Channel security paper at falconstor.com [16]. Most of these resources discussed SAN security at a very high level.

- **Specific searches of the EMC website:**

  Using the search feature of the EMC.com website yielded little information of value. EMC product documentation does a great job of explaining the value of SAN technology, but when, "information protection," is mentioned, it is always in the context of data availability and recovery during hardware failure, upgrades, and system backups. Information protection in the context of information theft, malicious data corruption, and intentional denial of service is not addressed.

- **Requests for information from the local EMC support engineer:**

  The EMC support engineer was the most valuable resource for EMC SAN security information. The EMC white paper, Best Practices for

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Managing a Secure Enterprise Storage Network [15] provided an excellent overview of security issues and controls for EMC SAN security (A version of this paper was eventually found on the EMC website). Also, the SymmIP [7] and SymmRemote [8] user's guides detailed the configuration and use of two key programs used by EMC service engineers to remotely connect to and control EMC service processors.

The problem with the SymmIP and SymmRemote documents is that they are marked, "EMC Confidential," making it a challenge to apply their valuable content without exceeding the intent of EMC to closely guard some details of system operation. This is unfortunate, as any determined hacker probably will find a source for this information, while legitimate customers must make repeated requests for this important information, and the development of meaningful EMC SAN security benchmarks by the security community is hampered in the name of security by obscurity.

- **EMC hardcopy product documentation:**

  All system documentation was available. The most valuable manuals covered zoning [2], LUN masking [1], and access controls [5].

- **CVE Dictionary Searches:**

  CVE (Common Vulnerabilities and Exposures) is a public (http://cve.mitre.org/) dictionary of known security issues. A search of CVE for the keywords EMC or SAN did not yield any know security issues that could be applied to this audit.

- **Requests for information from META Group:**

  META Group provides IT consulting services to its subscribers. With our corporate subscription I was able to request a phone conference with a META Group resource to discuss SAN security best practices. Through this conference I obtained a pre-published, draft copy of, SAN Fabric Security: Defending the Port(s) [20], which follows the typical META 2-page, high-level white paper format.

  This paper discusses management console security, authentication of devices in the SAN fabric, encryption of communication with the management console, SAN zoning, and security reporting. The paper focuses mostly on authentication within the SAN fabric, which is not applicable to this audit because EMC does not yet have an offering in this area.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **SANS Website and Reading Room:**

  The SANS website (http://www.sans.org) and SANS Reading Room (http://rr.sans.org/) were search for information on securing or auditing Storage Area Networks. No relevant information was found.

- **On-line searches for mailing lists discussing EMC SAN issues:**

  Internet search engines were used again, but these searches were focused on finding mailing lists and list archives for groups of people discussing EMC SAN issues. No SAN oriented lists were found.

- **Browsing large local bookstores for books on SANs:**

  Large chain bookstores usually have a few titles addressing Storage Area Networks. Four books addressing SANs were found at a local store. Three of them [12, 13, 14] did not mention SAN security in the table of contents or the index. In these books security was usually briefly mentioned in the areas discussing the concepts of *zoning* and *LUN masking*.

  The fourth book, IP SANs: A Guide to iSCSI, iFCP, and FCIP [10], was the only book that had a section specifically addressing security issues. While the book primarily addressed Internet Protocol (IP) based SANs, Fiber Channel SAN security was also discussed in order to put IP SAN security in the proper context. This book was also one of the rare resources that discussed the security issues of the SAN management interface, and not just the security of the Fiber Channel fabric.

- **EMC training classes:**

  Security is covered in EMC's, Basic Network Environment course. The course costs $1,125. Unfortunately there is no training budget for this audit.

In summary, there is no current practice for EMC SAN auditing. EMC SAN security focuses on information protection through zoning and LUN masking. In some resources SAN physical topology and management controls are also addressed.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Improving Current Methodologies and Techniques

As stated previously, there is no known audit checklist or procedure for EMC SANs. The process used to find the resources that do exist was described above. The most comprehensive document found on SAN security is the 12-page EMC document, Best Practices for Managing a Secure Enterprise Storage Network [15]. That document is one of the few sources found that focuses on SAN security, addressing more than the confidentiality and integrity offered by zoning and LUN masking.

The EMC best practices document also addresses the security of the physical topology of the SAN, levels of trust for systems connected to the SAN by Fiber Channel, and limiting/segregating the management controls of the SAN by device pool, access group, and function. No specific procedures or checklists are given, but other product specific white papers and manuals are referenced.

Still, there are areas that are virtually ignored in all the resources found. Monitoring and logging security violations is not addressed. The impact of corporate data classification standards on SAN design must be considered. Physical security is assumed, but no guidance is given on protecting data on disks that may be reassigned within the SAN, or disks that may leave the premises when EMC support personnel preemptively replace them. Discussion of the security of service processors and the modems connected to them is completely absent.

Through product literature, documentation, discussions with local SAN support staff and EMC support personnel, we will identify all the SAN points of access, risks that need to be addressed, and build audit checklists addressing all of the security controls that need to be in place. As we are auditors and not experts on SAN technology, it is possible that the result of our work will not be definitive, but we are confident that it will be an excellent starting point on which future auditors and security professionals will be able to build.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. EMC SAN Audit Checklists

Checklist Key

X. *The basic vulnerability/issue being addressed.*	
Reference	*An active link (cross-reference) to the source of the information and the page number if applicable.*
Control Objective	*What type of security control the checklist item addresses. Usually prevention, detection, or correction of a security incident.*
Likelihood	*The difficulty of an attacker exploiting the vulnerability if controls are not in place.* *Low: Very difficult to exploit* *Medium: Somewhat difficult to exploit* *High: Easy to exploit*
Consequence	*The amount of a damage, financial or to reputation that may result if the vulnerability is exploited.* *Low: Little or no damage* *Medium: Moderate but recoverable damage* *High: Possibility of serious damage to reputation or financially*
Risk → *Risk Level*	*Risk if the control is not implemented.*
Compliance	*Issues that affect compliance and mitigating controls that might be available.*
Subjective/ Objective Test	*Instructions on how to test that the control is implemented and is being enforced.*

Risk Level is calculated using the following table:

Likelihood	+	Consequence	=	Risk
High	+	High	=	High
High	+	Medium	=	Medium
High	+	Low	=	Low
Medium	+	High	=	Medium
Medium	+	Medium	=	Medium
Medium	+	Low	=	Low
Low	+	High	=	Low
Low	+	Medium	=	Low
Low	+	Low	=	Low

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There are a number of related systems and applications in the SAN that need to be audited. The audit checklists have been broken into logically related groups.

SymmIP (ver. 2.06) and SymmRemote (ver. 2.06) Checklist

version 1.0 August 24, 2002

A modem connected to each SAN service processor allows the SAN to dial EMC to report failing disks and other system diagnostics. In response EMC support personnel can dial into the SAN to maintain the system. SAN owners value this feature because it reduces administrative burdens and allows problems to be solved before they become emergencies.

SymmIP and SymmRemote are the programs that let EMC support personnel dial into and remotely control EMC service processors for SAN maintenance tasks. Controlling and monitoring remote access of the SAN is important for recognizing suspicious or unauthorized SAN access through the attached modems. The applications need to be audited to ensure that they are securely configured, log appropriate events, and are monitored for suspicious activity.

1. Is SymmIP disabled when service is not needed?	
Reference	[7] p. 2-6
Control Objective	Prevention of unauthorized access by disabling unneeded services.
Likelihood	Low
Consequence	Medium
Risk → Low	An unauthorized user could gain system access and cause a denial of service or modify access controls.
Compliance	Having SymmIP disabled prevents EMS support personnel from dialing in without authorization and gives hackers a much smaller window of activity to attempt system access. But this also prevents EMC from proactively fixing problems and would be inconvenient to corporate support staff.
Subjective Test	Ask corporate SAN support how this is handled, if they have a written policy, and if there are logs or other evidence of compliance.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Is the SymmIP enable/disable password known?	
Reference	[7] p. 2-6
Control Objective	Prevention of unauthorized access by disabling unneeded services.
Likelihood	Low
Consequence	Low
Risk → Low	Inability to lock down a system.
Compliance	Knowing the enable/disable password allows the SAN administrator to control when the service processor can be accessed by modem.
Subjective Test	Ask local SAN administrator if enable/disable password is known. Where is it stored and how is access to it controlled?

3. When SymmIP is disabled SymmRemote is automatically set to accept modem connections but RAS should be set to start manually. Is this working correctly?	
Reference	[7] p. 2-8
Control Objective	Prevention of unauthorized access by disabling unneeded services.
Likelihood	Low
Consequence	Medium
Risk → Low	Disabling SymmIP might accidentally enable RAS which has weaker mechanisms for authenticating users.
Compliance	Accidentally enabling RAS may make it easier for unauthorized persons to access the service processor.
Objective Test	1) Disable SymmIP a) At the service processor, click on the *Start* menu. b) Click on *Settings*. c) Click on *Add/Remove Programs*. d) Locate SymmIP in the list and double-click on it. e) Enter the enable/disable password and click *OK*. 2) See if RAS service is set for manual start a) At the service processor, click on the *Start* menu. b) Click on *Settings*. c) Click on *Control Panel*. d) Double-Click on *Services*. e) Check that *Remote Access Server* is set for manual start or is disabled.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. Are SymmRemote connections and file transfers logged?	
Reference	[8] p. 5-4
Control Objective	Detection of a security incident using an audit trail. The SymmRemote logs record: user, time, connection length, and file copies.
Likelihood	Low
Consequence	Low
Risk → Low	An attacker who has gained access to SymmRemote and is doing reconnaissance may go undetected. This could lead to the early warning signs of an attack being missed.
Compliance	All available logging should be enable even if it is not periodically reviewed to that they are available when a security incident occurs.
Objective Test	In the SymmRemote host's window, select the *Settings* menu item and then the *General* tab. Confirm that *Log connections* and *Log file transfers* are set.

5. Are SymmRemote logs periodically review by local support staff?	
Reference	none
Control Objective	Detection of a security incident through log monitoring.
Likelihood	Low
Consequence	Low
Risk → Low	An attacker who has gained access to SymmRemote and is doing reconnaissance may go undetected. This could lead to the early warning signs of an attack being missed.
Compliance	Failure to log SymmRemote activity makes it difficult to detect suspicious system activity, but it takes significant time to correlate these logs to other information sources. Efforts may be more effective elsewhere.
Subjective Test	Ask corporate SAN support how this is handled, if they have a written procedure, and if there are logs or other evidence of compliance.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. Are stronger case-sensitive passwords, reasonably low logon validation options, and logon disabling options configured in SymmRemote?	
Reference	[8] p. 5-3
Control Objective	Prevention of a security incident by maintaining strong authentication controls.
Likelihood	Medium
Consequence	Medium
Risk → Medium	Weak authentication controls increase the chance of a system compromise.
Compliance	There is not reason while these controls should not be implemented.
Objective Test	In the SymmRemote host's window, select the *Settings* menu item and then the *Logon Security* tab. • Confirm that *Make passwords case sensitive* is set. • Confirm that *Time allowed for logging on* is set to no more than 5 minutes. • Confirm that *Logon attempts per call* is not greater than 5. • Confirm that *Disable logons after* is enabled and set for no more than 10 failed attempts. • Confirm that *Re-enable logons after* is set to at least 15 minutes. These setting are difficult to test because the SymmRemote client would be required and it is not distributed to EMC customers.

7. Is SymmRemote set to require data encryption?	
Reference	[8] p. 5-5
Control Objective	Prevention of confidential data disclosure by using encryption.
Likelihood	Low
Consequence	Low
Risk → Low	If connection is made over insecure network the data should be encrypted or an attacker may intercept authentication information and sensitive data.
Compliance	We know of no reason why the SymmRemote feature should not be enabled.
Objective Test	In the SymmRemote host's window, select the *Settings* menu item and then the *Security* tab. Confirm that *Require data encryption* is set.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8. Is the SymmRemote Master Password set?	
Reference	[8] p. 5-6
Control Objective	Segregation of duties by ensuring that only authorized SAN support personnel can alter security settings.
Likelihood	Low
Consequence	Low
Risk → Low	If the Master Password is not set an attacker could temporarily disable security settings so that his actions are not logged and the security incident may be missed.
Compliance	Setting the Master Password will require it to be documented and kept secret among the SAN administrators.
Objective Test	In the SymmRemote host's window, select the *Settings* menu item and then the *Security* tab, and then click on *Master Password*. Confirm that the password fields are not blank. If the fields are blank, attempt to change a SymmRemote security setting. If the change is successful the Master Password is not set.

9. Can a remote attacker easily dial in to the service processor and try to brute force passwords?	
Reference	None
Control Objective	Prevention of a security incident making sure it is not trivial for an attacker to dial into the service processor.
Likelihood	Low
Consequence	Med
Risk → Low	If a remote attacker can dial in and attempt authentication he may be able to cause a denial of service by shutting down components of the SAN
Compliance	RAS or simple terminal protocols should not be used for remote access.
Objective Test	Use a terminal (such as Windows Hyperterminal) to dial the EMC modem. Does it answer? Are you able to get a prompt for authentication?

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Connectrix DS-32M, Connectrix Manager (version 4.01), and Connectrix Service Processor Checklist

version 1.0 August 24, 2002

The Connectrix switch is managed through its connected service processor, or through embedded telnet and web servers. This checklist covers the security configuration of the Connectrix, its service processor, and the Connectrix Manager software running on the service processor. Default passwords need to be changed and unnecessary services should be disabled.

10. Ensure that the default Administrator password for the web server embedded in the DS-32M has been changed.	
Reference	[9] p. D-1
Control Objective	Prevention of a security incident by changing default passwords.
Likelihood	High
Consequence	High
Risk → High	An unauthorized user could reconfigure the switch causing a denial of service.
Compliance	It might be argued that this is not necessary if the ED-32M is on a private network, but the password should be changed for defense in depth. Even if the embedded web server is disabled the password should be change in case the web server is accidentally re-enable.
Objective Test	Using a computer on the same network as the DS-32M, type the switches IP address in a web browser. When prompted for a username and password, enter ‘Administrator’ and ‘password’ respectively. If authentication succeeds the password has not been changed.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

11. Ensure that the default Operator password for the web server embedded in the DS-32M has been changed.	
Reference	[9] p. D-1
Control Objective	Prevention of a security incident by changing default passwords.
Likelihood	High
Consequence	High
Risk → High	An unauthorized user could view switch configuration.
Compliance	It might be argued that this is not necessary if the DS-32M is on a private network, but the password should be changed for defense in depth. Even if the embedded web server is disabled the password should be change in case the web server is accidentally re-enable.
Objective Test	Using a computer on the same network as the DS-32M, type the switches IP address in a web browser. When prompted for a username and password, enter 'Operator' and 'password' respectively. If authentication succeeds the password has not been changed.

12. Is the Connectrix web server enabled or telnet enabled?	
Reference	[9] p. 1-16
Control Objective	Prevention of a security incident by disabling unnecessary services.
Likelihood	Medium
Consequence	Low
Risk → Low	An attacker could reconfigure the switch causing a denial of service or as an initial step to a more significant attack.
Compliance	There is no reason for these services to remain enabled after the Connectrix is initially configured, as it will be managed through other means. It may temporarily be re-enabled when necessary.
Objective Test	• Start Connectrix Manager • Click on DS32M • In Product Manager click on Configure • Is enable web server checked? • Is enable telnet server checked? • Can you telnet to port 80 on the Connectrix from its service processor?

© SANS Institute 2000 - 2002, Author retains full rights.

13. Has Connectrix Manager default Administrator password been changed?	
Reference	[4] p. 2-2
Control Objective	Prevention of a security incident by changing default password.
Likelihood	High
Consequence	High
Risk → High	An attacker on the same network as the Connectrix service processor could change system settings, causing a denial of service.
Compliance	The default password must be changed.
Objective Test	At the Connectrix service processor start Connectrix Manager. Try logging in with the default username of ‘Administrator’ and the default password of ‘password’.

14. Is Microsoft Personal Web Services enabled on the service processor?	
Reference	Identified by inspection of the Connectrix service processor.
Control Objective	Prevention of a security incident by disabling unnecessary services and making management software less accessible.
Likelihood	High
Consequence	High
Risk → High	Microsoft Personal Web Server is easily compromised, allowing an attacker to control the service processor with the potential of a denial of service or destruction of data. Also, this web server allows Connectrix Manager software to be downloaded, which could be used to attempt remote compromise of the system.
Compliance	This service should not be enabled. SAN administrators should make the management software available only to authorized users through a corporate file share with security restrictions. Even if the service processor is on a secured management LAN, this service should be disabled as an additional layer of security.
Objective Test	Using a web browser on a PC connected to the service processor LAN, type the service processor’s IP address into the browser address bar. Any web page returned indicates that the service is running.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

15. Are Connectrix Manager Access restrictions used to limit what IP addresses can remotely connect to Connectrix Manager?	
Reference	[4] p. 3-13
Control Objective	Prevention of a security incident through network based access controls.
Likelihood	Medium
Consequence	High
Risk → Medium	If Connectrix Manager access controls are not enabled at attacker will have less difficulty in remotely connecting to Connectrix Manager on the service processor.
Compliance	These access controls should be set to as few trusted hosts as possible.
Objective Test	Start Connectrix Manager, select *Configure*, and then select *Session Options*. Ensure that *Specify remote network addresses* is set and contains only a few trusted hosts. Attempt to connect to Connectrix Manager from trusted and un-trusted hosts and make sure that connections are only accepted from trusted hosts.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ESN Manager (version 4.3) Checklist

version 1.0 August 24, 2002

Zoning and LUN masking are the common SAN security areas of focus, controlling which devices can communicate, and what disks can be accessed. Symmetrix access controls limit configuration and management of Symmetrix resources.

Zoning is often used as a SAN manageability tool, but is also critical in keep SAN data confidential.

> **The typical security concerns of Fiber Channel SANS are not focused on penetration from the outside, but segregation of storage resources within the SAN… Fiber Channel enforces basic separation of applications and departments within the SAN through zoning. (Clark, p. 168)**

16. What type of zoning strategy is in use?	
Reference	[15] p. 7
Control Objective	Prevention of confidential data disclosure by enforcing the principle of lease privilege.
Likelihood	Low
Consequence	Low
Risk → Low	A zoning strategy should be defined that meets the manageability and security requirements of the organizations. Without a defined zoning strategy there is no way to ensure that the zoning configuration enforces the organizations security requirements.
Compliance	Strategies that involve port zoning make SAN manageability less flexible and may not be necessary in shared environments where multiple customers may connect to the same SAN switch.
Subjective Test	Ask the SAN administrator what zoning strategy is in use. Is it documented? Is the zoning strategy designed only with manageability, security, or both in mind? (If any port zoning is in use it is configured

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

17. Analyze zoning configuration.	
Reference	[2] p. 4-3
Control Objective	Prevention of confidential data disclosure by ensuring that the zone strategy (implicit or implied) is in use.
Likelihood	Low
Consequence	Low
Risk → Low	Accidental disclosure of confidential data may result if the zoning strategy is not followed.
Compliance	Generally the zoning strategy must be followed. However in some configurations multiple systems may need access to the same disk. As long as zoning is configured to allow the minimum necessary communication between systems risks will be minimized.
Objective Test	*Graphical method:* Ask the SAN administrator to use ESN Manager to list the zones and explore each zone to see its members. *Command line method:* Ask the SAN administrator to use the FiberZone command line interface to list all zones in the FiberZone database: **`fzone zone –list`** For as many zones as practical, have the SAN admin. list the members of each zone: **`fzone zone –info {`** ***`zone_name`*** **`|`** ***`zone_id`*** **`}`** *Questions to ask:* Have the SAN administrator explain what each member of the zone is. Does each zone follow the zoning strategy? For example, for Single HBA Zoning, does each zone have only one Host Bus Adapter as a member? Does each zone have the minimum number of members that are operationally necessary?

