Storage Area Network (SAN) Checklist for Sharing Peripherals Across the Network Security Technical Implementation Guide Version 1 Release 1.3

19 MAY 2006

Developed by DISA for the DOD

Database Reference Number: ____________________________

Database entered by: ________________ Date: ____________

Technical Q/A by: ___________________Date: ____________

Final Q/A by: ______________________ Date: ____________

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

Summary of Changes

19 MAY 2006 – Modified various vulnerability checks and fixes.
14 April 2006 – Added VMS 6.0 review procedures.
14 April 2006 – Added VMS 6.0 Vulnerability Key to each checklist item.

VMS 6.0 SPAN SAN Review Procedures

The following is an outline of the process for performing a SPAN SAN review and entering the results using VMS 6.0.

1. Ensure that asset is registered in VMS under the correct organization. The asset will have the posture of Computing → Network → Data Network → SANS → SANS Switch or SANS Device depending on the asset type. If the asset has an identifiable operating system the posture will also include the appropriate OS.
2. If the asset is registered skip to Step 4 otherwise you must register the asset. You will find the appropriate selection criteria by selecting Asset Finding Maint → Assets/Findings → By Location → your location → Computing and then click on the file icon to create the asset.
3. On the General tab fill out the Host Name and appropriate values for the other fields on this tab.
4. Determine the enclave that the asset is within.
5. If the asset is in the correct enclave, skip to step 9.
6. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen.
7. For registered enclaves, choose the enclave.
8. If the enclave is not present, contact your team lead or your IAM and report that the enclave is not present.

   NOTE: Every effort should be made when registering or updating an asset to include the asset within an enclave.
9. Since at this time there is no scripted review process that automatically generates an import file, only the fields required by VMS need to be filled in unless there are other elements in the asset posture that require specific fields for their scripts. Any additional fields may be filed in for documentation purposes. The more documentation the better for identifying the system correctly.
10. Print the Checklist and perform a manual review for the SAN component,
11. Manually key results into VMS.
    Reviewers: By navigating to the pertinent visit, selecting the asset, and expanding the appropriate element for this review.
    Systems Administrators: by navigating to the your location, selecting the asset and expanding the appropriate element for review. If the asset is not found in the visit, contact your Team Lead and have them enter the asset into the visit.
    The appropriate element will be SANS Switch or SANS Device depending upon the assets posture.
12. Process any additional reviews required by additional elements within the asset posture.

SAN03.001.00 V0006603 CAT I Zoning is not used to protect the SAN.

8500.2 IA Control: ECCD-2, ECCD-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3.1

Vulnerability Zoning is not used to protect the SAN..

Checks

SPAN SAN03.001.00

The reviewer with the assistance of the IAO/NSO, verify that zoning is used to protect the SAN

Fixes

SPAN SAN03.001.00

Develop a zone topography, from the topography create a plan to implement zoning, obtain CM approval of the plan and then, following the plan, reconfigure the SAN to support zoning.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN03.002.00 V0006608 CAT II Hard zoning is not used to protect the SAN.

8500.2 IA Control: ECCD-1, ECCD-2

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3.1.3

Vulnerability Hard zoning is not used to protect the SAN.

Checks

SPAN SAN03.002.00

The reviewer, with the assistance of the IAO/NSO, will verify that hard zoning is used to protect the SAN.

Fixes

SPAN SAN03.002.00

If zoning has not been implemented, develop a zone topography, from the topography create a plan to implement hard zoning, obtain CM approval of the plan and then, following the plan, reconfigure the SAN to support hard zoning.

If zoning has been imple

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN03.003.00 V0006605 CAT II The default zone visibility is not set to "none"

8500.2 IA Control: ECCD-2, ECCD-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3.1

Vulnerability The default zone visibility setting is not set to “none”.

Checks

SPAN SAN03.003.00

Reviewer with the assistance of the IAO/NSO, verify that the default zone visibility setting is set to “none”.. If this setting is not available mark this check as N/A.