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

18. Is the zoning configuration in the FiberZone database being enforced on the SAN?	
Reference	Testing method identified by Unix administrator
Control Objective	Prevention of confidential data disclosure by ensuring that the zone strategy (implicit or implied) is in effect.
Likelihood	Medium
Consequence	High
Risk → Medium	Accidental disclosure of confidential data may result if the zoning strategy is not followed.
Compliance	The configuration in the zoning database must be confirmed by this test.
Objective Test	Using a Solaris server with a JNI Fiber Channel card to the EMC modify sd.conf to look for all LUNs on all possible targets (0-255). Then, modify the JNI conf file to automap all visible devices. Run the *format* command as root before and after the modification (which require a reboot). If additional SAN devices appear from other zones then the zoning configuration is not being enforced properly.

19. If port zoning is part of the zoning strategy, ensure that it is implemented.	
Reference	[1] p. 3-8
Control Objective	Prevention of confidential data disclosure by ensuring that the zone strategy (implicit or implied) is in use.
Likelihood	Low
Consequence	High
Risk → Low	Accidental disclosure of confidential data may result if the zoning strategy is not followed.
Compliance	Port zoning may not be used if the impact to SAN manageability is too great.

Objective Test	Ask the SAN administrator to use the Volume Logix command line interface to list all zones in the FiberZone database:
	`fpath lsdb`
	For each FA port in the VCM database, the attached WWNs will be listed. If port zoning (a.k.a. SID Lockdown) is in effect for any WWN a note will be printed under the WWN number. For example:
	`*NOTE: The SID value 123456 has been locked down for this WWN on this FA*`

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

LUN Masking (a.k.a. Storage Device Masking) provides another level of security for storage devices. Even with zoning in place, two systems zoned to the same FA port on a storage array can access the same devices. Volume Logix, part of ESN Manager enables access control to Symmetrix volumes.

20. Is LUN Masking used as an additional layer of access controls for Symmetrix devices?	
Reference	[15] p. 10
Control Objective	Prevention of confidential data disclosure by ensuring that LUN masking is in use.
Likelihood	Low
Consequence	High
Risk → Low	If LUN masking is not enabled, hosts attached to the same FA port could access each other's confidential data.
Compliance	It is possible that a host may need access to all available devices on a SAN port, making LUN masking unnecessary for some zones. However explicitly defining what devices should be available is recommended as an additional layer of security in case more devices are added to the port in the future.
Objective Test	Ask the SAN administrator if LUN masking is in use for all zones. If the answer is yes subsequent audit steps will verify this.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

21. Is LUN masking enforced at the server level or storage device level?	
Reference	[15] p. 10
Control Objective	Prevention of confidential data disclosure by ensuring that LUN masking is controlled at the storage device level where security can be more easily controlled than in a distributed system.
Likelihood	Medium
Consequence	High
Risk → Medium	If LUN masking is not controlled at the storage device level, the security at each Fiber Channel attached host becomes a part of Symmetrix device security, increasing the chances that confidential information will be accessible by unauthorized individuals.
Compliance	Enforcing LUN masking at the server level would rely on the security of each server, which is much more difficult to control and may be outside the responsibilities of the SAN administrator. LUN masking should be enforced at the storage device level.
Objective Test	*Graphical method:* Have the SAN administrator use ESN Manager to browse hosts in the SAN topology map. Disks the Volume Logix allow the selected system to write to will be outlined in blue. Disks that are being masked from the system are not outlined. *Command line method:* On the SAN management station list the Volume Logix database device name: **`fpath lshostdev`** One raw device will be listed for each path to the VCMDB. If no devices are listed, Volume Logix is not enabled. Either LUN masking is enforced at the server level or it is not in use at all. Server level security is out of scope for this audit. The test for this item is covered by the test for item 18.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

22. Is the VCMDB Access feature enabled?	
Reference	[1] p. 1-5, [15] p. 11
Control Objective	Prevention of confidential data disclosure and ensuring system availability by securing the database that enforces LUN masking.
Likelihood	Medium
Consequence	High
Risk → Medium	If the Volume Logix database is not secured, a user on any Fiber Channel attached system with a copy of Volume Logix or ESN Manager could alter the database, allowing unauthorized access to SAN data or denying legitimate access to Symmetrix volumes.
Compliance	The VCMDB Access feature must be enabled to prevent an attacker on any Fiber Channel connected host in the SAN from modifying storage device access rights.
Objective Test	Setting and checking this is not documented in the Volume Logix manual. Directed to EMC support.

23. If LUN masking is enabled at the device level, are hosts only permitted to access the minimum required Symmetrix devices?	
Reference	[1] p. 2-15
Control Objective	Prevention of confidential data disclosure and corruption by enforcing Symmetrix access controls at the device level.
Likelihood	Medium
Consequence	High
Risk → Medium	Systems connected to the same Symmetrix FA port could read or write each other's confidential data.
Compliance	It is possible that a host may need access to all available devices on a SAN port, making LUN masking unnecessary for some zones. However explicitly defining what devices should be available is recommended as an additional layer of security in case more devices are added to the port in the future.
Objective Test	Using the same testing method from checklist item **Error! Reference source not found.**, see if additional devices appear from within the zone. If they do this is an indication that LUN masking is not operating as configured.

© SANS Institute 2002, Author retains full rights.

Symmetrix Access Controls determine what privileges hosts attached to the SAN will have. Without proper access controls other Symmetrix security controls could be rendered ineffective.

24. Has the default ESN manager password been changed?	
Reference	[3] p. 2-3
Control Objective	Prevention of confidential data disclosure and maintaining data availability by controlling access to ESN manager.
Likelihood	Medium
Consequence	High
Risk → Medium	An attacker who gains access to the management station may use ESN Manger to alter configuration of the SAN, possibly accessing, altering, or deleting confidential data.
Compliance	The ESN Manager password should be changed even though command line programs on the management station with similar functionality require no authentication.
Objective Test	Start ESN Manager and try to log in with the default password of '2P%0'.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

25. Is Symmetrix access control administration limited to an administrative group from the management station?	
Reference	[5] p. 2-7
Control Objective	Prevention of a security incident by limiting management functions to the SAN management station.
Likelihood	Low
Consequence	High
Risk → Low	The default access controls may allow administration of access controls from any SAN host, allowing any host administrator unlimited access to storage devices.
Compliance	Access controls should be implemented to, at a minimum, allow SAN Fiber Channel based administration from designated management stations.

Objective Test	**`symacl list –v`**
	Check that only the admin group has ADMIN rights and that only the management station is a member of the admin group. To get the unique access ID for the management station run:
	`symacl –unique`
	This can be tested by loading ESN Manager on SAN host that is not authorized to administer Symmetrix access controls and trying to modify access control rights. Use the SYMCLI grant or remove commands to modify access rights. [5] p. 2-14

26. Does each admin user have a unique user access PIN?	
Reference	[5] p. 2-8
Control Objective	Detection of a security incident by having each employee use a unique PIN when performing symacl operations. This allows the system changes to be traced back to an individual during the investigation of a security incident.
Likelihood	Low
Consequence	Medium
Risk → Low	Correction of a security incident by being able to attribute SAN configuration changes to a specific person.
Compliance	Users must be required to identify themselves in a unique way when performing SAN management functions.
Subjective Test	Ask the SAN administrator how this is handled. If possible, have the SAN administrator demonstrate multiple employees performing symacl commands using different PINs.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

27. Are Symmetrix access controls used to limit specific hosts to managing specific devices with the least amount of privilege necessary?	
Reference	[5] p. 2-11, p. 2-17, p. 2-20
Control Objective	Prevention of a security incident by enforcing least privilege on Symmetrix device configuration.
Likelihood	Low
Consequence	Medium
Risk → Low	SAN hosts may be able to perform management on more than the minimum necessary devices.
Compliance	These controls may not be necessary in a single customer environment. However different departments within the same company often need to be considered as different customers with a shared SAN.
Objective Test	From the management station: **symacl list –v** **symacl –sid *SymmID*|ALL list –accgroup** **symacl –sid *SymmID*|ALL list –accpool** **symacl –sid *SymmID*|ALL list –acl** The host access ID of the host you are on can be checked with the command: **symacl -unique** Check rights, groups, and pools. Have Grant/Deny access strategy explained by admin. Does the 'unknown' access ID exist? Try to perform an operation from a host that should not have that privilege. Was the operation successful?

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

28. What Grant/Deny access strategy is in use?	
Reference	[5] p. 2-20 – 2-23
Control Objective	Prevention of a security incident by having a defined access control strategy that can be enforced in daily operations.
Likelihood	Low
Consequence	Low
Risk → Low	If a defined access control strategy does not exist then proper access controls are difficult to enforce and exceptions will be more difficult to detect on subsequent audits.
Compliance	An access control strategy must be in place.
Subjective Test	Do all hosts have the ALL access right to unregistered nodes? Do all hosts have the ALL access right to non-pooled devices? Is “General Absolute Control Strategy” used? Have the SAN administrator explain the access control strategy. Does is reflect any of the strategies described in the Access Control Product Guide?

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SAN Physical Topology and Physical Security Checklist

version 1.0 August 24, 2002

Outside of the SAN fabric, the primary security concern is unauthorized management of the SAN which can be accomplished from the service processors (covered above), or from the Local Area Network that the SAN is attached, through official or rouge management consoles.

The architecture of the SAN and its management network must enforce proper restriction of SAN management.

29. How is physical access to the SAN devices and service processors controlled?	
Reference	[15] p. 6
Control Objective	Prevention of a security incident by controlling physical access to the SAN devices and service processors.
Likelihood	Low
Consequence	High
Risk → Low	An attacker may remove information from, or destroy the SAN. Access to the service processors may allow access controls to be changed.
Compliance	There should be at least one layer or auditable physical security. Two or more layers are preferable.
Objective Test	Have the SAN administrator demonstrate all the layers of physical security and how they work.

30. Are the service processors screens locked when not in use?	
Reference	[15] p. 6
Control Objective	Prevention of a security incident by preventing local access to the operating system on the service processors.
Likelihood	Low
Consequence	High
Risk → Low	An attacker that gains local access to the service processors can subvert all network based access controls.
Compliance	This is a valuable layer of additional security for the service processors but could cause problems for EMC support engineers trying to perform systems maintenance over SymmRemote or locally during off hours.
Objective Test	When performing the audit ask for a tour of the data center and request to see the service processors. If the screen is not locked ask the SAN administrator if someone is currently performing local administration.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

31. Are the Ethernet interfaces for the SAN, including the Symmetrix, Connectrix, service processors, and management (control) station on a private network?	
Reference	[15] p. 6
Control Objective	Prevention of a security incident by tightly controlling network access to all SAN components.
Likelihood	Medium
Consequence	High
Risk → Medium	Multiple management interfaces are exposed to attack if they are not protected on a private management network.
Compliance	Some mitigating controls exist but a private network is strongly recommended by EMC.
Objective Test	Ask the SAN administrator for a SAN network diagram. Try to ping SAN components from a host on the corporate LAN. Does an nmap scan of the Connectrix switch reveal any open ports?

32. If the SAN is on a private network, how is it connected to the corporate LAN? If by firewall/VPN what rules are in place?	
Reference	[15] p. 6
Control Objective	Prevention of a security incident by tightly controlling network access to all SAN components while allowing a path for remote administration.
Likelihood	Medium
Consequence	High
Risk → Medium	Prevention of a security incident by protecting the SAN LAN from the corporate LAN.
Compliance	Some path between the corporate LAN and the SAN private LAN is required for management. A firewall with VPN capability is needed to protect this connection.
Objective Test	Try to nmap the SAN LAN from the corporate LAN. If a firewall exists request a copy of the firewall rules for review. Are minimum necessary connections allowed through the firewall?

© SANS Institute 2000 - 2002, Author retains full rights.

33. Is EMC Control Center installed in a 1, 2, or 3 tier configuration?	
Reference	[6] p. 1-5
Risk → na	Not applicable
Likelihood	Not applicable
Control Objective	The Control Center configuration will help determine necessary security controls.
Consequence	Not applicable
Compliance	Any configuration is acceptable as long as proper controls are in place.
Subjective Test	Ask the SAN administrator to describe the Control Center configuration.

34. Is a nethost file used to control access to EMC Control Center?	
Reference	[6] p. 3-6
Control Objective	Prevention of a security incident by limiting access to Control Center based on IP address.
Likelihood	Low
Consequence	Medium
Risk → Low	An attacker may remotely perform SAN management and alter security controls.
Compliance	A management LAN and firewall may mitigate this risk.
Objective Test	Check that the netconfig file exists on the management station. On Windows it should be located at C:\Progrma Files\EMC\SYMAPI\config\nethost. Does it list the minimum required nodes and addresses for remote (tier 2 or tier 3) functionality? To test the effectiveness of the nethost file load a Control Center application on another host on the network now specified in the nethost file and see if remote management is allowed from that host.

© SANS Institute 2002, Author retains full rights.

35. Does EMC support have un-escorted access to the building, data center, and SAN? If so what hours?	
Reference	none
Control Objective	Prevention of a security incident by maintaining tight control of physical SAN access.
Likelihood	Low
Consequence	Low
Risk → Low	A rouge EMC engineer could remove confidential data from the SAN.
Compliance	Not applicable
Subjective Test	Ask the SAN administrator how EMC support Engineer physical access to the SAN is controlled.

36. Is EMC support access to the building logged and does the SAN security administrator periodically review the logs?	
Reference	none
Control Objective	Detection of a security incident by monitoring unaccounted EMC engineer access to the data center.
Likelihood	Low
Consequence	Low
Risk → Low	A rouge EMC engineer may be able to remove confidential data from the SAN undetected.
Compliance	Reviewing and correlating logs is time consuming and might not be performed very often (unless you have an intern). A motivated attacker could probably justify any system access.
Subjective Test	Ask the SAN administrator for an example log and evidence that the log was reviewed an correlated with systems logs.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Data Classification and Control Checklist

version 1.0 August 24, 2002

Not all data are created equal. Security controls for public data are different than those required for top-secret data. Within a SAN environment disks may be reused for different purposes over time. The same disk may be used multiple times for different projects, involving different departments, and data of various sensitivities.

Also, in an EMC environment, when a disk begins to fail it is preemptively replaced by EMC support, often without the customer's knowledge. This level of service is often valued, but creates a situation where sensitive corporate data may leave its control. Applying corporate data classification models and policies to SAN storage is essential in ensuring that corporate assets are appropriately protected.

This checklist is designed to ensure that data is properly classified as mandated by policy, protected with appropriate controls and procedures, and monitored to make sure data remains within corporate control.

37. Does the organization have a data classification policy?	
Reference	none
Control Objective	Prevention of confidential data disclosure by enforcement of security controls mandated by policy.
Likelihood	Medium
Consequence	Medium
Risk → Medium	Data can only be protected properly if it is first evaluated for level of confidentiality and the consequences of loss of control of the data.
Compliance	Without a data classification policy the SAN administrator is forced to treat all data equally.
Objective Test	Ask the SAN administrator for a copy of the corporate data classification model. Does it specify different data levels and what controls are required for each level? Are SAN specific controls included?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

38. When SAN disk space is allocated to a server is the organization's data classification model used to determine special requirements for data handling by the SAN administrator or data owner?	
Reference	none
Control Objective	Prevention of confidential data disclosure through accurate labeling of data.
Likelihood	Low
Consequence	Medium
Risk → Low	The risk is that data will not be designated using the corporate data classification model, and consequently not be protected with appropriate security controls.
Compliance	Without proper classification data cannot be protected in accordance to its sensitivity.
Objective Test	Ask the SAN administrator for documents illustrating tracking of classification of data on each disk. Is it sufficient to identify which disks require which types of controls?

39. Are separate SAN device pools used to store data of different data classifications so that access controls can be applied to device pools?	
Reference	[5] p. 2-11
Control Objective	Prevention of confidential data disclosure by enforcing least privilege and segregation of duties.
Likelihood	Low
Consequence	Medium
Risk → Low	Without application of access controls to device pools, systems attached to the SAN may have access to devices without need, or may have more administrative control than necessary, possibly leading to a breach of confidentiality.
Compliance	Without the use of device pools it will be difficult to track which devices have store data of each classification.
Semi-Objective Test	Have the SAN administrator list device pools, access groups, and access control entries from the management station with the command: **`symacl list –v`** Verify that device pools and access groups have been created. Do access control entries give different access groups different rights to the same pool? Have the SAN administrator explain how the access control entries enforce least privilege and segregation of duties.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

40.	Is the SAN administrator notified each time a failing disk is replaced by EMC and are there data handling and disposal agreements between the corporation and EMC?
Reference	none
Control Objective	Detection of a security incident through log monitoring and correlation.
Likelihood	Medium
Consequence	High
Risk → Medium	The corporation will loose control of confidential data.
Compliance	The SAN administrator must be notified each time a disk is removed from the premises. A procedure for wiping disks before removal should be in place. An agreement covering these procedures should be created between the corporation and EMC.
Objective Test	Ask SAN administrator for e-mail or logs demonstrating awareness of disk replacements. Are these correlated with SAN logs or building security access logs for EMC personnel?

41.	Are disks with highly confidential data formatted before reuse?
Reference	none
Control Objective	Prevention of confidential data disclosure through proper data disposal.
Likelihood	Low
Consequence	Medium
Risk → Low	Computer forensics tools could recover data on disks reassigned within the SAN.
Compliance	Disks re-used within the SAN may have residual sensitive data from a previous use. All disks should be formatted before reuse.
Objective Test	Ask the SAN administrator for process documentation describing when and how disks must be reformatted. Are there logs indicating that disks are routinely formatted?

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

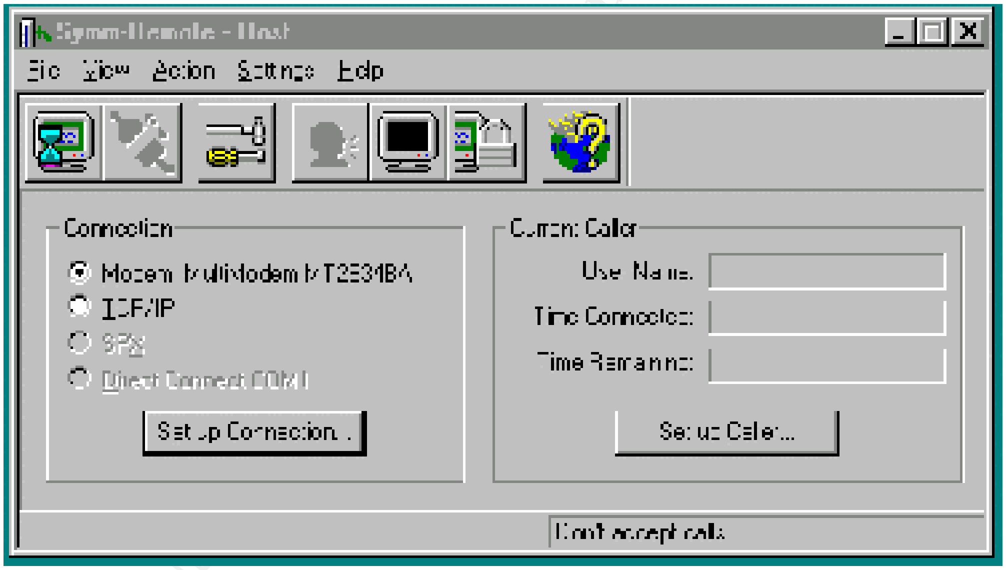
3. Audit Results

SymmIP (ver. 2.06) **and SymmRemote** (ver. 2.06) **Checklist Results**

version 1.0 August 24, 2002

1. Is SymmIP disabled when service is not needed?

SymmIP is not installed on the service processors. Figure X shows that SymmIP is not listed in Add/Remove Programs. Therefore it is not installed. Also Figure 2 shows that SymmRemote is configured to accept modem connections. If SymmIP were being used SymmRemote should be set to accept TCP/IP connections.



Connection
● Modem MultiModem MT2834BA
○ TCP/IP
○ SPX
○ Direct Connect COM1

Current Caller
User Name:
Time Connected:
Time Remaining:

Can't accept calls

Figure 2 – SymmRemote

2. Is the SymmIP enable/disable password known?

Not applicable. SymmIP is not installed.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. When SymmIP is disabled SymmRemote is automatically set to accept modem connections but RAS should be set to start manually. Is this working correctly?

Not applicable. SymmIP is not installed.

4. Are SymmRemote connections and file transfers logged?

Figure 3 shows that SymmRemote connections and file transfers are logged.

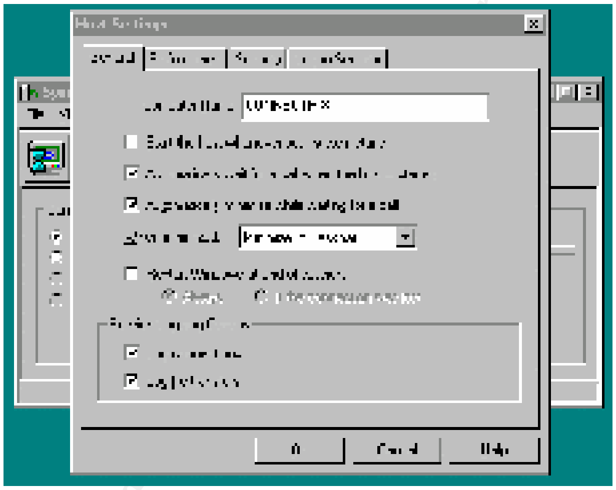


Figure 3 - SymmRemote Host Settings

5. Are SymmRemote logs periodically review by local support staff?

SymmRemote logs are not reviewed according to the SAN administrator.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6. Are stronger case-sensitive passwords, reasonably low logon validation options, and logon disabling options configured in SymmRemote?

All Logon Security settings meet minimum expectation as shown in Figure 4. These settings cannot be tested without a SymmRemote client.

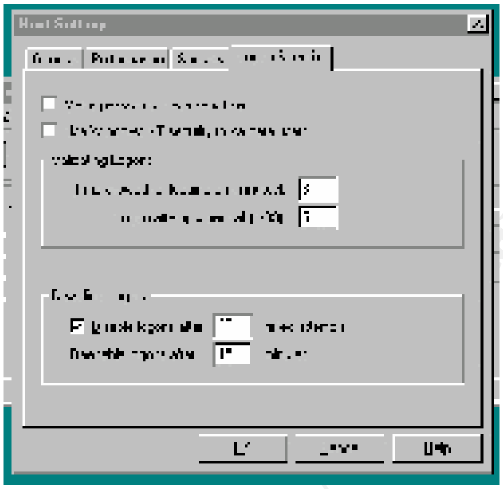


Figure 4 - SymmRemote Logon Security

7. Is SymmRemote set to require data encryption?

SymmRemote is not configured to require data encryption. (See Figure 5)

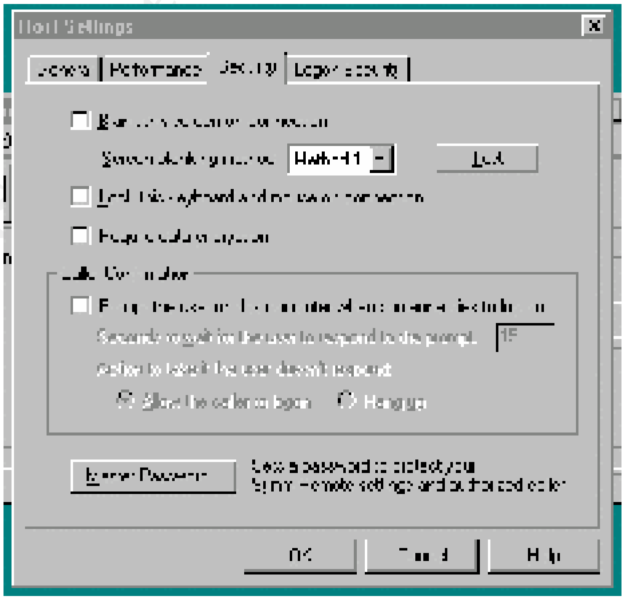
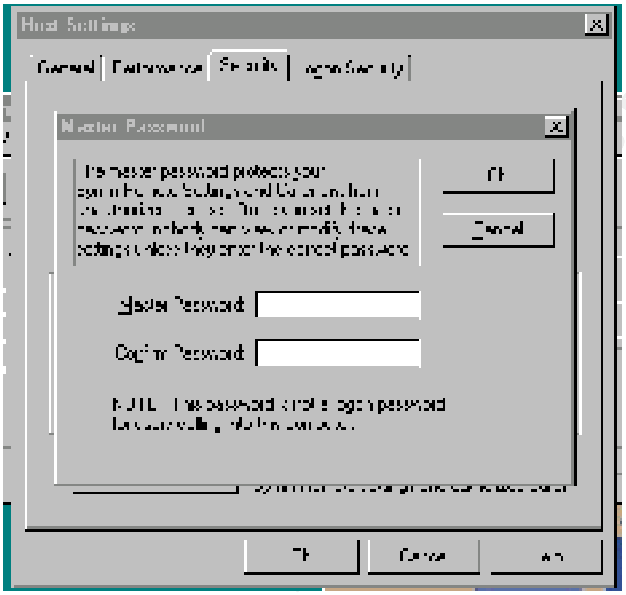

Host Settings
Performance
□ Require data encryption
Seconds to wait for the user to respond to the prompt: 15
Action to take if the user doesn't respond
○ Allow the caller to logon
○ Hang up
OK
Help

Figure 5 - SymmRemote Security

© SANS Institute 2002, Author retains full rights.

8. Is the SymmRemote Master Password set?

The SymmRemote master password is not set as illustrated by Figure 6. As shown in Figure 7, this condition allows a security setting to be changed. In this case the *Time allowed for logging in* was changed from 3 minutes to 4 minutes.



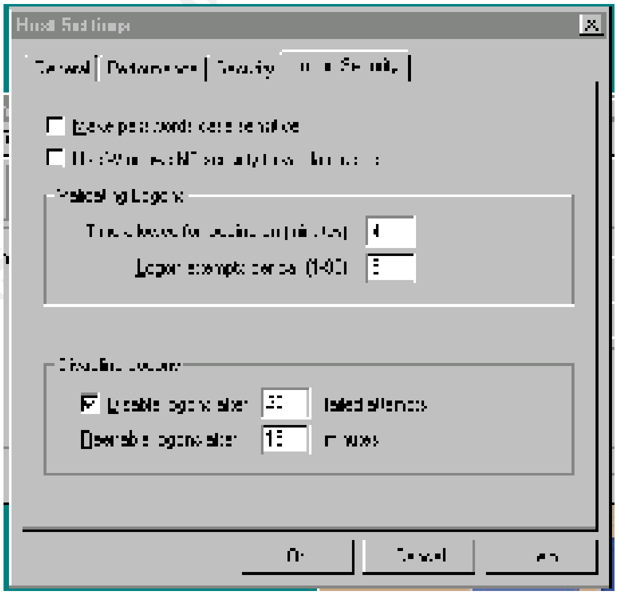
The master password protects your SymmRemote Settings and Caller entries from unauthorized changes. This [illegible] prevents anybody from viewing or modifying these settings unless they enter the correct password.

Master Password:

Confirm Password:

NOTE: This password is not a logon password for connecting into this computer.

Figure 6 - SymmRemote Master Password Setting



□ Make passwords case sensitive

□ Use Windows NT security for [illegible]

Protecting Logons

Time allowed for logging in (minutes) 4

Logon attempts per call (1-10) 3

Disabling Logons

☑ Disable logons after 30 failed attempts

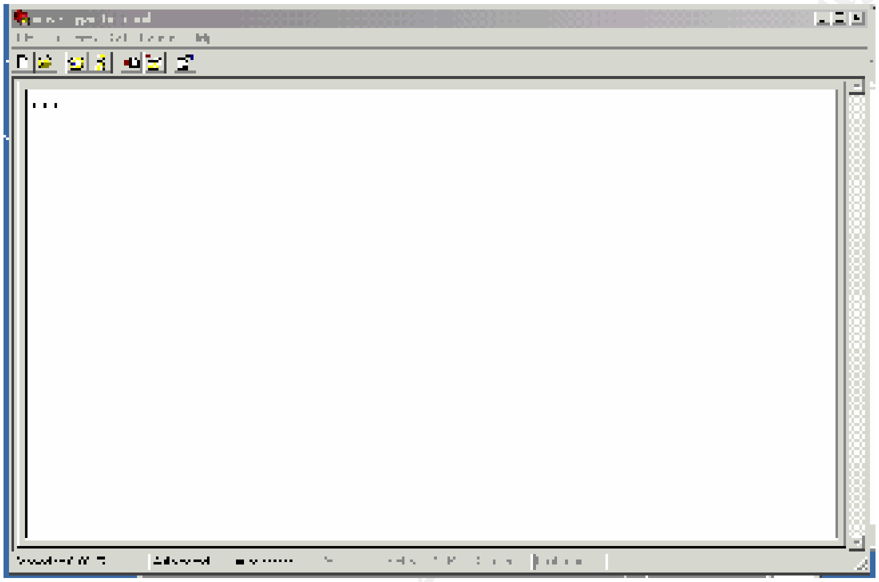
Reenable logons after 15 minutes

Figure 7 - Security Setting Changed

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

9. Can a remote attacker easily dial in to the service processor and try to brute force passwords?

Figure 8 and Figure 9 show that simply dialing into the service processor with various terminal settings does not give access to an authentication prompt, but the modem does answer as expected.



```
...
```

Figure 8 - Dialing into the service processor

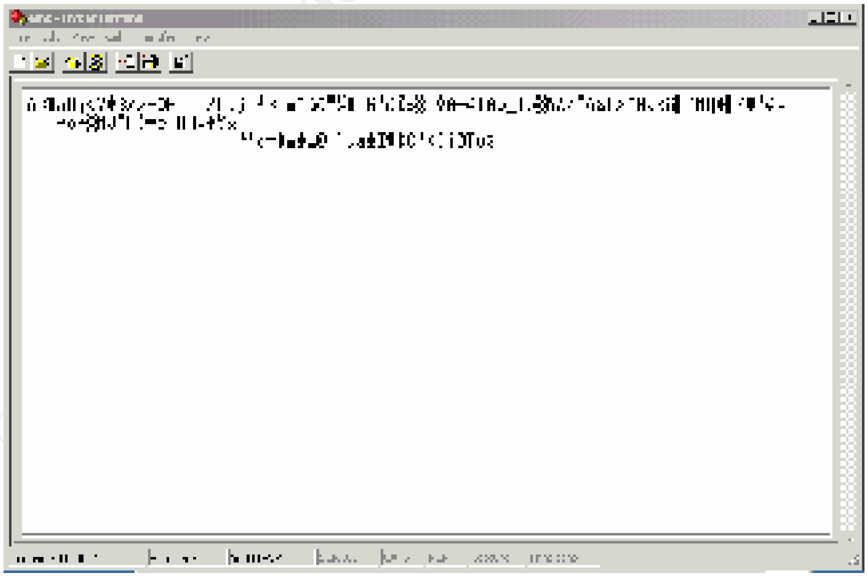
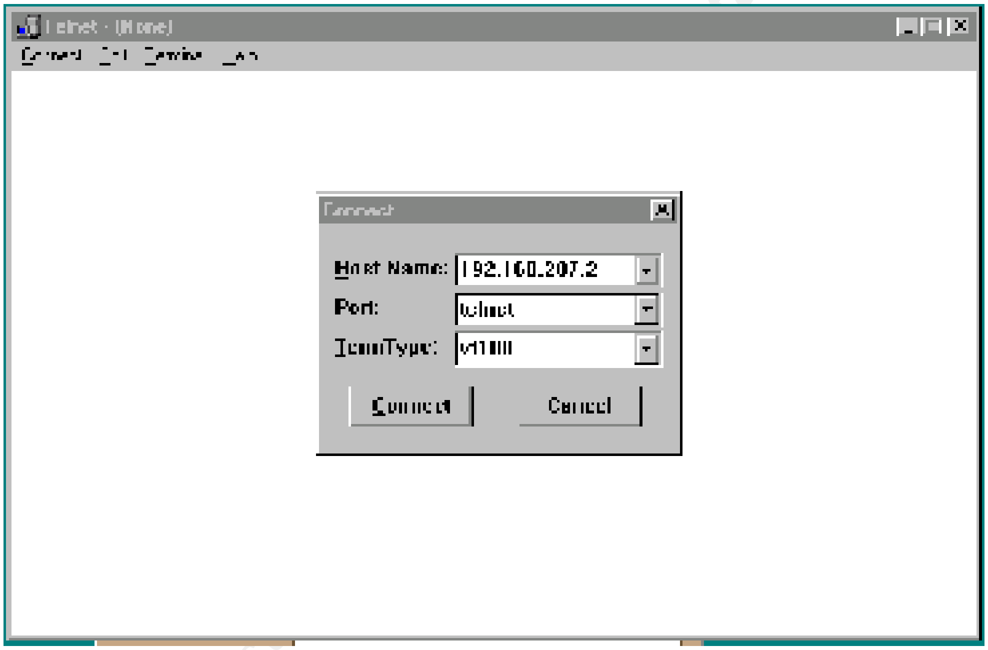


Figure 9 - Dialing into the service processor

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10. Ensure that the default Administrator password for the web server embedded in the DS-32M has been changed.

The Connectrix embedded web server could not be contacted. Figure 10 and Figure 11 demonstrate testing the telnet service on the Connectrix switch. Telnet was not enabled. A similar test was performed to port 80 and no web service was found.



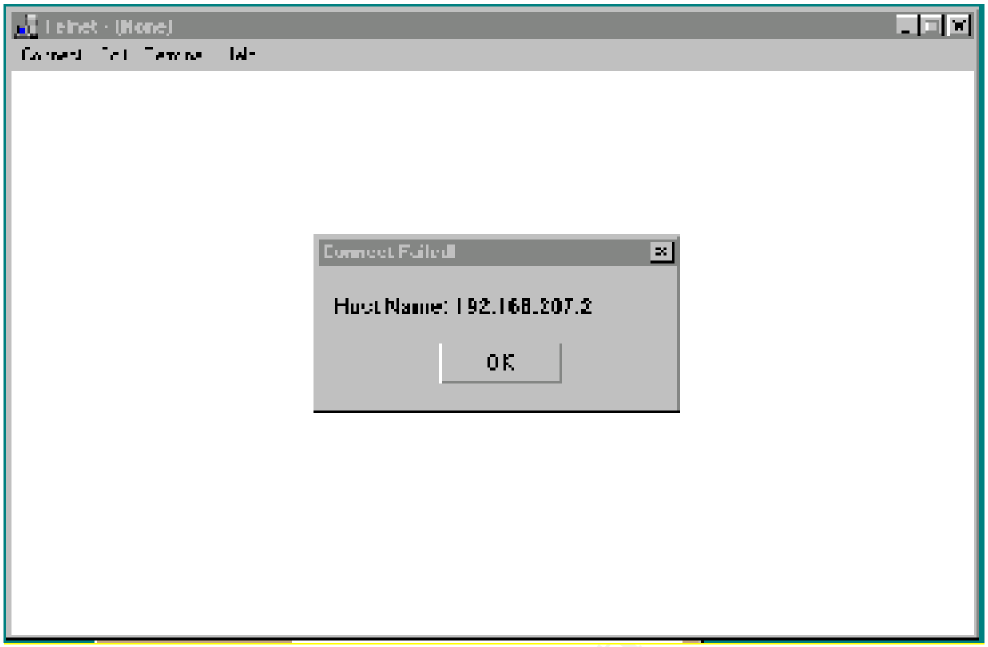
Host Name: 192.168.207.2

Port: telnet

TermType: vt100

Figure 10 - Telnet to Connectrix Switch

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Host Name: 192.168.207.2

Figure 11 - Failed Telnet to Connectrix Switch

11. Ensure that the default Operator password for the web server embedded in the DS-32M has been changed.

See previous test.

12. Is the Connectrix web server enabled or telnet enabled?

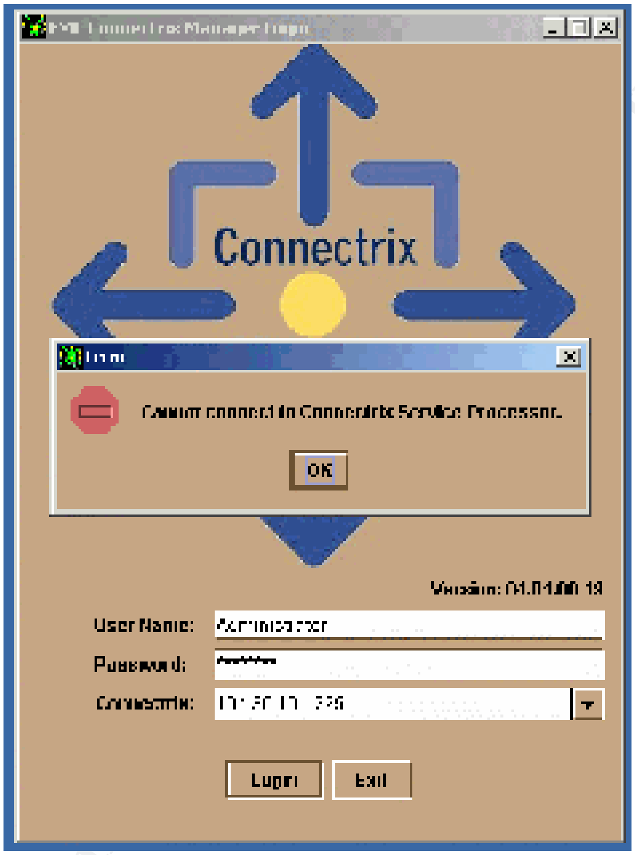
See test 11.

© SANS Institute 2000 - 2002, Aut

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

13. Has Connectrix Manager default Administrator password been changed?

The Connectrix default password has been changed. The auditor attempted to logon to Connectrix Manager remotely using the Administrator account and default password. Figure 12.



Cannot connect to Connectrix Service Processor.