Fixes

SPAN SAN03.003.00

Locate all clients that have not been explicitly placed into a zone. Create a plan to explicitly place these clients into the correct zone(s) and after doing so the plan will include the modification of the default zone visibility setting to “none”. Obta

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN03.004.00 V0006606 CAT III Hard zoning, using Port World Wide Names (PWWN)

8500.2 IA Control: ECCD-1, ECCD-2

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3.1.1

Vulnerability Hard zoning, using Port World Wide Names (PWWN), is not used to protect the SAN.

Checks

SPAN SAN03.004.00

The reviewer with the assistance of the IAO/NSO, verify that hard zoning, using Port World Wide Names (PWWN), is used to protect the SAN.

Fixes

SPAN SAN03.004.00

Develop a plan to migrate the SAN to Hard Zoning, obtain CM approval of the plan, and the implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN03.005.00 V0006607 CAT I The zoning tables on all affected HBAs reset

8500.2 IA Control: DCSS-2, DCSS-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3.1.1

Vulnerability The zoning tables on all affected HBAs are not reset (force a state change update) after making zoning changes.

Checks

SPAN SAN03.005.00

The reviewer will interview the IAO/NSO to validate that the zoning tables on all affected HBAs are reset (force a state change update) after making zoning changes. This reset is a manual activity so the interview is to find that the IAO/NSO is aware of this requirement and does it.

Fixes

SPAN SAN03.005.00

Develop and document a procedure to reset (force a state change update) all effected HBAs whenever SAN zoning configuration changes are made.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.001.00 V0006609 CAT III SAN devices not added to the site SSAA

8500.2 IA Control: DCID-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability SAN devices are not added to the site System Security Authorization Agreement (SSAA).

Checks

SPAN SAN04.001.00

The reviewer will interview the IAO/NSO to validate that SAN devices are added to the site System Security Authorization Agreement (SSAA).

Fixes

SPAN SAN04.001.00

Update the SSAA following the SSAA review and acceptance procedures to include the SAN.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.002.00 V0006610 CAT II Compliance with Network Infrastructure and Enclave

8500.2 IA Control: DCCS-2, DCCS-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability The SANs are not compliant with overall network security architecture, appropriate enclave, and data center security requirements in the Network Infrastructure STIG and the Enclave STIG

Checks

SPAN SAN04.002.00

The reviewer will interview the IAO/NSO to validate that SANs are compliant with overall network security architecture, appropriate enclave, and data center security requirements in the Network Infrastructure STIG and the Enclave STIG

Fixes

SPAN SAN04.002.00

Perform a self assessment with the Network Infrastructure checklist and the Enclave checklist or schedule a formal review with FSO.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.003.00 V0006613 CAT II All security related patches are not installed.

8500.2 IA Control: VIVM-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability All security related patches are not installed.

Checks

SPAN SAN04.003.00

The reviewer will, with the assistance of the IAO/NSO, verify that all security related patches are installed.

Fixes

SPAN SAN04.003.00

After verifying that the patches do not adversely impact the production SAN, create a plan for installing the patches on the SAN, obtain CM approval of the plan, and implement the plan installing the patches.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.004.00 V0006619 CAT II Component Compliance with applicable STIG

8500.2 IA Control: DCCS-2, DCCS-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability Prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructure, components are not configured to meet the applicable STIG requirements.

Checks

SPAN SAN04.004.00

The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructure, components are configured to meet the applicable STIG requirements.

Fixes

SPAN SAN04.004.00

Perform a self assessment using the applicable checklists or scripts on any component device that has not been reviewed or request a formal review from FSO.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.005.00 V0006622 CAT II Servers and hosts OS STIG Requirements

8500.2 IA Control: DCCS-2, DCCS-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability Servers and other hosts are not compliant with applicable Operating System (OS) STIG requirements.

Checks

SPAN SAN04.005.00

The reviewer will interview the IAO/NSO and view the VMS to verify that servers and other hosts are compliant with applicable Operating System (OS) STIG requirements.