Version: 04.04.00 19

User Name: Administrator

Password: ********

Connectrix: [illegible]

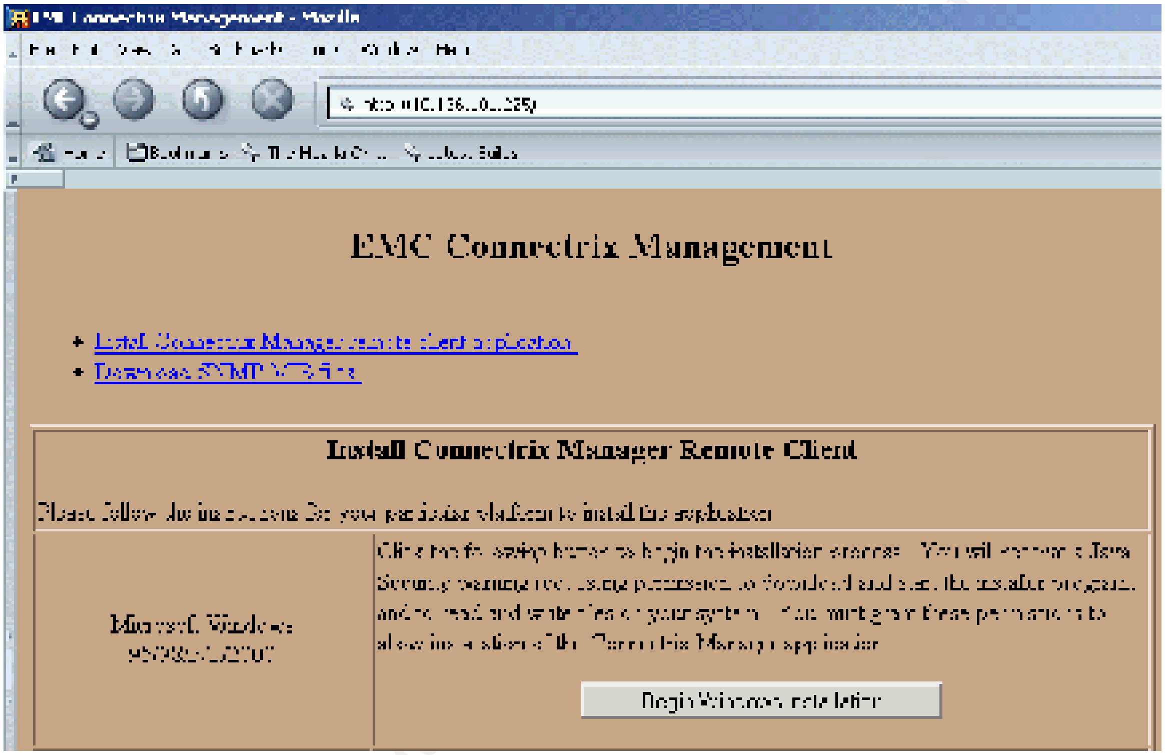
Figure 12 - Connectrix Manager Logon Failure

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

14. Is Microsoft Personal Web Services enabled on the service processor?

Microsoft Personal Web Server was demonstrated to be running on the Connectrix service processor by browsing to the processor's IP address.


EMC Connectrix Management - Mozilla
File Edit View Go Bookmarks Tools Window Help
Home
Bookmarks

http://10.136.[illegible]

EMC Connectrix Management

- Install Connectrix Manager remote client application
- Download SNMP MIB files

Install Connectrix Manager Remote Client

Please follow the instructions for your particular platform to install the application.

Microsoft Windows 95/98/NT/2000	Click the following button to begin the installation process. You will receive a Java Security warning requesting permission to download and start the installer program, and to read and write files on your system. You must grant these permissions to allow installation of the Connectrix Manager application. Begin Windows Installation

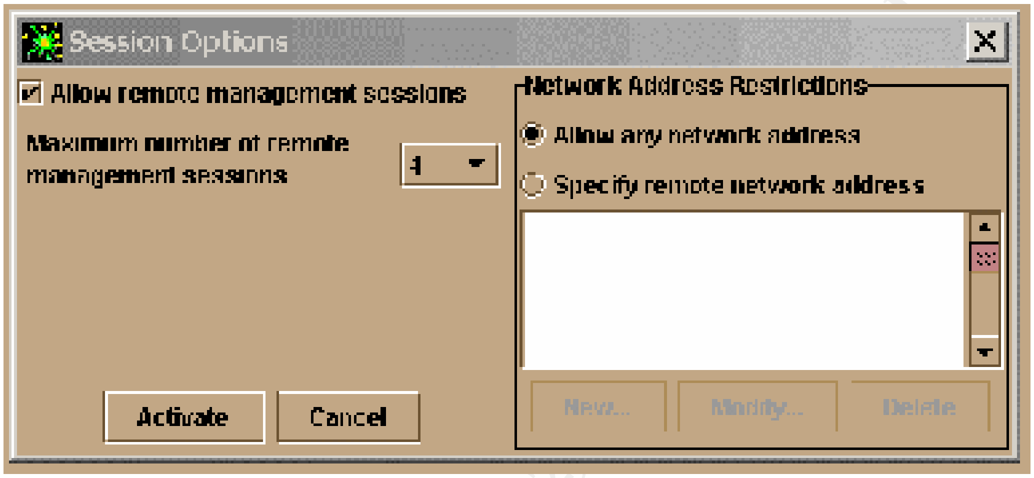
Figure 13 - PWS on the Connectrix

© SANS Institute Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

15. Are Connectrix Manager Access restrictions used to limit what IP addresses can remotely connect to Connectrix Manager?

Connectrix Manager access restrictions are not set.



Session Options

☑ Allow remote management sessions

Maximum number of remote management sessions: 4

Network Address Restrictions

● Allow any network address

○ Specify remote network address

Figure 14 - Connectrix Manager Network Access Restrictions

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

16. What type of zoning strategy is in use?

The SAN administrator reported that the Single HBA zoning strategy is in use.

17. Analyze zoning configuration.

Inspection of the zoning configuration in ESN Manager show that no zone contains more than one HBA. Figure 15 demonstrates this for four zones.

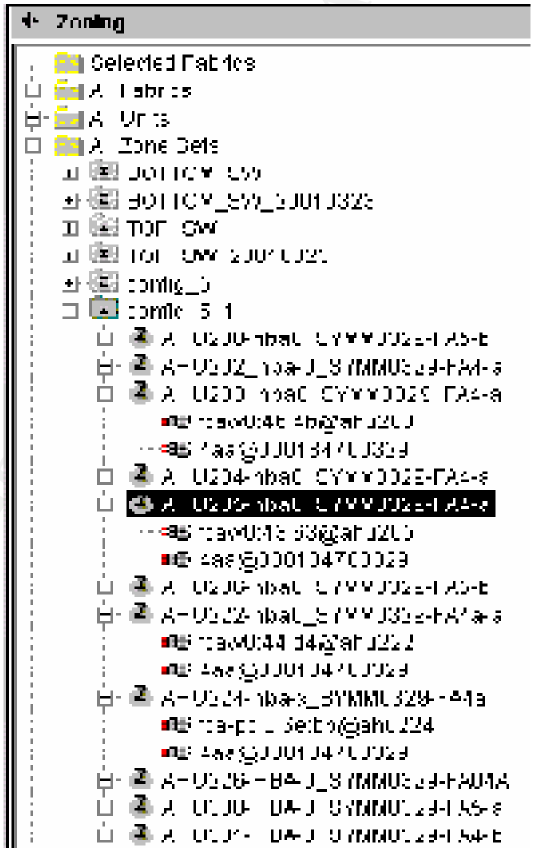


Figure 15 - Example of Single HBA Zones

© SANS Institute 2000 - 2002, Author retains full rights.

18. Is the zoning configuration in the FiberZone database being enforced on the SAN?

The next 6 exhibits show that altering the Solaris SAN configuration files did not result in any additional SAN zone or device (LUN) access.

Original sd.conf:

```
bash-2.03# more sd.conf
#
# Copyright (c) 1992, by Sun Microsystems, Inc.
#ident  "@(#)sd.conf    1.9     98/01/11 SMI"
name="sd" class="scsi" class_prop="atapi" target=0 lun=0;
name="sd" class="scsi" class_prop="atapi" target=1 lun=0;
name="sd" class="scsi" class_prop="atapi" target=2 lun=0;
name="sd" class="scsi" class_prop="atapi" target=3 lun=0;
name="sd" class="scsi" target=4 lun=0;
name="sd" class="scsi" target=5 lun=0;
name="sd" class="scsi" target=6 lun=0;
name="sd" class="scsi" target=8 lun=0;
name="sd" class="scsi" target=9 lun=0;
name="sd" class="scsi" target=10 lun=0;
name="sd" class="scsi" target=11 lun=0;
name="sd" class="scsi" target=12 lun=0;
name="sd" class="scsi" target=13 lun=0;
name="sd" class="scsi" target=14 lun=99;
name="sd" class="scsi" target=15 lun=0;
```

Original jnic146x.conf (many comments removed):

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Bash-2.03# more jnic146x.conf
##
## JNI Corporation jnic146x driver (Solaris SCSI) configuration
file.
##
## jnic146x.conf
##
FcLoopEnabled   = 0;
FcFabricEnabled = 0;
FcEngHeartbeatInterval = 5;
FcLinkUpRecoveryTime = 1000;
BusyRetryDelay = 5000;
FailoverDelay = 60;
TimeoutResetEnable = 0;
QfullRetryCount = 5;
QfullRetryDelay = 5000;
LunRecoveryInterval = 50;
FcLinkSpeed = 3;
JniCreationDelay = 30;
FlogiRetryCount = 5;
FcFlogiTimeout = 10;
PlogiRetryCount = 5;
PlogiControlSeconds = 30;
FcEmldEngTcbCount = 1789;
def_hba_binding = "null";
def_wwnn_binding = "$xxxxxxxxxxxxxxxx";
def_wwpn_binding = "$xxxxxxxxxxxxxxxx";
def_port_binding = "xxxxxx";
target0_hba      = "jnic146x0";
target0_lun0_hba = "jnic146x0";
target0_wwnn     = "xxxxxxxxxxxxxxxx";
target0_wwpn     = "xxxxxxxxxxxxxxxx";
target0_port     = "xxxxxx";

target_throttle = 256;
lun_throttle = 64;
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
target0_throttle = 256;
target0_lun_throttle = 64;
target0_lun1_throttle = 64;

LunDiscoveryMethod = 0;
CmdTaskAttr = 1;
automap = 0;
jnic146x0-automap = 0;
target14_hba="jnic146x1";
target14_wwpn="50060482bfd19d4d";
```

© SANS Institute 2000 - 2002, Author retains full rights.

Original format output:

```
# format
Searching for disks...done
AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
          /pci@8,600000/SUNW,qlc@4/fp@0,0/ssd@w21000004cf96af15,0
       1. c1t1d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
          /pci@8,600000/SUNW,qlc@4/fp@0,0/ssd@w21000004cf96b168,0
       2. c3t14d99 <EMC-SYMMETRIX-5567 cyl 20458 alt 2 hd 15 sec
64>
          /pci@8,700000/JNI,FCR@3,1/sd@e,63
```

Modified sd.conf (partial):

```
bash-2.03# more sd.conf
#
# Copyright (c) 1992, by Sun Microsystems, Inc.
#ident  "@(#)sd.conf    1.9     98/01/11 SMI"
name="sd" class="scsi" class_prop="atapi" target=0 lun=0;
name="sd" class="scsi" class_prop="atapi" target=1 lun=0;
```

```
name="sd" class="scsi" class_prop="atapi" target=2 lun=0;
name="sd" class="scsi" class_prop="atapi" target=3 lun=0;
name="sd" class="scsi" target=4 lun=0;
 .
 .
 .
name="sd" class="scsi" target=4 lun=255;
name="sd" class="scsi" target=5 lun=0;
.
 .
 .
name="sd" class="scsi" target=5 lun=255;
 .
 .
 .
name="sd" class="scsi" target=14 lun=0;
name="sd" class="scsi" target=14 lun=1;
name="sd" class="scsi" target=14 lun=2;
name="sd" class="scsi" target=14 lun=3;
name="sd" class="scsi" target=14 lun=4;
name="sd" class="scsi" target=14 lun=5;
name="sd" class="scsi" target=14 lun=6;
name="sd" class="scsi" target=14 lun=7;
name="sd" class="scsi" target=14 lun=8;
 .
 .
 .
name="sd" class="scsi" target=14 lun=99;
name="sd" class="scsi" target=14 lun=100;
name="sd" class="scsi" target=14 lun=101;
 .
 .
 .
name="sd" class="scsi" target=14 lun=253;
name="sd" class="scsi" target=14 lun=254;
name="sd" class="scsi" target=14 lun=255;
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
name="sd" class="scsi" target=15 lun=0;
 .
 .
 .
```

Modified jnic146x.conf (many comments removed):

```
Bash-2.03# more jnic146x.conf
##
## JNI Corporation jnic146x driver (Solaris SCSI) configuration
file.
##
## jnic146x.conf
##
FcLoopEnabled   = 0;
FcFabricEnabled = 0;
FcEngHeartbeatInterval = 5;
FcLinkUpRecoveryTime = 1000;
BusyRetryDelay = 5000;
FailoverDelay = 60;
TimeoutResetEnable = 0;
QfullRetryCount = 5;
QfullRetryDelay = 5000;
LunRecoveryInterval = 50;
FcLinkSpeed = 3;
JniCreationDelay = 30;
FlogiRetryCount = 5;
FcFlogiTimeout = 10;
PlogiRetryCount = 5;
PlogiControlSeconds = 30;
FcEmldEngTcbCount = 1789;
def_hba_binding = "null";
def_wwnn_binding = "$xxxxxxxxxxxxxxxx";
def_wwpn_binding = "$xxxxxxxxxxxxxxxx";
def_port_binding = "xxxxxx";
target0_hba      = "jnic146x0";
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
target0_lun0_hba = "jnic146x0";
target0_wwnn     = "xxxxxxxxxxxxxxxx";
target0_wwpn     = "xxxxxxxxxxxxxxxx";
target0_port     = "xxxxxx";

target_throttle = 256;
lun_throttle = 64;
target0_throttle = 256;
target0_lun_throttle = 64;
target0_lun1_throttle = 64;

LunDiscoveryMethod = 0;
CmdTaskAttr = 1;
automap = 1;
jnic146x1-automap = 1;
jnic146x0-automap = 1;
```

Resulting format output:

```
# format
Searching for disks...done
AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
          /pci@8,600000/SUNW,qlc@4/fp@0,0/ssd@w21000004cf96af15,0
       1. c1t1d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
          /pci@8,600000/SUNW,qlc@4/fp@0,0/ssd@w21000004cf96b168,0
       2. c3t14d99 <EMC-SYMMETRIX-5567 cyl 20458 alt 2 hd 15 sec
64>
          /pci@8,700000/JNI,FCR@3,1/sd@e,63
```

19. If port zoning is part of the zoning strategy, ensure that it is implemented.

Port zoning is not part of the zoning strategy. Not applicable.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

20. Is LUN Masking used as an additional layer of access controls for Symmetrix devices?

The SAN administrator reports that LUN Masking is configured from ESN Manager.

21. Is LUN masking enforced at the server level or storage device level?

ESN Manager is used to enforce LUN Masking at the storage device level. Figure 16 demonstrates that LUN Masking is enforced through ESN Manager. While the zoning configuration makes it possible for the selected host to see many devices, the LUN Masking configuration makes it so that only the devices outlined in blue can actually be seen by the host.

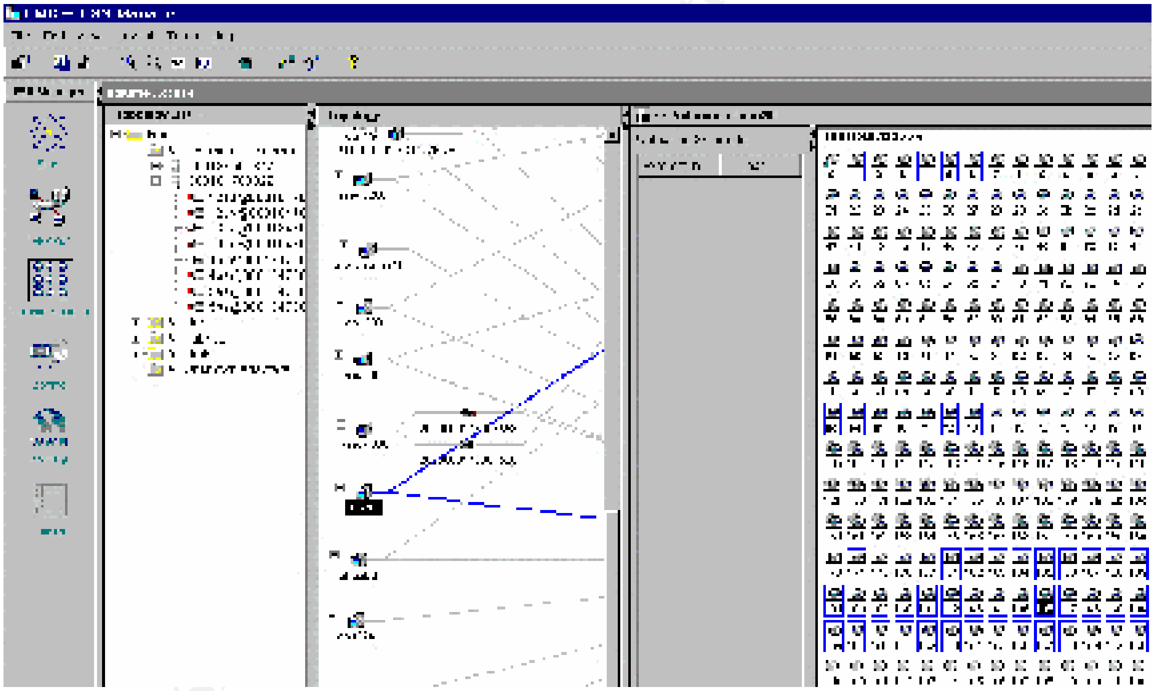


Figure 16 - LUN Masking through ESN Manager

22. Is the VCMDB Access feature enabled?

The SAN administrator reports that the VCMDB Access feature is not enabled. It should be noted that neither the system documentation nor the SAN administrator knows how to set or check this setting. The system documentation refers the customer to EMC support for help with this feature. The SAN administrator has demonstrated interest in enabling this feature.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

23. If LUN masking is enabled at the device level, are hosts only permitted to access the minimum required Symmetrix devices?

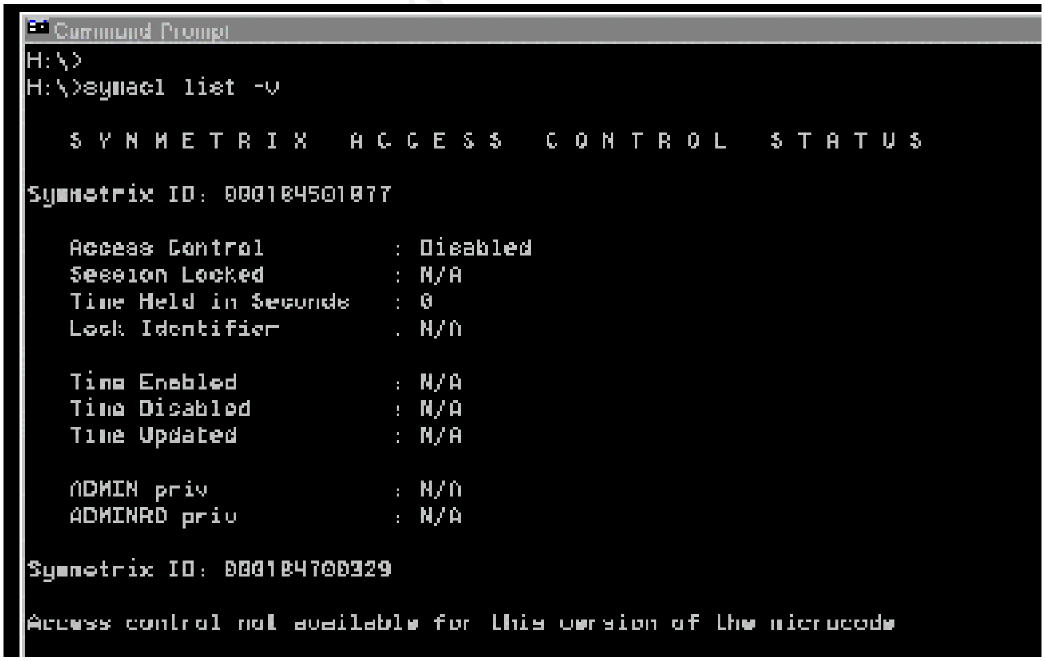
See the test results from checklist item 18.

24. Has the default ESN manager password been changed?

The SAN administrator demonstrated while logging in to ESN Manager that the default password has not been changed.

25. Is Symmetrix access control administration limited to an administrative group from the management station?

This test demonstrates that the Symmetrix microcode version installed does not support access controls. Administrator intent was for this to be configured but time did not permit.



```
H:\>
H:\>symacl list -v

   S Y M M E T R I X   A C C E S S   C O N T R O L   S T A T U S

Symmetrix ID: 000184501077

   Access Control          : Disabled
   Session Locked          : N/A
   Time Held in Seconds    : 0
   Lock Identifier         : N/A

   Time Enabled            : N/A
   Time Disabled           : N/A
   Time Updated            : N/A

   ADMIN priv              : N/A
   ADMINRD priv            : N/A

Symmetrix ID: 000184700329

Access control not available for this version of the microcode
```

Figure 17 - Symmetrix access control settings

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

26. Does each admin user have a unique user access PIN?

Not applicable. Symmetrix access controls not support with current microcode.

27. Are Symmetrix access controls used to limit specific hosts to managing specific devices with the least amount of privilege necessary?

Not applicable. Symmetrix access controls not support with current microcode.

28. What Grant/Deny access strategy is in use?

Not applicable. Symmetrix access controls not support with current microcode.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SAN Physical Topology and Physical Security Checklist Results

version 1.0 August 24, 2002

29. How is physical access to the SAN devices and service processors controlled?

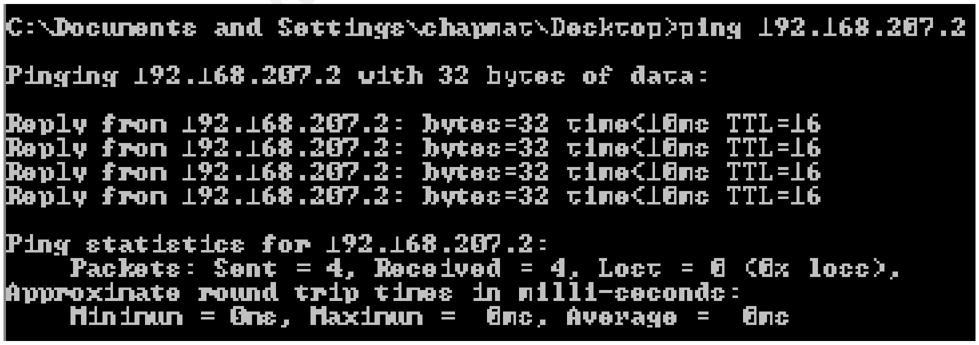
Two separate doors requiring keycard access provide physical access control to the EMC. Additionally, a hex wrench is required to open the EMC cabinets.

30. Are the service processors screens locked when not in use?

EMC service processor screens are not locked when not in use. May hamper access by EMC support services.

31. Are the Ethernet interfaces for the SAN, including the Symmetrix, Connectrix, service processors, and management (control) station on a private network?

The Symmetrix network interfaces are on a private network. All other interfaces are on the corporate network. Figure 18 demonstrates that the Connectrix switch can be pinged from the local LAN (but not from another network as it appears that the default gateway of the switch is not set correctly).



```
C:\Documents and Settings\chapmat\Desktop>ping 192.168.207.2

Pinging 192.168.207.2 with 32 bytes of data:

Reply from 192.168.207.2: bytes=32 time<10ms TTL=16
Reply from 192.168.207.2: bytes=32 time<10ms TTL=16
Reply from 192.168.207.2: bytes=32 time<10ms TTL=16
Reply from 192.168.207.2: bytes=32 time<10ms TTL=16

Ping statistics for 192.168.207.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure 18 - Pinging the Connectrix switch

However an nmap scan did not reveal any open ports:

```
# nmap –sS 192.168.207.2
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try -
P0

Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# nmap –sT 192.168.207.2
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try -
P0

Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds

# nmap –sU 192.168.207.2
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try -
P0

Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds
```

Using tcpdump it was shown that the service processor and the switch do use TCP to communicate on high port numbers.

```
20:46:23.766600 192.168.101.1.1548 > 192.168.207.2.2048: . ack 161 win
20:46:43.577689 192.168.101.1.1548 > 192.168.207.2.2048: P 160:176(16)
ack 161 win 8404 (DF)
20:46:43.581459 192.168.207.2.2048 > 192.168.101.1.1548: . ack 176 win
3866 (DF) [tos 0xc0]
20:46:43.582537 192.168.207.2.2048 > 192.168.101.1.1548: . 161:177(16)
ack 176 win 4000 (DF) [tos 0xc0]
20:46:43.695561 192.168.101.1.1548 > 192.168.207.2.2048: . ack 177 win
8388 (DF)
```

32. If the SAN is on a private network, how is it connected to the corporate LAN? If by firewall/VPN what rules are in place?

Parts of the SAN are directly connected to the corporate LAN without protection of VPN or firewall.

33. Is EMC Control Center installed in a 1, 2, or 3 tier configuration?

EMC Control Center is installed in a 2-tier configuration.

34. Is a nethost file used to control access to EMC Control Center?

The EMC Control Center nethost file is not configured. The SAN administrator is working on getting more specific documentation from EMC on how to configure this feature.

© SANS Institute 2000 - 2002, Author retains full rights.

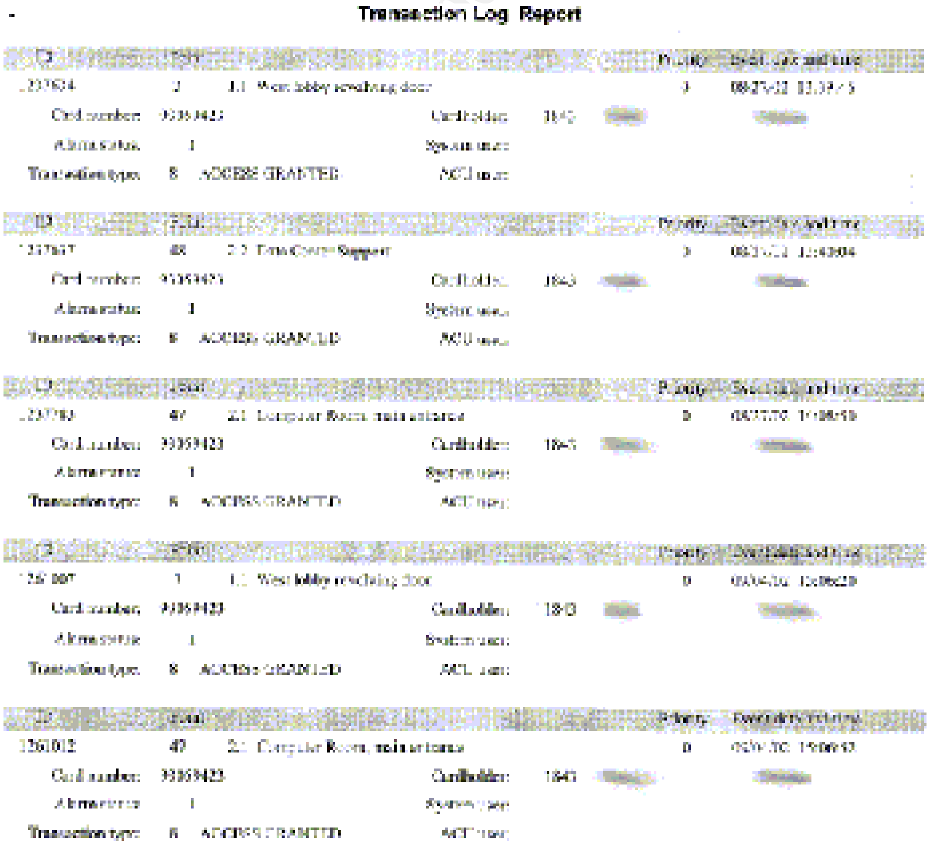
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

35. Does EMC support have un-escorted access to the building, data center, and SAN? If so what hours?

A specific EMC support engineer has 24x7-unescorted access to the data center and the SAN. The support engineer is required to note his access on a log connected to the frame. The auditor was not able to obtain a copy of this log during the audit period. Later it was determined that not log exists. All communication is verbal.

36. Is EMC support access to the building logged and does the SAN security administrator periodically review the logs?

All keycard access to the building is logged. Access logs of the EMC support engineer are not reviewed or correlated to systems logs. Figure 19 and Figure 20 are partial reports of EMC support engineer access to the building. The logs show the engineer moving through the outer door, inner door, and then into the data center. The engineer's name has been grayed out.

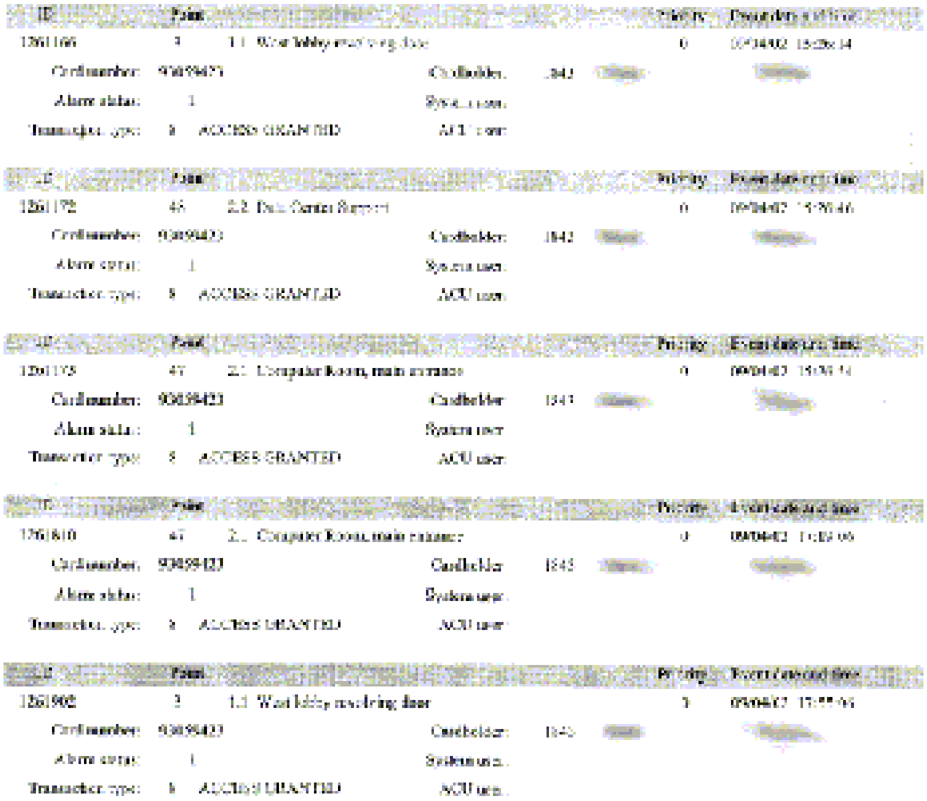


Transaction Log Report

```
ID            Point                                          Priority   Date and time
1237634       2      1.1 West lobby revolving door            0          08/27/02 13:37:45
   Card number:      33069423                  Cardholder:    1843  [redacted]  [redacted]
   Alarm status:     1                         System user:
   Transaction type: 8   ACCESS GRANTED        ACU user:

ID            Point                                          Priority   Date and time
1237657       48     2.2 Data Center Support                  0          08/27/02 13:43:04
   Card number:      33069423                  Cardholder:    1843  [redacted]  [redacted]
   Alarm status:     1                         System user:
   Transaction type: 8   ACCESS GRANTED        ACU user:

ID            Point                                          Priority   Date and time
1237703       47     2.1 Computer Room main entrance          0          08/27/02 14:08:59
   Card number:      33069423                  Cardholder:    1843  [redacted]  [redacted]
   Alarm status:     1                         System user:
   Transaction type: 8   ACCESS GRANTED        ACU user:

ID            Point                                          Priority   Date and time
1256007       1      1.1 West lobby revolving door            0          09/04/02 15:06:20
   Card number:      33069423                  Cardholder:    1843  [redacted]  [redacted]
   Alarm status:     1                         System user:
   Transaction type: 8   ACCESS GRANTED        ACU user:

ID            Point                                          Priority   Date and time
1261012       47     2.1 Computer Room, main entrance         0          09/04/02 15:09:43
   Card number:      33069423                  Cardholder:    1843  [redacted]  [redacted]
   Alarm status:     1                         System user:
   Transaction type: 8   ACCESS GRANTED        ACU user:
```

Figure 19 - Building access log 1

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



```
ID              Point                                           Priority   Event date and time
1261166         3       1.1  West lobby revolving door              0      09/04/02  15:29:34
     Cardnumber:  93059423                  Cardholder:   1843   [redacted]        [redacted]
    Alarm status:    1                     System user:
Transaction type:  8    ACCESS GRANTED         ACU user:

ID              Point                                           Priority   Event date and time
1261172         46      2.2  Data Center Support                    0      09/04/02  15:29:46
     Cardnumber:  93059423                  Cardholder:   1843   [redacted]        [redacted]
    Alarm status:    1                     System user:
Transaction type:  8    ACCESS GRANTED         ACU user:

ID              Point                                           Priority   Event date and time
1261173         47      2.1  Computer Room, main entrance           0      09/04/02  15:30:34
     Cardnumber:  93059423                  Cardholder:   1843   [redacted]        [redacted]
    Alarm status:    1                     System user:
Transaction type:  8    ACCESS GRANTED         ACU user:

ID              Point                                           Priority   Event date and time
1261810         47      2.1  Computer Room, main entrance           0      09/04/02  16:03:06
     Cardnumber:  93059423                  Cardholder:   1843   [redacted]        [redacted]
    Alarm status:    1                     System user:
Transaction type:  8    ACCESS GRANTED         ACU user:

ID              Point                                           Priority   Event date and time
1261902         3       1.1  West lobby revolving door              0      09/04/02  17:55:06
     Cardnumber:  93059423                  Cardholder:   1843   [redacted]        [redacted]
    Alarm status:    1                     System user:
Transaction type:  8    ACCESS GRANTED         ACU user:
```

Figure 20 - Building access log 2

© SANS Institute 2000 - 2002, Author retains full rights.

Data Classification and Control Checklist Results

version 1.0 August 24, 2002

37. Does the organization have a data classification policy?

The organization does have a data classification policy but it has not been communicated widely. See Appendix A – Corporate Data Classification Model.

38. When SAN disk space is allocated to a server is the organization's data classification model used to determine special requirements for data handling by the SAN administrator or data owner?

Data is not treated differently based on its classification.

39. Are separate SAN device pools used to store data of different data classifications so that access controls can be applied to device pools?

Not applicable; data classification is not tracked on the SAN and Symmetrix access controls are not currently supported.

40. Is the SAN administrator notified each time a failing disk is replaced by EMC and are there data handling and disposal agreements between the corporation and EMC?

The SAN administrator is supposed to be notified by the EMC support engineer when a failing component is replaced. This communication is verbal. It may be possible to correlate EMC building access with system logs but this is not done due to resource constraints. There is no data handling agreement between EMC and the organization.

41. Are disks with highly confidential data formatted before reuse?

SAN disks are not formatted before reuse according to the SAN administrator.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Securability of the SAN

In order for the system to be considered secure the confidentiality, integrity, and availability of its data must be assured. The first step in achieving these goals is to use zoning and LUN masking to limit accessibility to the data. In this respect the system meets our expectations. Each connected host is configured so that it can only communicate with the minimum necessary systems on the SAN (zoning). Further, each host has access to the minimum necessary devices within its zone (LUN masking).

To ensure that these controls remain in place the management interfaces of the system must be protected. These protections are not sufficient for a system that controls almost all corporate data. Thus our recommendations will concentrate on short and long term implementation of controls to protect these interfaces.

The objective of the audit was to identify the risks to the system and recommend policies, procedures, and controls. These recommendations must strike a balance between the organization's acceptable level of risk and the impact of the controls on the manageability of the system. Three general areas of risk were identified during the audit: IP based SAN management, Fiber Channel based SAN management, and data classification and handling procedures. Recommendations for each of these areas will be addressed in the management report.

Addressing all the risks identified in the management report will not eliminate all risks to the SAN. Some residual risks will remain either because the likelihood of the vulnerability being exploited is low, or the management costs of implementing proper controls is too high compared to the risk reduction.

The use of Single HBA Zoning limits communication between systems while maintaining manageability. The security of Single HBA Zoning relies on systems in the zone being identified by their WWN number. It is possible that this number can be spoofed similarly to IP addresses or MAC addresses. Using Port Zoning would greatly reduce the risk successful WWN spoofing, but would also decrease manageability by requiring more configuration changes when moving or replacing HBAs within the SAN.

Once access is gained to the data center there are no significant controls protecting the SAN devices or service processors from physical access. Adding locks to the cabinets and locking the service processor screens would add a layer of physical protection, but would require coordination will EMC support engineers, who may be accessing the SAN at any hour to preemptively replace failing disk drives. The potential for interruption of system maintenance makes addressing this risk too inconvenient.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

When EMC support engineers access the data center they are required to log their activity. It is possible to correlate system logs, building access logs, and activity logs to detect unaccounted access to the SAN, but doing so would greatly tax already overburdened resources. The ability of an EMC engineer to identify valuable data and the likelihood that this would happen are considered low.

No device pools or other mechanisms are used to treat data according to its classification. The chance of data on devices moved within the SAN of being recovered is low. It should be sufficient to treat all data the same within the SAN. If extra security is required then encryption should be used at the filesystem or database level. Disks being replaced by EMC engineers should be wiped before they leave the premises.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Auditability of the SAN

The audit (including the research) was successful in identifying the security risks to the SAN, leading to recommendations to eliminate or mitigate those risks, while at the same time keeping the system manageable. While the system is auditable, there are some checklist items that are difficult to verify.

Testing the configuration of SymmIP and SymmRemote to prove that they are enforced is difficult because the SymmIP and SymmRemote clients are needed to perform the tests. These client programs are not installed at the customer site because they are used by EMC support engineers to provide remote support. Testing these controls would require the cooperation of EMC and may have to be preformed off-site. The resources to do this were not sought for this audit.

Some checklist items pertaining to the Connectrix were not completed because of the inability to contact the Connectrix switch over the network. It turned out that the switch had no default route. This mis-configuration provides an unintended layer of security. This extra security cannot be counted on because the configuration may be corrected in the future.

Using a locally connected computer, it was determined that the Connectrix switch was not running embedded web or telnet servers. This makes the system more secure, but we were not able to determine how these embedded servers are turned on or off. Because we could not turn them on we could not check that their default passwords have been changed (also indicating that they probably have not been changed.) It is important that these passwords be changed even if the servers are not running, in case they are accidentally turned on in the future.

Lastly and most importantly, although zoning and LUN masking were tested, the tests as designed do not give us the highest level of confidence that the configuration is completely secure.

Determining that the zoning and LUN masking configurations allow the minimum possible access is difficult. In a large SAN there are many hosts, zones, and devices, making for a large number of possible configurations. Also, with multiple systems sharing information, performing fail-over duties for each other, or simply having multiple redundant paths to the same data, analyzing a configuration can be difficult, increasing exponentially with the size of the system. Some method of automating the analysis would be helpful here. It would also be helpful to document both command line and GUI interface tests so that the auditor can use the method that he or she prefers.

Assuming the corrected configuration is understood, testing that the configuration is being enforced is also challenging. For this audit the configuration was tested by reconfiguring one of the SAN hosts to attempt to “see” more devices than are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

supposed to be permitted. This type of test is unsatisfactory because it depends on the host's ability to locate devices on the SAN using its native capabilities. How do you know that something does not exists simply because you have not found it? A prepared attacker may have more advanced tools that "sniff" the Fiber Channel fabric or "map" the SAN.

One way to improve this type of test would be to install the SAN management tools on a host that is configured so that it is not allowed to perform SAN management. Using the auto-discovery features of these tools should not reveal any more information than was intended for the system. (Care should be taken to remove these tools once the test is over, so that a future attacked is not accidentally aided in his exploits.)

Despite these issues we feel the audit is effective in identifying risks to the system.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. EMC Audit – Management Report

Executive Summary

A risk assessment and security audit of the corporate EMC SAN (Storage Area Network) was successfully performed between Sept. 6th and Sept. 12th, 2002. Overall the audit results are favorable. Controls to limit which SAN systems can communicate and what data they can access are in place and operating as intended. This is a significant portion of the most important risks addressed by this audit.

The risks that were identified fall into the broad areas of IP based management, Fiber Channel based management, and data classification and handling. Summaries of the risks, recommended controls, and estimated costs will be presented below, followed by a list of SAN security policies and procedures that should be developed.

SAN Risks Identified during the Audit

IP Based Management

The management station, Connectrix switch, and its service processor are on the corporate LAN. If these systems are not protected an attacker can use them to disrupt SAN operation, causing a denial of service, or make configuration changes which may make confidential data accessible to the wrong systems, possibly compromising secret information.

Recommendations

A management LAN (Figure 21) should be established to secure the out-of-band (IP based communication) management of the SAN. A firewall with VPN capability should be used to segment the management network from the corporate LAN, while allowing remote connections from approved hosts by approved users.

Additionally SymmIP should be installed on the service processors to provide a stronger authentication mechanism and provide better traffic protection for remote connections from EMC support.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

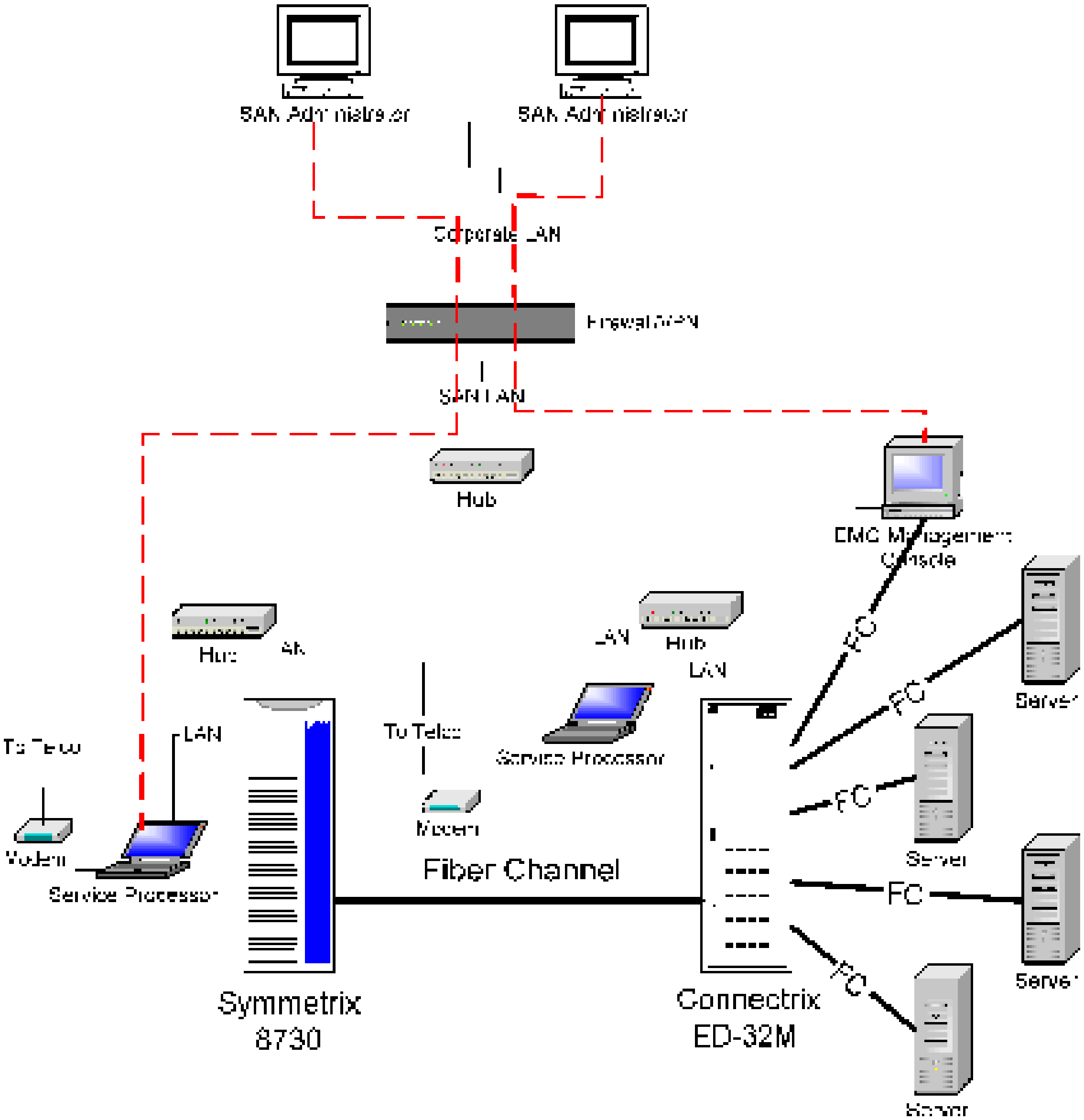


Figure 21 - Recommended SAN Network

Estimated Cost

The cost of establishing the management LAN should be under $5,000 including labor and a firewall device. Installation of SymmIP is probably covered by the EMC support contract.

Compensating Controls

Until the management LAN can be established, a number of configuration improvements can be made to help secure the SAN interfaces to the corporate LAN and remote support. These improvements should remain in place after a management LAN is established, as they will provide an extra layer of security in case of firewall problems.

- The SymmRemote data encryption option should be turned on since there is not cost associated with doing so.
- The SymmRemote master password should be set so that only authorized personnel can change its security configuration. There is no associated cost.
- The Connectrix service processor web server should be disabled since it adds very little value to system manageability. There is no associated cost.
- Connectrix Manager access restrictions should be configured so that only authorized hosts may connect to it. There is no associated cost.
- The EMC Control Center *nethost* file should be configured so that only authorized hosts may connect to it. There is no associated cost.

Fiber Channel based Management

Symmetrix Access Controls and the VCMDB Access feature have not been implemented. Without these controls an attacker on a system with a Fiber Channel connection to the SAN may alter the LUN masking database or make other configuration changes to the SAN. This could result in the compromise, corruption, or unavailability of important data.

Recommendations

The configuration of zoning and LUN masking controls must be protected. Symmetrix Access Controls and the VCMDB Access feature should be implemented to protect these SAN management features.

Estimated Cost

In order to implement Symmetrix Access Controls the microcode will have to be updated. Also, turning on any of these features will require careful planning and activation during approved maintenance hours. Depending on the estimated number of hours, this may require a specially funded project.

Data Classification and Handling Procedures

The corporate data classification policies have not been widely communicated and therefore are not integrated with SAN management procedures. All data are treated equally even though confidential data may need to be managed more cautiously. Also, when failing disks are preemptively removed by EMC support there is no procedure to erase the data on the disks before they leave the corporation's control. There is no agreement between the corporation and EMC on how data is disposed of.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Recommendations

All IT departments should have the data classification policies formally communicated to them. Each department's responsibilities should be evaluated to determine how their procedures should be modified to handle data by classification.

An agreement between the company and EMC should be established to formalize the disposal of data on disks that are being replaced. Procedures for wiping the disks of data before removal should be instituted.

Estimated Cost

Formally communicating data classification policies may be covered under larger security awareness efforts. A significant time investment may be required to develop and deliver the appropriate security training to all IT departments. A more limited awareness level may be achieved through an e-mail campaign, downloadable presentation, and a quiz to verify that the material has been reviewed.

Establishing an informal agreement between the company and EMC on procedures to wipe disks before they are removed may not be difficult. A checklist should be developed and used during each disk replacement to be sure that procedure is followed and is auditable. A formal agreement between the company and EMC will be more difficult and expensive, as it will require the participation of legal counsel.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Recommended Policies and Procedures

In addition to implementing the recommended controls, existing and new practices should be documented and published.

- All available security controls should be configured unless manageability is impacted to the point where the risk of not implementing a control is acceptable. This includes enabling all logging (even if proactive monitoring is not an option), changing default passwords, using encryption options, and disabling unnecessary services. Administrators should have unique user IDs when possible.
- All SAN disks should be reformatted before they are removed from the building. The EMC support engineer should log disk removal and confirm that the formatting procedure was completed.
- All SAN components must be on a management LAN, protected by a firewall, with all remote access established through VPN connections.
- The zoning and LUN masking policies and implementation details should be documented.
- The corporate data classification model should be extended to provide administrators guidance in enforcing data classification and protecting data in their specific areas of responsibility.

Conclusion

The fundamental controls for SAN security are already in place. Once a management LAN, access controls, and data handling procedures are installed and enforced through policy, a reasonably complete architecture for SAN security will have been established.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. EMC. ESN Manager Version 1.1 Volume Logix Command Line Interface Reference. Hopkinton: EMC Corporation, May 2001.

2. EMC. ESN Manager Version 1.1 FiberZone Command Line Interface Reference. Hopkinton: EMC Corporation, May 2001.

3. EMC. ESN Manager Version 2.1 Product Guide. Hopkinton: EMC Corporation, July 2002.

4. EMC. EMC Connectrix Manager Version 4.02 User Guide. Hopkinton: EMC Corporation, December 2001.

5. EMC. EMC Solutions Enabler SYMCLI Access Control Component Version 4.3 Product Guide. Hopkinton: EMC Corporation, June 2001.

6. EMC. EMC Control Center Version 4.3 Installation Guide. Hopkinton: EMC Corporation, June 2001.

7. EMC. SymmIP Release Version 2.06 User Guide. Hopkinton: EMC Corporation, June 2001.

8. EMC. SymmRemote Version 2.06 User Guide. Hopkinton: EMC Corporation, June 2001.

9. EMC. Connectrix ED64M User Guide. Hopkinton: EMC Corporation, July 2001.

10. EMC. Connectrix DS-32M User Guide. Hopkinton: EMC Corporation, July 2001.

11. Clark, Tom. IP SANs: A Guide to iSCSI, iFCP, and FCIP. Protocols for Storage Area Networks. Addison-Wesley, December 2002.

12. Vacca, John. The Essential Guide to Storage Area Networks. Prentice Hall PTR, November 2001.

13. Thornburgh, Ralph H. and Schoenborn, Barry J. Storage Area Networks – Designing and Implementing a Mass Storage System. Prentice Hall PTR, September 2000.

14. Barker, Richard and Massiglia, Paul. Storage Area Network Essentials: A Complete Guide to Understanding and Implementing SANs. Wiley Computer Publishing, October 2001.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

15. EMC. “Best Practices for Managing a Secure Enterprise Storage Network.” 3 July 2002. URL: http://www.emc.com/pdf/techlib/c902_best_practices.pdf (22 Aug. 2002).

16. FalconStor. “Fiber Channel Security Whitepaper.” URL: http://www.falconstor.com/Whitepapers/FibreChannelSecurity.pdf (22 Aug 2002).

17. Cook, Rick. “Masking and zoning for SAN security.” May 2002. URL: http://searchstorage.techtarget.com/tip/1,289483,sid5_gci821426,00.html (11 July 2002).

18. Poelker, Christopher. “Storage Networking: SANs Expert(s).” June 2001. URL: http://searchstorage.techtarget.com/ateQuestionNResponse/0,289625,sid5_cid400671_tax286192,00.html (11 July 2002).

19. Farley, Marc. “Storage Networking: A to Z Expert(s).” October 2001. URL: http://searchstorage.techtarget.com/ateQuestionNResponse/0,289625,sid5_cid417753_tax286191,00.html (11 July 2002).

20. Goodwin, Phil. “SAN Fabric Security: Defending the Port(s).” Not yet published. Stamford: META Group. (9 August 2002).

Bibliographic Sources

21. Pierce, Bill. “A ping Utility for Fiber Channel SANs.” Sys Admin September 2002 (2002): 22-25.

22. EMC. “Managing Storage Area Networks with ESN Manager.” 31 May 2002. URL: http://www.emc.com/pdf/techlib/c827_1.pdf (22 Aug. 2002).

23. Brocade. “Advancing Security in Storage Area Networks.” 2001. URL: http://www.brocade.com/products/pdf/Security2.pdf (22 Aug. 2002).

24. Coffed, Jeffery D. “Security for the SAN Workgroup.” 2000. URL: http://www.attotech.com/pdfs/SANSecure.pdf (22 Aug. 2002).

25. Screaming Media, Computer Technology Review. “SAN Security Architectures.” Oct. 2000. URL: http://industry.java.sun.com/javanews/stories/story2/0,1072,35188,00.html (11 July 2002).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

26. Radding, Alan. “SAN security: not a big problem – yet.” May 2001. URL: http://www.snwonline.com/implement/san_security_5-28-2001.asp?article_id=28 (11 July 2002).

27. Andress, Mandy. “SAN security goes IP.” May 2002. URL: http://www.infoworld.com/articles/fe/xml/02/05/13/020513fesecurity1.xml (11 July 2002).

28. SANS Institute. “GSNA Study Guide V11.” URL: http://www.giac.org/gsna_study_guide_v11.pdf (August 2002).

29. EMC Corporation, “Symmetrix 8000 Enterprise Plus Storage Systems Product Description Guide.” May 2002. URL: http://www.emc.com/pdf/products/symmetrix/symm8530.pdf (June 2002).

30. EMC Corporation, “EMC Connectrix Family Data Sheet.” November 2001. URL: http://www.emc.com/products/product_pdfs/ds/connectrix_ds.pdf (June 2002).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A – Corporate Data Classification Model

Business Requirements	Public	Private	Confidential	Restricted
Definition	Public data is non-sensitive information available for external release. The data owner acknowledges that there would be no adverse impact to The corporation in the case where this information was to be disclosed without authorization. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the company, its employees, or its customers. Security requirements are minimal at this level.	Internal data is Information that is only available to employees and approved non-employees. This information is not approved for general circulation outside the organization. There would be an inconvenience to The corporation, its partners, vendors, employees in the case where this information were to be disclosed without authorization. However, it would be unlikely to result in financial loss or serious damage to credibility. General authorization is required for users to access and communicate Internal	Sensitive company information. Intended for use only by designated named users. This information, if made public, would have significant adverse impact to The corporation. The company could incur financial or legal liabilities or there could be other adverse effects on The corporation, its partners, vendors, employees. Such information should not be copied or removed from the organization's operational control without specific authority. Security at	Information that is extremely sensitive and is intended for use only by named individuals within the company. Its unauthorized disclosure could seriously and adversely impact The corporation, its partners, vendors, employees. Security at this level is the highest possible.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Business Requirements	**Public**	**Private**	**Confidential**	**Restricted**
		Information.	this level should be very high.	
Examples	General marketing (brochures), retail pricing, parts catalogs, repair manuals, press releases	Employee communications, organizational charts, and telephone directories, employee benefits information, corporate procedures/policies	Dealer repair prices, wholesale prices of parts, vehicles, ordering information of parts, vehicles, Warranty claims and campaigns	Customer SSN information, legal documents, trade secrets, passwords / pins, strategic plans and financial results prior to release, Marketing strategy
Adversary & Length	No restrictions	Individual Weeks	Individual or Corporation 2 Years	Individual or Corporation 10 Years
Authentication	No restrictions	Unique User ID, Strong Password	Unique User ID, Strong Password	User ID, Two factor Authentication or Digital Certificate
Physical Transport	No restrictions	Internal: None External: Encryption (1) Authorization required	Internal: None External: Encryption (2) Authorization required	Internal: Encrypted External: Encryption (3) Authorization required
Storage Encryption	None	None	Encrypted on laptops and screened subnets.	Encrypted everywhere.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Strong Password:

Policy Based
90 day expiration
Minimum of 8 characters, Alphanumeric
15 failure disablement
Password history up to 5, minimum time between changes 24 hours

Encryption (1):

Public Key Size = 512
Session Key Size = 40

Encryption (2):

Public Key Size = 1024
Session Key Size = 112

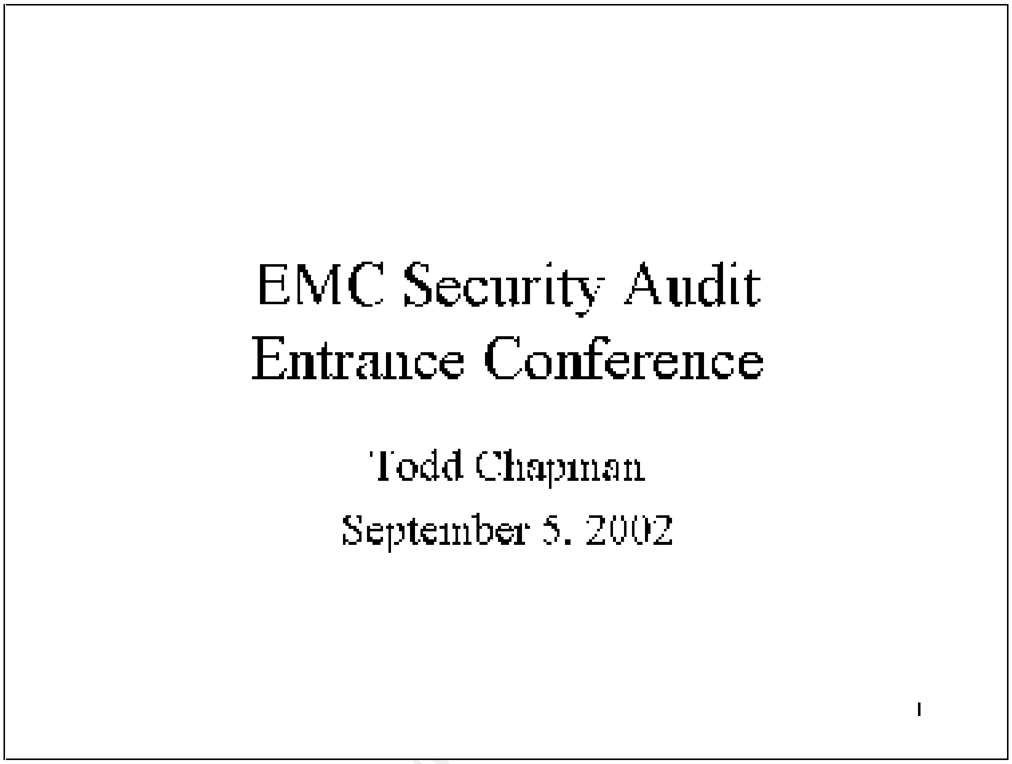
Encryption (3):

Public Key Size = 1024
Session Key Size = 128

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix B – Audit Entrance Conference Presentation

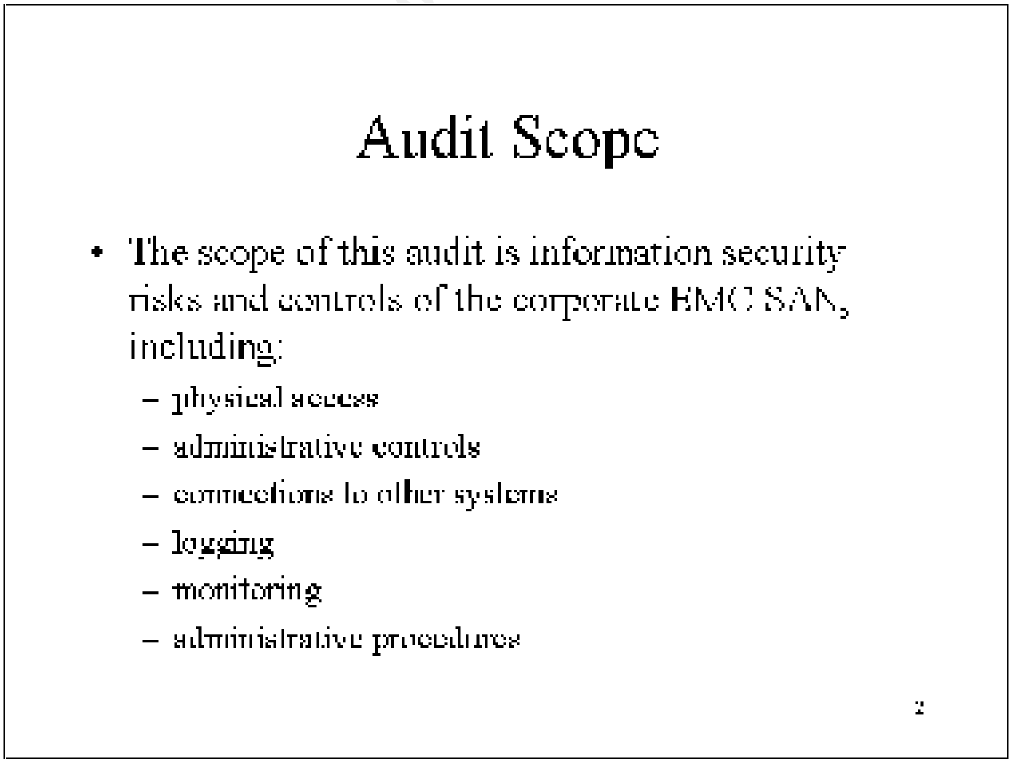


EMC Security Audit Entrance Conference

Todd Chapman

September 5, 2002

1

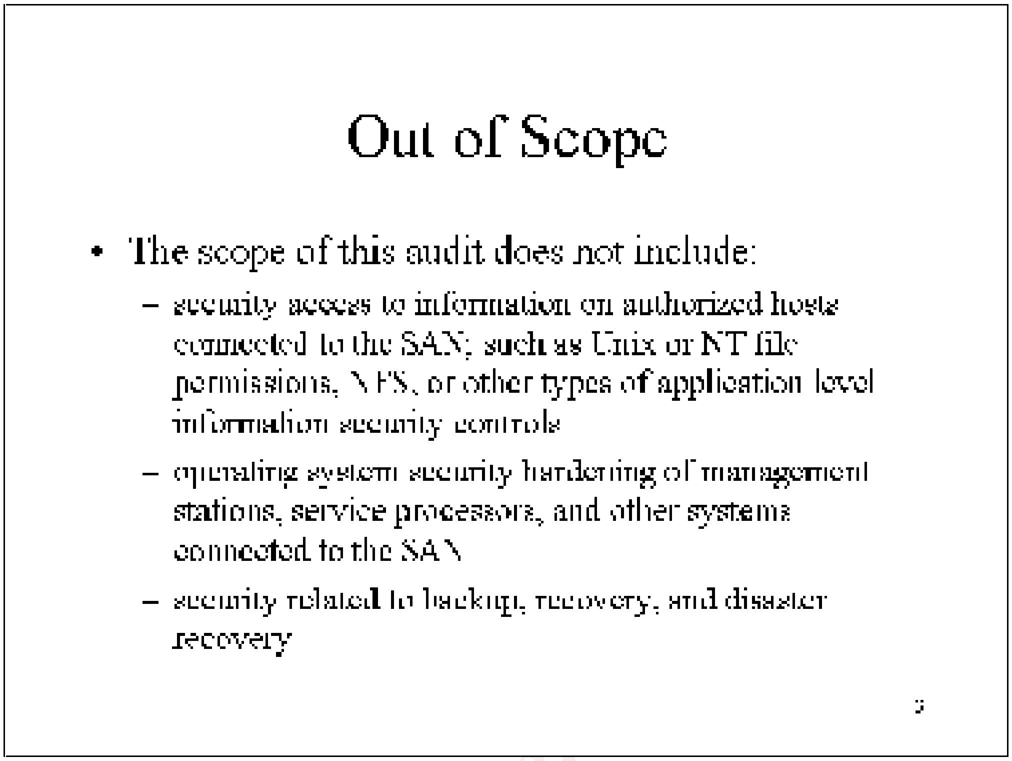


Audit Scope

- The scope of this audit is information security risks and controls of the corporate EMC SAN, including:
  - physical access
  - administrative controls
  - connections to other systems
  - logging
  - monitoring
  - administrative procedures

2

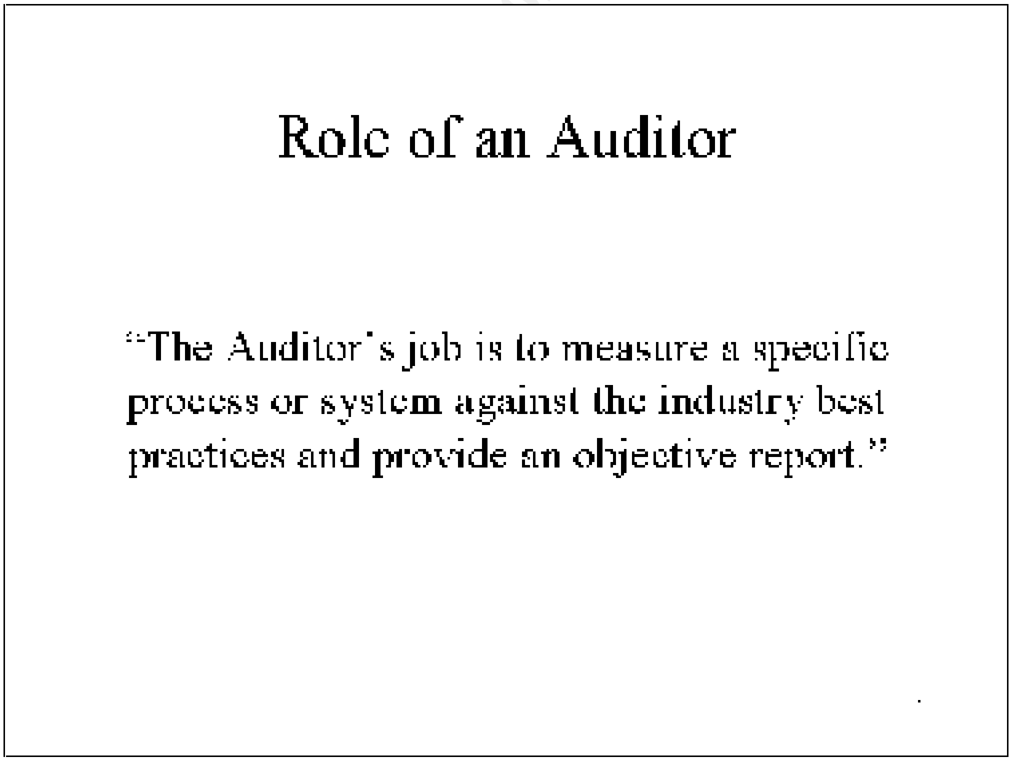
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Out of Scope

- The scope of this audit does not include:
  - security access to information on authorized hosts connected to the SAN; such as Unix or NT file permissions, NFS, or other types of application level information security controls
  - operating system security hardening of management stations, service processors, and other systems connected to the SAN
  - security related to backup, recovery, and disaster recovery

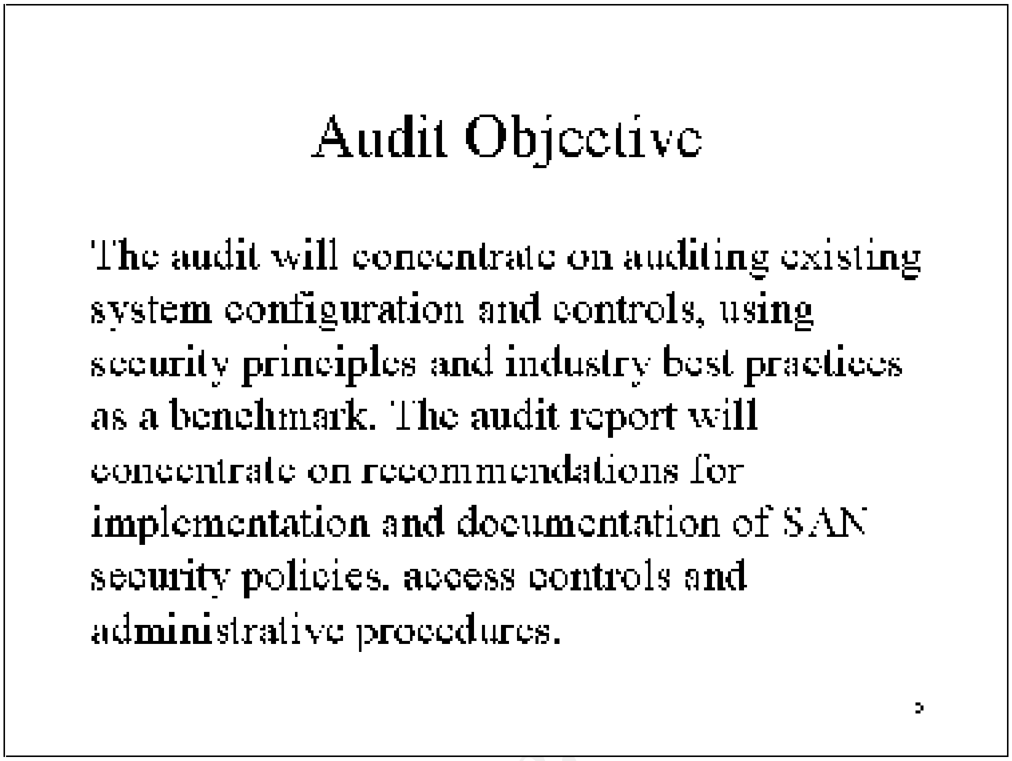
5



Role of an Auditor

"The Auditor's job is to measure a specific process or system against the industry best practices and provide an objective report."

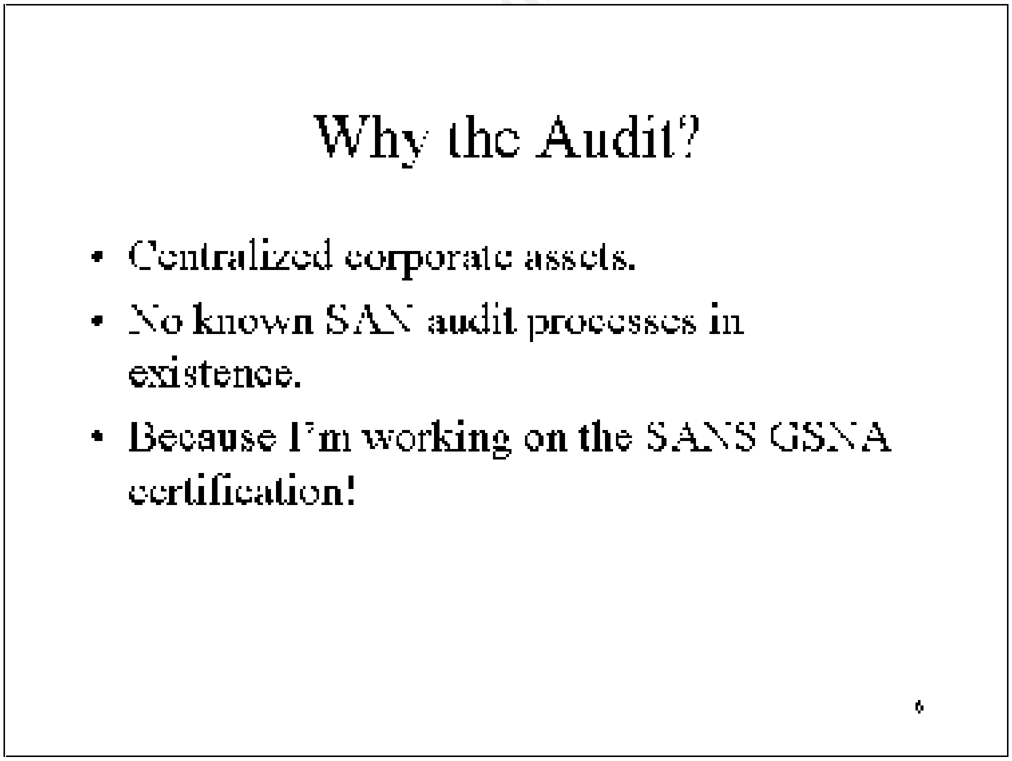
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Audit Objective

The audit will concentrate on auditing existing system configuration and controls, using security principles and industry best practices as a benchmark. The audit report will concentrate on recommendations for implementation and documentation of SAN security policies. access controls and administrative procedures.

5



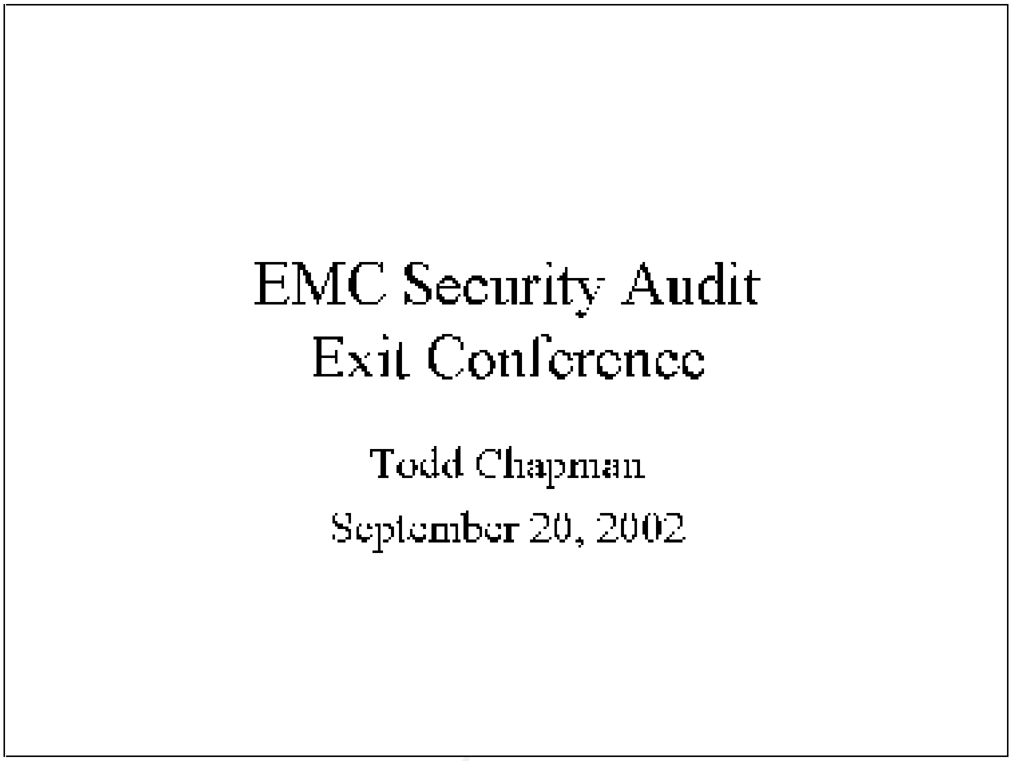
Why the Audit?

- Centralized corporate assets.
- No known SAN audit processes in existence.
- Because I'm working on the SANS GSNA certification!

6

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

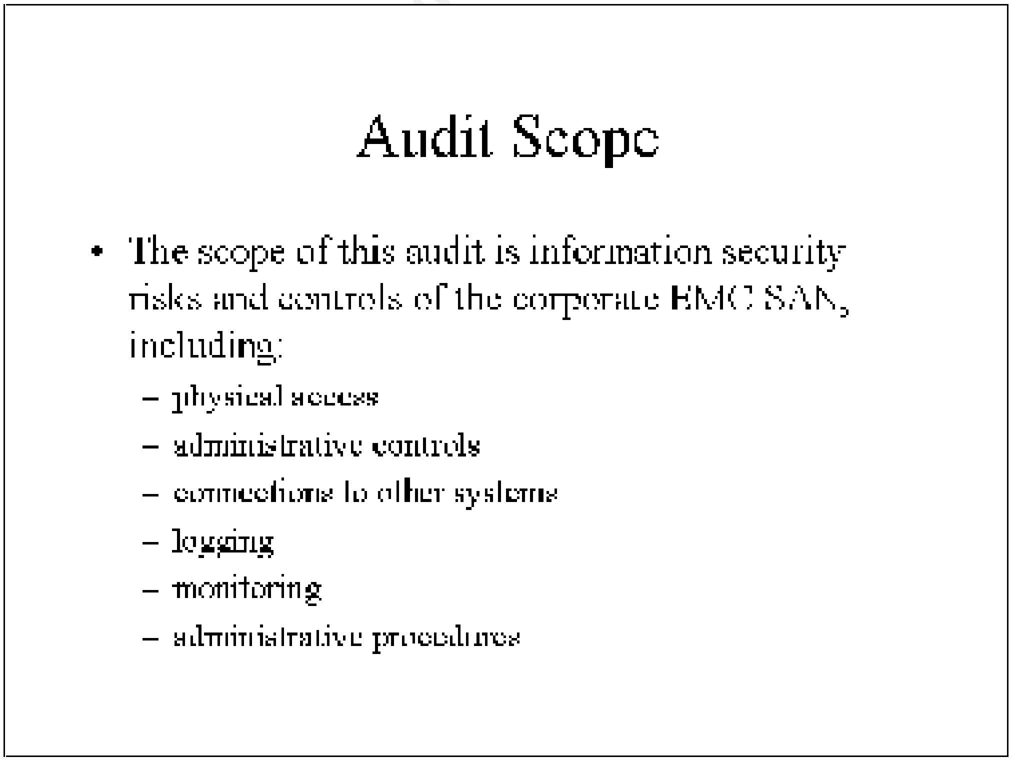
Appendix C – Audit Exit Conference Presentation



EMC Security Audit Exit Conference

Todd Chapman

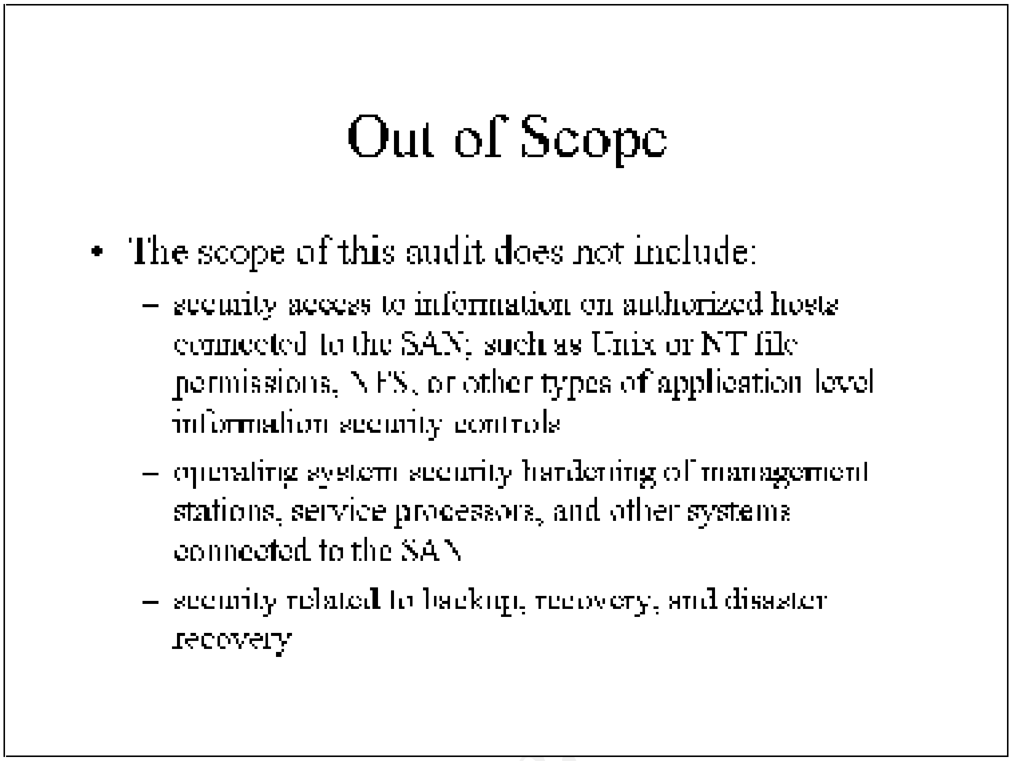
September 20, 2002



Audit Scope

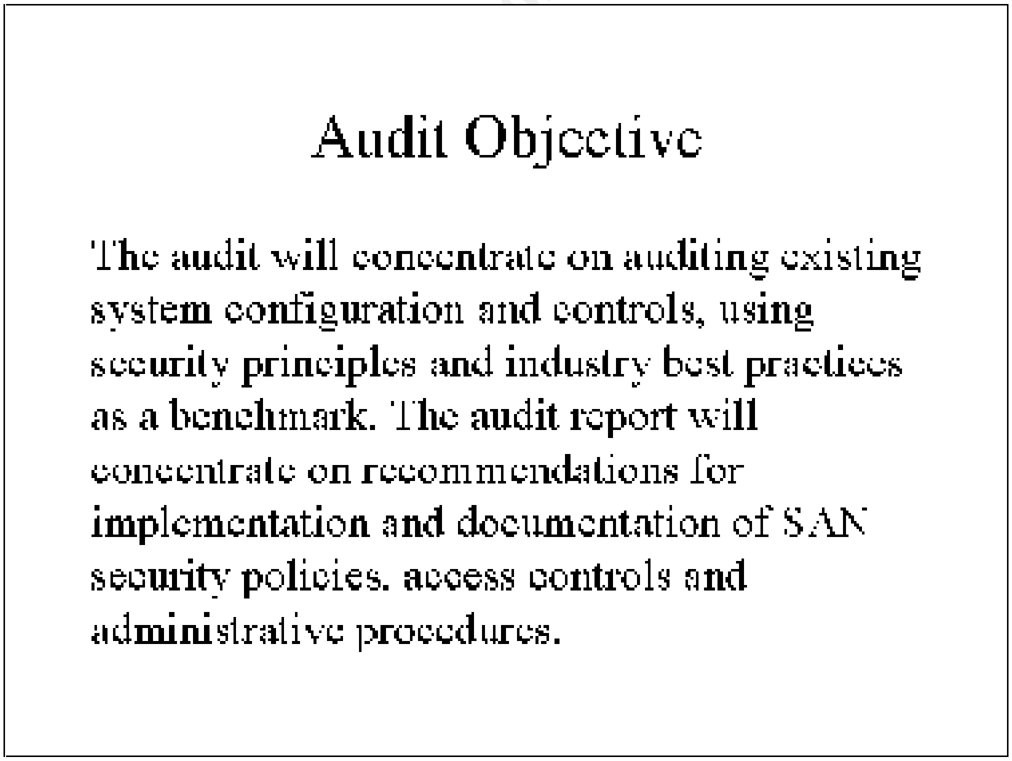
- The scope of this audit is information security risks and controls of the corporate EMC SAN, including:
  - physical access
  - administrative controls
  - connections to other systems
  - logging
  - monitoring
  - administrative procedures

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Out of Scope

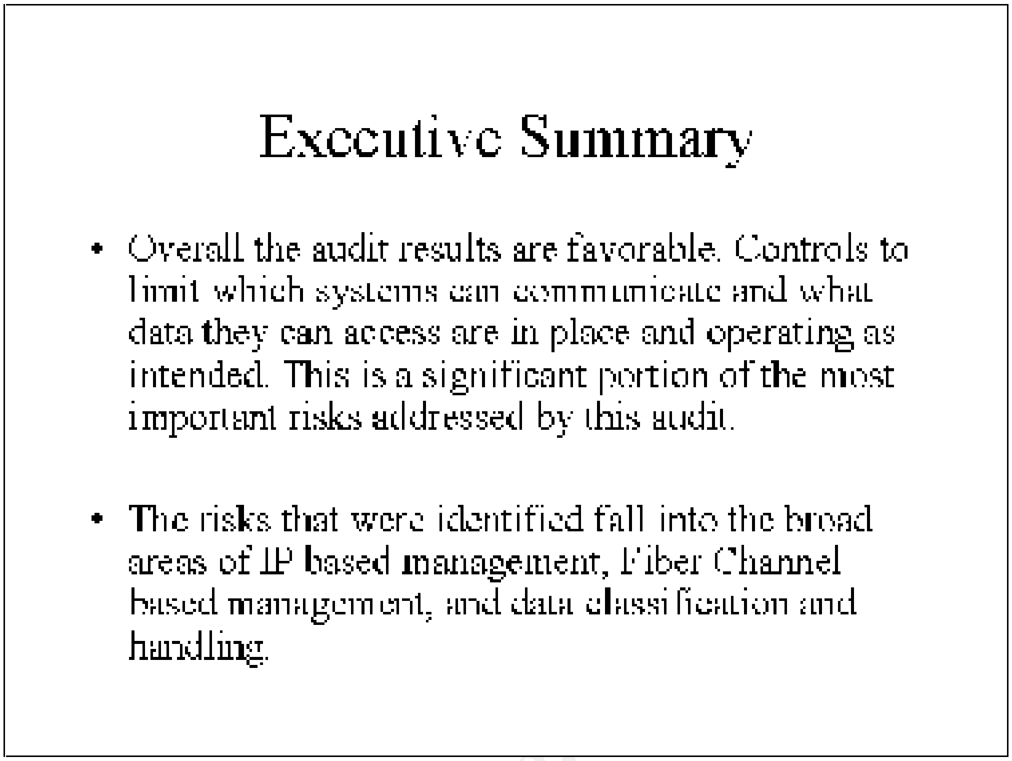
- The scope of this audit does not include:
  - security access to information on authorized hosts connected to the SAN; such as Unix or NT file permissions, NFS, or other types of application level information security controls
  - operating system security hardening of management stations, service processors, and other systems connected to the SAN
  - security related to backup, recovery, and disaster recovery



Audit Objective

The audit will concentrate on auditing existing system configuration and controls, using security principles and industry best practices as a benchmark. The audit report will concentrate on recommendations for implementation and documentation of SAN security policies. access controls and administrative procedures.

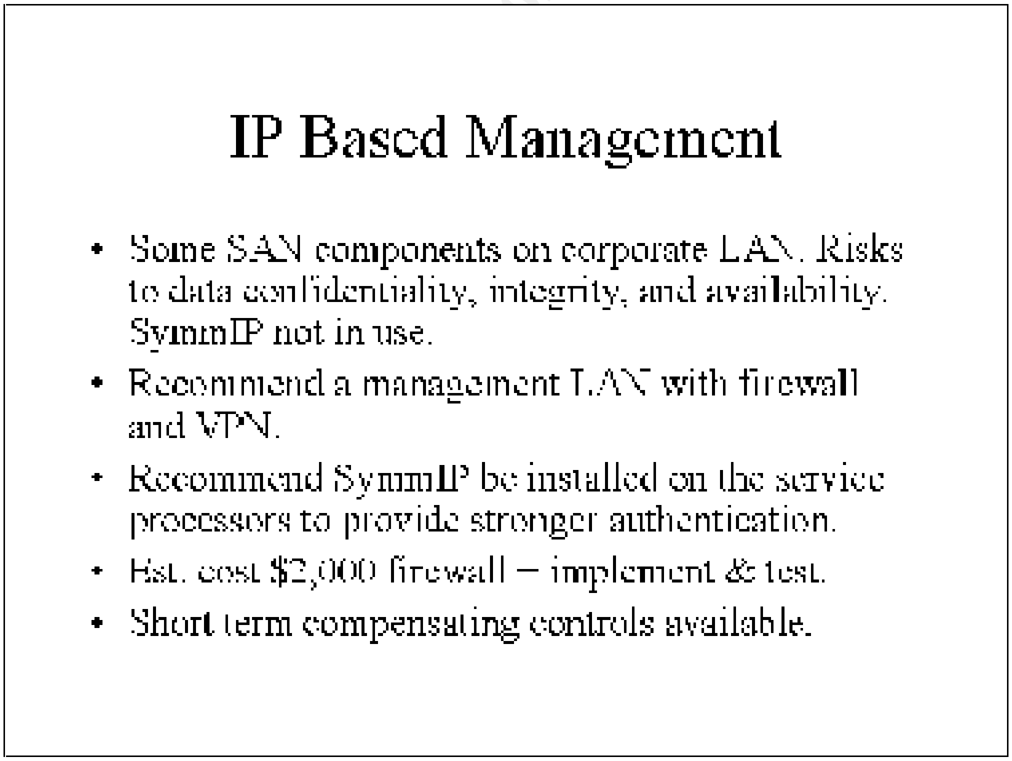
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Executive Summary

- Overall the audit results are favorable. Controls to limit which systems can communicate and what data they can access are in place and operating as intended. This is a significant portion of the most important risks addressed by this audit.

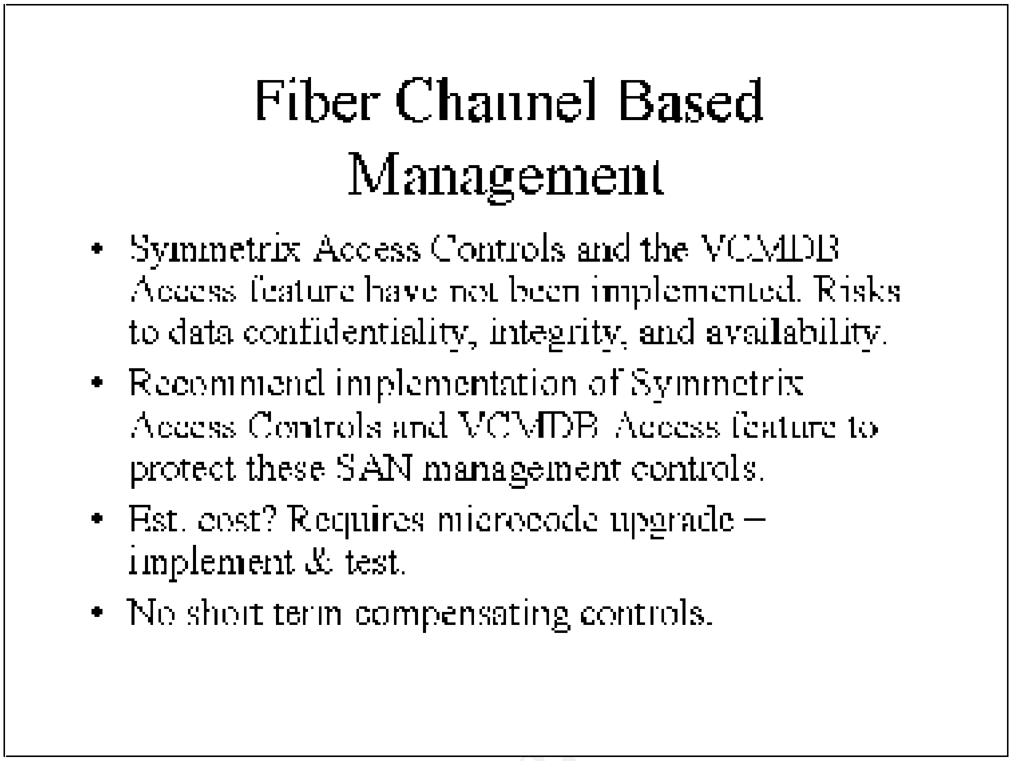
- The risks that were identified fall into the broad areas of IP based management, Fiber Channel based management, and data classification and handling.



IP Based Management

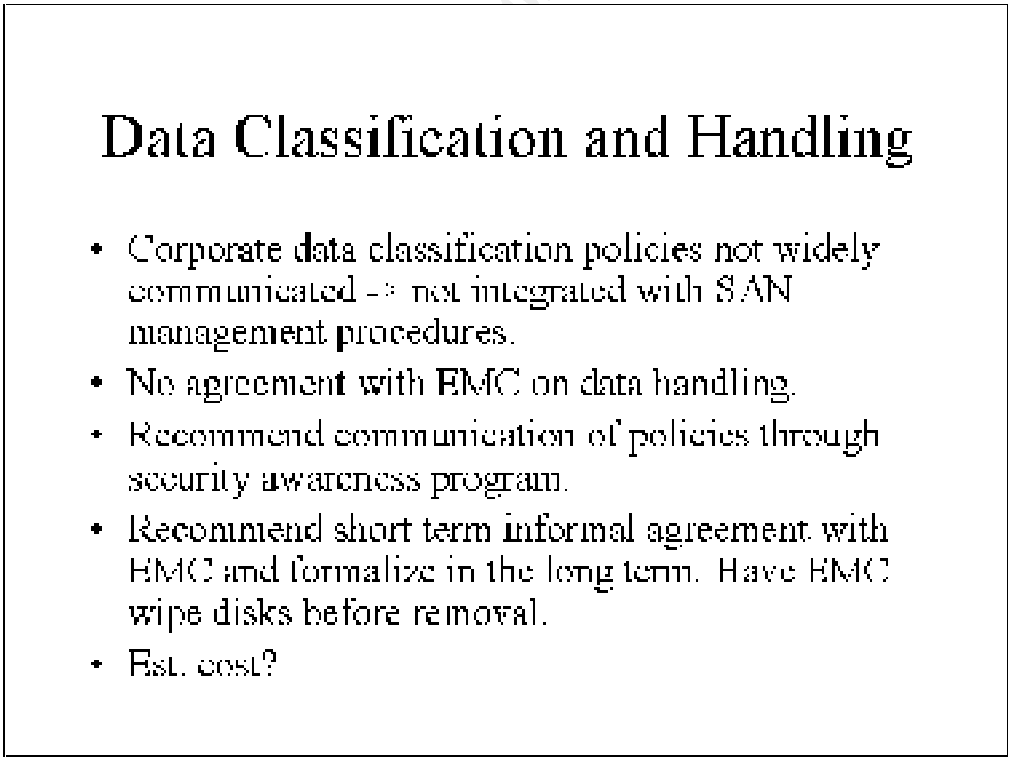
- Some SAN components on corporate LAN. Risks to data confidentiality, integrity, and availability. SymmIP not in use.
- Recommend a management LAN with firewall and VPN.
- Recommend SymmIP be installed on the service processors to provide stronger authentication.
- Est. cost $2,000 firewall – implement & test.
- Short term compensating controls available.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Fiber Channel Based Management

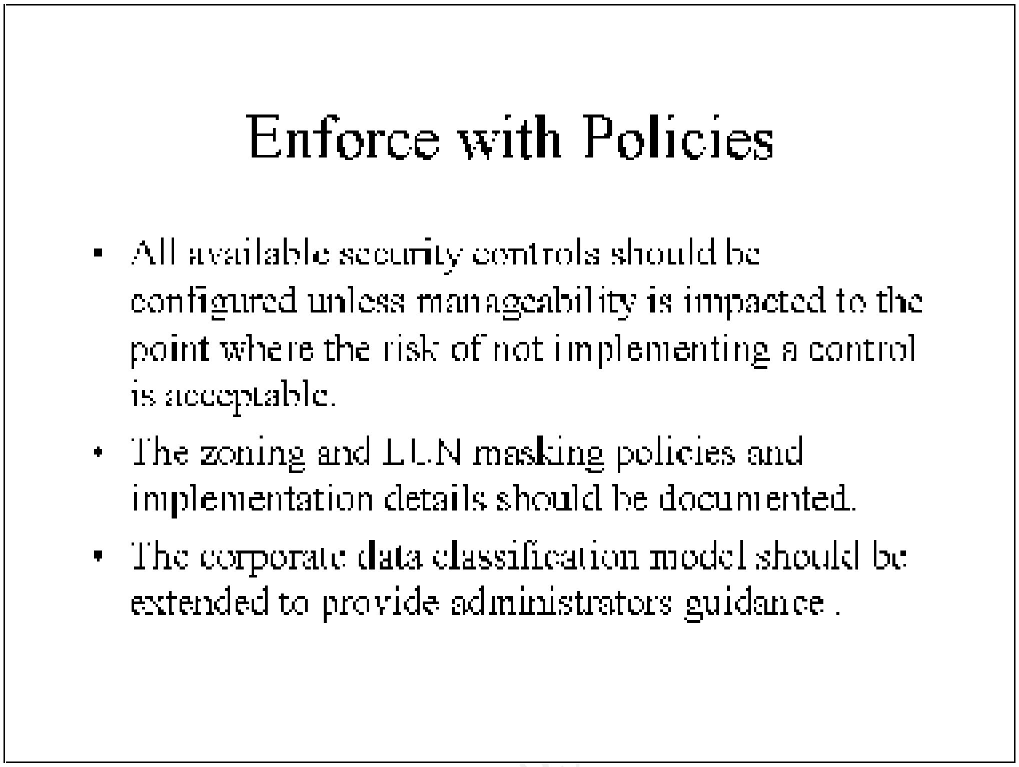
- Symmetrix Access Controls and the VCMDB Access feature have not been implemented. Risks to data confidentiality, integrity, and availability.
- Recommend implementation of Symmetrix Access Controls and VCMDB Access feature to protect these SAN management controls.
- Est. cost? Requires microcode upgrade – implement & test.
- No short term compensating controls.



Data Classification and Handling

- Corporate data classification policies not widely communicated -> not integrated with SAN management procedures.
- No agreement with EMC on data handling.
- Recommend communication of policies through security awareness program.
- Recommend short term informal agreement with EMC and formalize in the long term. Have EMC wipe disks before removal.
- Est. cost?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Enforce with Policies

- All available security controls should be configured unless manageability is impacted to the point where the risk of not implementing a control is acceptable.
- The zoning and LUN masking policies and implementation details should be documented.
- The corporate data classification model should be extended to provide administrators guidance .

© SANS Institute 2000 - 2002

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.