Fixes

SPAN SAN04.005.00

Perform a self assessment using the applicable OS checklists or scripts on any server or host in the SAN that has not been reviewer or request a formal review from FSO.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.006.00 V0006623 CAT I Anti-virus on servers and host.

8500.2 IA Control: ECVP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability Vendor supported, DOD approved, anti-virus software is not installed and configured on all SAN servers in accordance with the applicable operating system STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition

Checks

SPAN SAN04.006.00

The reviewer will verify that vendor supported, DOD approved, anti-virus software is installed and configured on all SAN servers in accordance with the applicable operating system STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition tables. If an OS review has reciently been completed verify that the anti-virus check was not a finding. Otherwise perform a manual check as described in the applicable OS checklist.

Fixes

SPAN SAN04.006.00

Install and correctly configure a DOD approved anti-virus.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.007.00 V0006628 CAT II SAN Topology Drawing

8500.2 IA Control: DCHW-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability A current drawing of the site’s SAN topology that includes all external and internal links, zones, and all interconnected equipment is not being maintained.

Checks

SPAN SA04.007.00

The reviewer will interview the IAO/NSO and view the drawings supplied to verify that a current drawing of the site’s SAN topology that includes all external and internal links, zones, and all interconnected equipment.

Fixes

SPAN SAN04.007.00

Create drawing of the site’s SAN topology that includes all external and internal links, zones, and all interconnected equipment.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.008.00 V0006631 CAT II Physical Access to SAN Network Devices

8500.2 IA Control: PECF-1, PECF-2

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability All the network level devices interconnected to the SAN are not located in a secure room with limited access.

Checks

SPAN SAN04.008.00

The reviewer will interview the IAO/NSO and view the network level devices to verify whether they are located in a secure room with limited access.

Fixes

SPAN SAN04.008.00

Develop a plan to move the network level devices to a location/room where the can be physically secured in a manner appropriate to the classification level of the data the handle. Obtain CM approval of the plan and then implement the plan moving the devi

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.009.00 V0006632 CAT II SAN Fabric Switch User Accounts with Passwords

8500.2 IA Control: IAIA-2, IAIA-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.1, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran Appendix B

Vulnerability Individual user accounts with passwords are not set up and maintained for the SAN fabric switch.

Checks

SPAN SA04.009.00

The reviewer, with the assistance of the IAO/NSO, will verify that individual user accounts with passwords are set up and maintained for the SAN fabric switch.

Fixes

SPAN SA04.009.00

Develop a plan to reconfigure the SAN fabric switch to require user accounts and passwords. This plan also needs to include the creation and distribution of user accounts and passwords for each administrator who requires access to the SAN fabric switch.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.010.00 V0006633 CAT III Sensitive Data in Transit Encryption

8500.2 IA Control: ECNK-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.1

Vulnerability All fabric switches for SANs that process sensitive information are not configured to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications.

Checks

SPAN SAN04.010.00

The reviewer will, with the assistance of the IAO/NSO, verify that all fabric switches are configured to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications for SANs that process sensitive information.

Fixes

SPAN SAN04.010.00

Develop a plan to reconfigure the SAN fabric switches to use FIPS-140-1/2 validated algorithms to encrypt switch-to-switch communications for SANs that process sensitive information. Obtain CM approval for the plan and then implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.011.00 V0006634 CAT III SAN Switch encryption and DOD PKI

8500.2 IA Control: IAIA-2, IAIA-1, ECNK-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.1

Vulnerability The fabric switches are not protected by encryption and DOD PKI and/or that the manufacturer’s default keys have not been changed prior to attaching to the SAN Fabric for SANs processing sensitive information..

Checks

SPAN SAN04.011.00

The reviewer will, with the assistance of the IAO/NSO, verify that fabric switches are protected by encryption and DOD PKI and that the manufacturer’s default keys are changed prior to attaching to the SAN Fabric for SANs processing sensitive information.

Fixes

SPAN SAN04.011.00

Develop a plan to implement encryption, DOD PKI and change the manufacturers default keys. Obtain CM approval for the plan and then execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.012.00 V0006635 CAT II SAN Network Management Ports Fabric Switch

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.1

Vulnerability Network management ports on the SAN fabric switches except those needed to support the operational commitments of the sites are not disabled.

Checks

SPAN SAN04.012.00

The reviewer will, with the assistance of the IAO/NSO, verify that all network management ports on the SAN fabric switches are disabled except those needed to support the operational commitments of the sites.

Fixes

SPAN SAN04.012.00

Develop a plan to locate and disable all network management ports that are not required to support the operational commitments of the sites. Obtain CM approval of the plan and then execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.013.00 V0006636 CAT II SAN management out-of-band or direct connect

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.1

Vulnerability SAN management is accomplished using the out-of-band or direct connection method.

Checks

SPAN SAN04.013.00

The reviewer will interview the IAO and view the SAN network drawings provided.

Fixes

SPAN SAN04.013.00

Develop a plan to migrate the SAN management to an out-of-band network or a direct connect method. Obtain CM approval for the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.014.00 V0006637 CAT III Management Console to SAN Fabric DOD PKI protected

8500.2 IA Control: IAIA-2, IAIA-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.2

Vulnerability Communications from the management console to the SAN fabric are not protected using DOD PKI.

Checks

SPAN SAN04.014.00

The reviewer will, with the assistance of the IAO/NSO, verify that communications from the management console to the SAN fabric are protected using DOD PKI.

Fixes

SPAN SAN04.014.00

Develop a plan to migrate to the use of DOD PKI authentication between the SAN management console and the SAN fabric. Obtain CM approval of the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.015.00 V0006638 CAT III Default PKI keys

8500.2 IA Control: IAIA-2, IAIA-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.2

Vulnerability The manufacturer’s default PKI keys have not been changed prior to attaching the switch to the SAN Fabric.

Checks

SPAN SAN04.015.00

The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer’s default PKI keys have been changed prior to attaching the switch to the SAN Fabric.

Fixes

SPAN SAN04.015.00

Depending on the functionality allowed by the device, develop a plan remove, disable or change the manufacturer’s default PKI certificate so that it cannot be used for identification and authorization. Obtain CM approval for the plan and implement the pl

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.016.00 V0006639 CAT III FIPS 140-1/2 for management to fabric.

8500.2 IA Control: ECNK-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.2

Vulnerability The SAN is not configured to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.

Checks

SPAN SAN04.016.00

The reviewer will, with the assistance of the storage administrator, verify that the SAN is configured to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.

Fixes

SPAN SA04.016.00

Develop a plan to implement FIPS-140-1/2 validated encryption to protect management-to-fabric communications. Obtain CM approval of the plan and execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.017.00 V0006645 CAT I Password SAN Management Console and Ports

8500.2 IA Control: IAIA-1, IAIA-2

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.2

Vulnerability All SAN management consoles and ports are not password protected.

Checks

SPAN SAN04.017

The reviewer will, with the assistance of the IAO/NSO, verify that all SAN management consoles and ports are password protected.

Fixes

SPAN SAN04.017.00

Develop a plan for implementing password protection on the SAN’s management consoles and ports. Obtain CM approval of the plan and execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.018.00 V0006646 CAT I Default SAN Management Software Password

8500.2 IA Control: IAIA-1, IAIA-2

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.2

Vulnerability The manufacturer’s default passwords have not been changed for all SAN management software.

Checks

SPAN SAN04.018.00

The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer’s default passwords have been changed for all SAN management software.

Fixes

SPAN SAN04.018.00

Develop a plan to change manufacturer’s default passwords for all SAN management software. Obtain CM approval of the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.019.00 V0006647 CAT I SAN Fabric Zoning List Deny-By-Default

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability The SAN fabric zoning lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the given port or by the site.

Checks

SPAN SAN04.019.00

The reviewer will, with the assistance of the IAO/NSO, verify that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols not required on the given port or by the site.

Fixes

SPAN SAN04.019.00

Develop a plan to identify all services and protocols needed by each port in the SAN, modify the routing lists to enforce a Deny-by-Default policy and allow only the identified services and protocols on each port that requires them. Obtain CM approval fo

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.020.00 V0006648 CAT III Logging Failed Access to Port, Protocols, Services

8500.2 IA Control: ECAR-2, ECAR-1, ECAR-3

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability Attempts to access ports, protocols, or services that are denied are not logged..

Checks

SPAN SAN04.020.00

The reviewer will, with the assistance of the IAO/NSO, verify that all attempts to any port, protocol, or service that is denied are logged.

Fixes

SPAN SAN04.020.00

Develop a plan to implement the logging of failed or rejected ports, protocols or services requests. The plan should include a projection of the storage requirements of the logged events. Obtain CM approval of the plan and execute it.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.021.00 V0006652 CAT II SNMP usage and configuration.

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability Simple Network Management Protocol (SNMP) is used and it is not configured in accordance with the guidance contained in the Network Infrastructure STIG.

Checks

SPAN SAN04.021.00

With the assistance of the IAO/NSO, verify that if Simple Network Management Protocol (SNMP) is used, it is configured in accordance with the guidance contained in the Network Infrastructure STIG section 5.1.2.

Fixes

SPAN SAN04.021.00

Develop a plan to implement SNMP that is compliant with the Network Infrastructure STIG. Obtain CM approval and execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.022.00 V0006656 CAT I Authorized IP Addresses allowed for SNMP

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability Unauthorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices.

Checks

SPAN SAN04.022.00

The reviewer will, with the assistance of the IAO/NSO, verify that only authorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices. This can be done with by checking the ACLs for the SAN device ports.

Fixes

SPAN SAN04.022.00

Develop a plan to restrict SNMP access to SAN devices to authorized IP addresses. Obtain CM approval for the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.023.00 V0006657 CAT II Only Internal Network SNMP Access to SAN

8500.2 IA Control: EBRP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability The IP addresses of the hosts permitted SNMP access to the SAN management devices do not belong to the internal network.

Checks

SPAN SAN04.023.00

The reviewer will, with the assistance of the IAO/NSO, verify that the IP addresses of the hosts permitted SNMP access to the SAN management devices belong to the internal network. The ACLs for the SAN ports should be checked.

Fixes

SPAN SAN04.023.00

Develop a plan to restrict SNMP access to SAN devices to only internal network IP addresses. Obtain CM approval of the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.024.00 V0006660 CAT III Fibre Channel network End-User Platform Restricted

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability End-user platforms are directly attached to the Fibre Channel network or access storage devices directly.

Checks

SPAN SAN04.024.00

The reviewer will, with the assistance of the IAO/NSO, verify that end-user platforms are not directly attached to the Fibre Channel network and may not access storage devices directly. If the SAN is small with all of its components collocated, this can be done by a visual inspection but in most cases the reviewer will have to check the SAN network drawing.

Fixes

SPAN SAN04.024.00

Develop a plan to remove end-user platforms from the SAN. Obtain CM approval for the plan and implement the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN04.025.00 V0007081 CAT II SAN Fixed IP Required.

8500.2 IA Control: DCBP-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4.3

Vulnerability SAN components are not configured with fixed IP addresses.

Checks

SPAN SAN04.25.00

The reviewer with the assistance of the SA will verify that all SAN components are configured with fixed IP addresses.

Fixes

SPAN SAN04.025.00

Configure all SAN components to have fixed IP addresses.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

SAN05.001.00 V0006661 CAT II Backup of critical SAN Software and configurations

8500.2 IA Control: COSW-1

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.5

Vulnerability Fabric switch configurations and management station configuration are not archived and/or copies of the operating system and other critical software for all SAN components are not stored in a fire rated container or are not collocated with the operational

Checks

SPAN SAN05.001.00

The reviewer will interview the IAO/NSO and view the stored information to verify that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software.

Fixes

SPAN SAN05.001.00

Develop a plan that will ensure that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes: