



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 permitted without express written permission.

Security Audit of a Solaris Server Running Sun ONE Directory Server v5.2

Philip Hlavaty
GIAC GSNA Practical Assignment
Version 3.2
March 21, 2005

Abstract

The Sun ONE Directory Server v5.2 is an LDAP-based application that can act as a central repository for user information on any given network. It is imperative that the application, along with server on which it resides, is thoroughly secure. This report will provide an audit checklist that will test a variety of factors that, if left unchecked, can lead to data compromise. Towards the end of the report, we will explore potential solutions for correcting any problems that may have been discovered on the system.

© SANS Institute 2000 - 2005, Author retains full rights.

Table of Contents

<u>Abstract</u>	2
<u>1 Research in Audit, Measurement Practice, and Control</u>	5
<u>1.1 Scope of the Audit</u>	5
<u>1.2 Purpose of the Directory Server</u>	5
<u>1.3 System to be Audited</u>	5
<u>1.4 Risk Evaluation</u>	6
<u>1.4.1 Documentation/Training</u>	7
<u>1.4.2 Physical Security</u>	7
<u>1.4.3 Solaris Security/System Hardening</u>	8
<u>1.4.4 Application Setup</u>	8
<u>1.5 Current State of Practice</u>	9
<u>2 Create an Audit Checklist</u>	13
<u>2.1 Item #1 – Access to Updated Documentation</u>	13
<u>2.2 Item #2 – Process for Documentation Control</u>	14
<u>2.3 Item #3 – Physical Access to the Server</u>	14
<u>2.4 Item #4 – Physical Safety Controls</u>	15
<u>2.5 Item #5 – Installation of a Solaris Hardening Package</u>	15
<u>2.6 Item #6 – Tripwire Installation and Configuration</u>	17
<u>2.7 Item #7 – Syslog Setup</u>	17
<u>2.8 Item #8 – Solaris Patch Updates</u>	18
<u>2.9 Item #9 – Configuration of DS Access Controls</u>	18
<u>2.10 Item #10 – Password Strength</u>	19
<u>2.11 Item #11 – DS Logging Setup</u>	19
<u>2.12 Item #12 – Replication Setup</u>	20
<u>2.13 Item #13 – Password Security Policy</u>	21
<u>2.14 Item #14 – Lockdown of DS-specific Directories</u>	22
<u>2.15 Item #15 – Data Backup Plan</u>	22
<u>2.16 Item #16 – Startup/Shutdown Scripts</u>	23
<u>2.17 Item #17 – Vulnerability Scans</u>	23
<u>3 Conduct the Audit Testing, Evidence and Findings</u>	25
<u>3.1 Test #1 – Access to Updated Documentation</u>	25
<u>3.2 Test #2 – Process for Documentation Control</u>	26
<u>3.3 Test #3 – Physical Access to the Server</u>	27
<u>3.4 Test #4 – Physical Safety Controls</u>	28
<u>3.5 Test #5 – Installation of a Solaris Hardening Package</u>	28
<u>3.6 Test #6 – Tripwire Installation and Configuration</u>	34
<u>3.7 Test #7 – Syslog Setup</u>	35
<u>3.8 Test #8 – Solaris Patch Updates</u>	40
<u>3.9 Test #9 – Configuration of DS Access Controls</u>	40
<u>3.10 Test #10 – Password Strength</u>	43
<u>3.11 Test #11 – DS Logging Setup</u>	44
<u>3.12 Test #12 – Replication Setup</u>	47

<u>3.13</u>	<u>Test #13 – Password Security Policy</u>	57
<u>3.14</u>	<u>Test #14 – Lockdown of DS-specific Directories</u>	59
<u>3.15</u>	<u>Test #15 – Data Backup Plan</u>	60
<u>3.16</u>	<u>Test #16 – Startup/Shutdown Scripts</u>	61
<u>3.17</u>	<u>Test #17 – Vulnerability Scans</u>	63
<u>4</u>	<u>Audit Report</u>	66
<u>4.1</u>	<u>Executive Summary</u>	66
<u>4.2</u>	<u>Audit Findings and Recommendations</u>	67
<u>4.2.1</u>	<u>Documentation/Training</u>	67
<u>4.2.2</u>	<u>Physical Security</u>	68
<u>4.2.3</u>	<u>Solaris Security/System Hardening</u>	68
<u>4.2.4</u>	<u>Application Setup</u>	70
<u>Appendix A</u>		74
	<u>gsna-be-ldap2.SOL.20050312</u>	74
	<u>/etc/inetd.conf</u>	83
	<u>/etc/system</u>	87
	<u>/etc/services</u>	88
<u>Appendix B</u>		92
<u>Appendix C</u>		95

© SANS Institute 2000 - 2005, Author retains full rights.

2 Research in Audit, Measurement Practice, and Control

2.1 Scope of the Audit

This paper will describe the audit process of a Solaris Enterprise server running the Sun ONE Directory Server (DS) v5.2 application. This application is an extremely powerful and versatile distributed directory server based on an industry standard known as Lightweight Directory Access Protocol (LDAP) [24]. This DS is a Java-based application that is ideal for handling high volumes of user authentication traffic. As a result, this particular DS is one of the most widely deployed LDAP-based applications on the market. [23]

Because of its usefulness and popularity, it is important to understand the security risks involved in using this particular application because of the sensitivity of the information that Directory Servers can contain. If this system is compromised, an attacker can obtain potentially damaging information about each user that is stored in the database. This audit will attempt to uncover any potential security threats and vulnerabilities within the Sun ONE DS v5.2 so as to minimize the risk of compromising any sensitive information.

2.2 Purpose of the Directory Server

The Sun ONE DS that is being audited for this paper is used as the primary method of authentication for the system in which it exists. The information for users that attempt to access the web server from outside the firewalls, for example, is stored in this DS. This information includes user names, passwords, password lockout and expiration criteria, and other personal data that is used by the web server. The DS is also used to authenticate users who are logging in to other Solaris servers in the system via SSH. The PAM modules on these servers have been modified so that all authentications take place via the LDAP protocol. Our DS has also been modified so that we enforce our internal security policy, where we lockout users after a certain period of inactivity, and we force users to change their passwords on a regular basis.

2.3 System to be Audited

The Sun ONE Directory Server v5.2 is installed on a Sun Ultra 5/10 UPA/PCI Solaris server running SunOS 5.9. There is an UltraSPARC-III processor running at 360 MHz on the server, and it has 512 MB of RAM and a system clock frequency of 90 MHz. The server is protected from the Internet by:

- Two Cisco border routers
- Two f5 Big IP Load Balancers on the external interface of the network
- Two Cyberguard v5.2 firewalls
- Two f5 Big IP Load Balancers on the internal interface of the network

Other servers on the internal interface of the firewall can access the LDAP server via a Cisco switch. All traffic to and from each of the servers on the back end must go through this switch.

One of the most useful features of Sun ONE DS v5.2 is its remarkable replication ability. If a DS is installed on two separate servers in a network, they can replicate their information to each other on an almost real-time basis [25]. As part of our network configuration, the load balancers just inside the firewalls direct all LDAP related traffic to the primary DS server, and then this server replicates all its information to the standby DS server. This ensures that no data is lost between the two servers if they are both trying to replicate the information to each other simultaneously.

For the purposes of this audit, we are going to focus our efforts only on the primary DS server in this network. The secondary DS server will come into play when we audit the replication setup. The same tests in the audit checklist could be run against the secondary DS server, but in order to simplify this report, the audit will be run only against the primary server.

A simplified version of the network is shown in the diagram below (Figure 1):

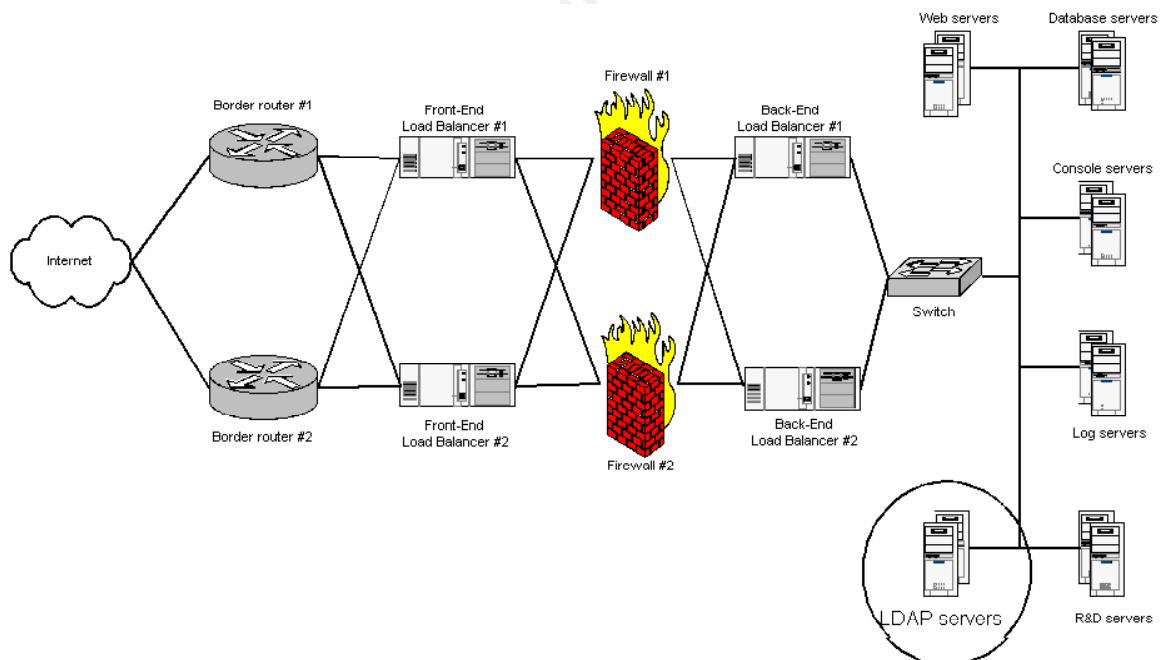


Figure 1 – Network Diagram

2.4 Risk Evaluation

Before performing this audit, we must first understand what the primary objective of this audit needs to be. According to Hoelzer's SANS presentation on Auditing, every auditor's primary objective is to measure and report on risk.

The simplest way to define risk is that it is a combination of the potential threats and vulnerabilities to the system being audited [8]. The tables in the following sections illustrate some of the threats and vulnerabilities in this system, and they attempt to specify how much risk each poses to the system.

2.4.1 Documentation/Training

Documentation/Training Risks			
Vulnerability	Threat	Likelihood	Risks/Impacts
Incomplete or out-of-date documentation (including installation instructions)	Medium	Medium-to-High	Medium-to-high risk. Bad documentation can easily lead to: <ul style="list-style-type: none"> • Poorly configured or inconsistent systems. • Increased incident handling times. • Lack of trust from management. • Lack of a proper backup/recovery procedure
Lack of proper training documentation and materials for new administrators	Medium	Medium-to-High	Medium-to-high risk. The vulnerability listed above can be a significant factor in creating this vulnerability. As new administrators become responsible for the upkeep and maintenance of the system, bad training documentation can lead to a significant loss of productivity from both the old and new administrators.

2.4.2 Physical Security

Physical Security Risks			
Vulnerability	Threat	Likelihood	Risks/Impacts
Granting access to the system to users that do not need access to it	Low-to-Medium	Medium	Low-to-Medium risk. Even though the system may be in a “trusted” environment, users that do not need access to a system (which includes both physical access and login privileges) should not be granted access. Unauthorized access increases the likelihood of lost or corrupted data, and the chances of accidental damage increase. [7]
Lack of disaster/data recovery plans	High	Medium	Potentially high risk. In the event of an uncontrolled mishap or disaster, the system and the data it contains must be physically secured or replaced as soon as possible in order to avoid the loss of invaluable data and time. [7]
Lack of safety devices or safety training	Medium-to-High	Low-to-Medium	Medium risk. Improper safety equipment and training to use such equipment can lead to physical system damage. [7]

2.4.3 Solaris Security/System Hardening

Solaris Security/System Hardening Risks			
Vulnerability	Threat	Likelihood	Risks/Impacts
Lack of installation of a proper Solaris hardening package	High	Medium	Medium-to-High risk. Improper hardening of a Solaris server can lead to a variety of exploits that would leave the system vulnerable to internal and external attacks. Failure to harden a server will likely result in unnecessary ports and services open on the server.
Improper logging client/server setup	Medium	Medium	Medium risk. If a logging service is not set up to log messages either locally to the system or to a centralized logging server, it will be nearly impossible to trace potential defects or intrusions into the system.
Out-of-date patching on the system	Medium	High	Medium-to-High risk. New patches are introduced so frequently that it is difficult to keep up with the most up-to-date patches, especially if the system is not set up for automatic patch downloading. Out-of-date patching can leave obscure security holes open in the system.
Failure to address other miscellaneous and network controls	Medium	High	Medium-to-High risk. The following items (among others) need to be considered to ensure that a server is properly hardened: <ul style="list-style-type: none">• Default users need to be locked down.• Remove unnecessary startup scripts.• Ensure secure method of local authentication (i.e., SSH).• Disable insecure login daemons ('r' commands, telnet, etc.)• Ensure correct allocation of disk space• Make sure passwords are "strong"• PAM setup

2.4.4 Application Setup

Application Setup Risks			
Vulnerability	Threat	Likelihood	Risks/Impacts
Ill-defined Access Controls on the DS	High	Medium	Medium-to-High risk. Access Controls define what actions users and administrators are allowed to perform with the data stored in the DS. Failure to lock down these controls can lead to unauthorized manipulation of data.

Weak administrator password	High	Medium	Medium-to-High risk. If the primary DS administrator's password can be cracked easily, this increases the chances of compromised data.
Weak DS owner password	High	Medium	Medium-to-High risk. For the same reasons as the above vulnerability, failure to lock down the owner of the DS directories can lead to compromised data.
Incorrect logging setup	Low-to-Medium	Low	Low-to-Medium risk. Failure to capture and/or properly store LDAP logs can make troubleshooting difficult. Improper rotation of the logs files can also fill up disk partitions.
Open permissions on the data directories	Medium	Low	Low risk. Administrators need to ensure that the permissions and ownerships of the directories where the DS data is stored are locked down so that only the owner of the DS (and possibly root) has access to those directories.
Incorrect replication setup	Medium	Medium	Medium risk. Administrators should take advantage of the enhanced replication features on Sun ONE DS v5.2 to ensure that all data is properly backed up.
Poor configuration of the company's password security policy.	Low-to-Medium	Low	Low risk. The DS needs to be configured so that passwords expire within a certain period to decrease the likelihood of cracking passwords. Other settings should be adjusted to enforce storing a password history, locking out inactive users, and encrypting passwords.
Creation of too many administrators	High	Medium	Medium-to-High risk. Administrators that are defined after the installation do not have an LDAP entry. Instead, they exist only as an entity in a local configuration file with a plaintext password that can be compromised if an attacker knows where to look.
Improper network configuration of the separate server instances	Low	Low	Low risk. Care must be taken to ensure that the proper IP address and port numbers are chosen for each instance so that there are no conflicts in the system.
Incorrectly-defined schema entries	Low	Low	Low risk. If an administrator decides that user-defined attributes need to be associated with the data entries, he/she must make sure that the new schema is set correctly so that information can be properly stored in the DS.

Lack of a data backup/archive plan	Medium	Medium	Medium risk. Although the DS offers an extremely useful replication feature, regular archives of the data stored on the server are necessary in order to quickly recover from a disaster. A lack of a consistent backup/archive plan will make it nearly impossible for the DS administrator to recover all the data that would be lost if all DS servers on a system were to fail.
------------------------------------	--------	--------	--

2.5 Current State of Practice

To begin creating an audit checklist for Sun ONE Directory Server v5.2, I first searched for documentation on the Internet describing what this application is and what it is used for. Obviously, the first place that I looked was Sun's documentation website (<http://docs.sun.com>). Doing a search for "directory server 5.2" on this site yielded over 150 results, and since all of them are directly from the vendor, I am confident that they are accurate. The following documents were particularly useful:

- <http://docs.sun.com/source/816-6733-10/index.html> [24] - A good high-level overview of the features of v5.2
- <http://docs-pdf.sun.com/816-6704-10/816-6704-10.pdf> [20] - General procedures on how to install and configure DS v5.2
- <http://docs.sun.com/source/816-6699-10/contents.html> [25] - Sun ONE's reference manual for managing and configuring the DS.

Once I had the foundation for my checklist, I began looking for other resources on what to include in my checklist and how to compile it. One of the best sources for this was the GIAC listing of reports done by people who have already earned their GSNA certification (http://www.giac.org/certified_professionals/listing/gsna.php). A quick scan of a few of the papers provided some high-level ideas on what else to include in my auditing checklist.

In addition to auditing the potential risks of the application being installed on my system, my research showed that there are three other areas that a comprehensive checklist should focus on: documentation, physical security, and the overall hardening of the system.

Finding sources to generate checklists for these areas were relatively simple. Most sources that provide a security checklist make some mention to the fact that documentation is an essential component in building and maintaining a system. Personal experience has shown that the best source for documentation for an application like this is the vendor itself. In addition, internal documentation is necessary to ensure that administrators know as much about

the system as possible. This might include:

- Physical location in the network
- Wiring diagrams
- Packages installed on the system
- Backup/recovery procedures
- Customized installation instructions for the application

A quick search on the Internet provided thousands of results when looking for physical security checklists. Computer systems are not the only resources that need to be physically secure; therefore, searching for this type of checklist produced the most results. Some of the better sources for generating a physical security checklist are:

- http://www.vascan.org/checklist/physical_security_check.html [31]
- <http://sans.org/rr/whitepapers/awareness/416.php> [6]
- http://rusecure.rutgers.edu/sec_plan/checklist.php [16]
- <http://www.tecrime.com/0secure.htm> [7]

Since this application is running on a Solaris server running SunOS 5.9, it is important to ensure the security of the box itself. This, even more so than the application, can lead to a variety of vulnerabilities and exploits. However, a full in-depth audit of the Solaris operating system is beyond the scope of this paper. For the purposes of this audit, I will conduct a basic audit of the Solaris server to ensure that no major vulnerabilities exist on the system. Some extremely good papers have been written that provided excellent guidance on what to include in a Solaris audit, and I have incorporated a few of those items in this paper. These resources include:

- <http://www.securityfocus.com/printable/infocus/1697> [5] - A good place to start to get a general overview of what an audit needs to include.
- <http://www.sun.com/blueprints/0503/817-2881.pdf> [13] - An overall review of JASS.
- <http://www.securitytribe.com/~roamer/whitepapers/checklist.doc> [21] - A simple checklist for conducting a Solaris audit.
- <http://www.sans.org/score/checklists/AuditingUnix.pdf> [3] - Another comprehensive checklist for Solaris.
- http://www.cert.org/tech_tips/usc20_full.html [30] - A good reference with links to other good references.

After conducting some further research on the Internet, I was unable to find any checklists that were used explicitly to conduct an audit of any type of Directory Server application. So, as far as I can tell, this is the first attempt that anyone has made to create a comprehensive Directory Server audit checklist. The basis for a majority of the items in the checklist comes from a combination of my

personal experience and resources on the Internet that describe some of the features and qualities of some different LDAP-based products. By getting an idea of how the majority of vendors and other administrators suggest a Directory Server should be configured, it was possible to compile a list of features that need to be checked to ensure that there is minimal data compromise. The following links were a few of the resources that assisted me in this endeavor:

- <http://www.openldap.org> [15] – A site dedicated to open source LDAP, complete with software, forums, and help pages.
- <http://www.nexor.com/media/whitepapers/directory%20solutions.pdf> [19] – A white paper on Nexor's LDAP-based product.
- <http://docs.sun.com/source/816-6733-10/index.html> [24] - A good high-level overview of the features of v5.2
- <http://docs-pdf.sun.com/816-6704-10/816-6704-10.pdf> [20] - All the background information you'll ever need for the Sun ONE Directory Server.

Possibly the most important part of this audit is the vulnerability scans. Even if we were to take the time and effort to check every for every potential exploit and vulnerability, there is still the possibility that something is going to be overlooked. Although the DS server resides behind the firewall in this network, it is important to ensure that we minimize the number of potential exploits that may exist on the back-end of the network. If the firewall is compromised, or if someone attempts to perform something malicious from the back-end of the network, this practice of defense-in-depth can help prevent possible exploits.

The two tools that will be used for this audit are Nessus and Nmap. Nessus is designed to automate the testing and discovery of known security problems, and it is widely considered to be one of the best vulnerability scanners available to the public [1]. Nmap is a utility that can rapidly scan any host on a network and determine a variety of characteristics about a server, such as what services are running on the server, what operating system the server is using, and what type of packet-filters are in place on the server [9]. There are many good papers about each of these tools, but the best place for information about each tool can be found at their base websites (www.nessus.org for Nessus [11] and www.insecure.org for Nmap [9]).



3 Create an Audit Checklist

The tables in this section of the report will attempt to provide a comprehensive checklist for a Solaris server running the Sun ONE Directory Server v5.2 application. The following items address a majority of the threats and vulnerabilities listed in Section 1 of this report. The checklist below follows the same organizational structure as the threat and vulnerability checklists in Section 1. Additionally, a couple of vulnerability scans will be conducted as part of the audit to check for any open ports or services that may have been missed during other parts of the audit. The Nessus and Nmap tools will be used to perform these scans. Here is a breakdown of the Audit Checklist:

- Documentation/Training – Items 1-2
- Physical Security – Items 3-4
- Solaris Security/System Hardening – Items 5-8, 17
- Application Setup – Items 9-16

3.1 Item #1 – Access to Updated Documentation

Purpose	To determine if administrators have access to the most up-to-date documentation. This includes vendor documentation and program-specific documentation.
Risk	Lack of proper documentation can lead to poorly configured or inconsistent DS setups. It is also important that new administrators have access to current documentation so that they don't need to rely solely on the expertise of previous administrators.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none">• Inspect the installation procedures and ensure they are accurate and readable.• Inspect the network diagrams and ensure they contain all pertinent information.• Ensure that administrators are aware of the documentation offered by the vendor.• Ensure that all of the above documentation is easily accessible by the proper administrators.
Pass / Fail	
Objective / Subjective	Subjective
Reference(s)	Personal experience Sourcefire Intrusion Detection System Deployment [22] VA Security Standard Compliance Checklist [31]

3.2 Item #2 – Process for Documentation Control

Purpose	To determine if there is a set process for documenting, maintaining, and storing the standard information installed on each DS.
Risk	As new DS's are installed on new systems, there needs to be a mechanism in place to ensure that the foundation of the Directory Server information is the same across all platforms. Although user information on a DS may change across different platforms, certain information, such as custom-defined user attributes or customized data containers, needs to be consistent and controlled.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none">• Ensure that this information is properly stored in a source-controlled area.• Ensure that there is a standard approval process in place for making changes to the DS information, both in the source-controlled area and in the live DS server.• Ensure that there is some sort of documentation that lists what information should be stored in each DS.
Pass / Fail	
Objective / Subjective	Objective and Subjective
Reference(s)	Personal experience Security Audit of a Network Associates Gauntlet 6.0 Firewall [17] High Technology Crime – Computer Forensics and Digital Evidence [7] VA Security Standard Compliance Checklist [31]

3.3 Item #3 – Physical Access to the Server

Purpose	To determine if all necessary controls are in place to ensure that only proper personnel have physical access to the DS server.
Risk	Granting physical access to the server to more people than necessary increases the chances of data corruption, data loss, and physical damage to the server itself (whether it may be accidental or not).

Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Determine if the server is located in some sort of restricted area. • Ensure that access to the restricted area is properly controlled by on-site security. • Check to ensure that there are procedures for properly escorting non-authorized personnel into the area.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience High Technology Crime – Computer Forensics and Digital Evidence [7] RU Secure: Security Checklist [16]

3.4 Item #4 – Physical Safety Controls

Purpose	To determine if the proper safety measures are in place to prevent physical damage to the DS server.
Risk	Improper safety equipment and training can lead to unnecessary and costly physical damage.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Ensure that proper fire prevention controls are in place. Also check the status of the manual fire extinguishers. • Ensure that a proper alarm system exists. • Determine whether there is proper ventilation around the server. • Ensure that proper electrical controls are in place.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Data Center Physical Security Checklist [6] RU Secure: Security Checklist [16] High Technology Crime – Computer Forensics and Digital Evidence [7]

3.5 Item #5 – Installation of a Solaris Hardening Package

Purpose	To determine whether or not the Solaris server has been properly locked down.
Risk	If unnecessary ports or services are left open on a Solaris server, there is a high risk for compromising the data being stored on the server.

**Testing Procedure /
Compliance Criteria**

- Check to see if a hardening package (e.g., JASS or YASSP) has been installed on the DS server.
- Check the /etc/inetd.conf to see what services are enabled. Since the server should be locked down as thoroughly as possible, the following services should be commented out:
 - ftp
 - tftp
 - sysstat
 - rexd
 - ypupdated
 - netstat
 - rstatd
 - rusersd
 - sprayd
 - walld
 - exec
 - talk
 - comsat
 - rquotad
 - name
 - uucp
 - telnet
 - imap
 - pop3
 - dtspc
 - fs
 - kcms
 - all rpc services
 - sadmind
 - login
 - finger
 - chargen
 - echo
 - time
 - daytime
 - discard
- Examine /etc/system and /etc/services files for what services are being started.
- Check /etc/rc* directories to ensure that appropriate services have been disabled at startup. Ensure the following startup scripts have been disabled:
 - Automounter
 - Sendmail
 - RPC
 - SNMP
 - NFS Client
 - NFS Server

Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal Experience Auditing System Security [13] Solaris Hardening Checklist [21] Auditing Unix – Solaris [3]
Comment	Performing a thorough audit of the hardening of the server is beyond the scope of this audit. However, the installation of a proper Solaris hardening package is a good first step to ensuring the overall security of the server.

3.6 Item #6 – Tripwire Installation and Configuration

Purpose	To determine whether Tripwire has been installed and properly initialized on the DS server.
Risk	Tripwire is a tool that checks to see if any important information has changed on the system. Without the proper installation and configuration of Tripwire, it becomes difficult to trace when and how important information may have been modified.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Determine whether a Tripwire package has been installed on the server. • If so, check the original Tripwire configuration file to ensure that information on the proper files is being captured. • Ensure that Tripwire has been properly initialized.
Pass / Fail	
Objective / Subjective	Objective and Subjective
Reference(s)	Solaris Hardening Checklist [21] Tripwire.org – Home of the Tripwire Open Source Project [29]

3.7 Item #7 – Syslog Setup

Purpose	To determine whether syslog messages are properly captured either locally or on a central logging server.
Risk	Failure to correctly configure log captures on the DS server can make it extremely difficult to trace defects and/or intrusions into the system.

Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Ensure that a logging package has been installed on the server. • Check the /etc/hosts file to ensure that logs are being sent to the correct log host. • Ensure that the following items are logged: <ul style="list-style-type: none"> ○ SU attempts ○ Failed login attempts ○ System events • Check the /etc/syslog.conf file to ensure that, at a minimum, anything above an “error” priority is being logged.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience Solaris Hardening Checklist [21] Auditing Unix – Solaris [3] Advanced System and Network Auditing [8]

3.8 Item #8 – Solaris Patch Updates

Purpose	To determine whether the most relevant up-to-date patches have been installed on the DS server.
Risk	Failure to properly keep up with the latest patch sets can leave obscure security holes open in the system.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Use a tool to determine if the latest patches are installed on the system. • If possible, determine whether the patches were obtained from a secure site.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Solaris Hardening Checklist [21] Auditing Unix – Solaris [3]

3.9 Item #9 – Configuration of DS Access Controls

Purpose	To determine if minimal permissions are given to users and administrators vi Access Control Instructions (ACIs)
Risk	Allowing more users than necessary to have certain permissions on the Directory Server can increase the chances of data compromise or exploitation.

Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> In the DS GUI, under the Directory tab, access the ACL list for each container. Highlight each container, and then select Object -> Set Access Permissions. Examine each ACL to ensure that only a minimal set of accesses is granted to users and administrators.
Pass / Fail	
Objective / Subjective	Subjective
Reference(s)	Personal experience Secure Directory Solutions: A Nexor White Paper [19] Sun ONE Directory Server 5.2 Product Brief [24] Server Management Guide: Sun™ ONE Server Console [20]

3.10 Item #10 – Password Strength

Purpose	To determine whether the DS Administrator is using a strong password that is in compliance with the company security policy. Also to determine whether the password is strong for the owner of the directories where the information is stored on the server.
Risk	Making either of these passwords easily guessable or crack-able significantly increases the odds of data compromise or manipulation by the wrong parties.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> Ask the administrator(s) who know these passwords to ensure that they adhere to the company's password security policy. The company's policy is defined as follows: <ul style="list-style-type: none"> Password must be at least 8 characters long Password must include at least 3 of the following types of characters: uppercase, lowercase, numbers, special characters, or symbols. Password cannot match any 8-character dictionary word. Password cannot contain any part of the username. Password must be changed every 180 days.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience Internal company documentation Focus on Windows: Password Policies [4]

3.11 Item #11 – DS Logging Setup

Purpose	To determine whether the access, errors, and audit logs have been properly configured on the server.
Risk	A lack of these logs makes it difficult to troubleshoot and track certain DS-related events, such as server requests and responses, DS errors, server startup and shutdown, and unsuccessful logins to the server.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none">• In the DS GUI, under the Configuration tab, highlight the entry for each type of log and note the logging directory.• In the terminal window, ensure that this directory exists, and ensure that the logs are being correctly written.• In the DS GUI, ensure that a rotation scheme is enabled for each type of log, and check to see whether appropriate values are set for the maximum size of each log.• Examine the properties of the directory where the logs are being written to ensure that there is enough disk space for all the log files.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience Sun ONE Directory Server 5.2 Product Brief [24] Server Management Guide: Sun™ ONE Server Console [20]

3.12 Item #12 – Replication Setup

Purpose	To determine whether replication is properly configured on the two DS servers, and to ensure that the replication features are working between the two servers.
Risk	If replication is not enabled, then the lone DS server becomes a single point of failure until the backup and recovery procedures are executed. Replication ensures that authentication can continue unabated on the secondary server until the problems with the first server can be diagnosed.

Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Inspect the configuration of the DS GUI to ensure that replication is set up correctly. Things to consider are <ul style="list-style-type: none"> ○ Consumer host name and port. ○ Configuration of “changelogs” directory. ○ Multiple-master vs. Master-consumer configuration. • If the DS’s are configured in a “multiple-master” setup, run a simple test to verify that replication is working properly in both directions: <ul style="list-style-type: none"> ○ On the primary DS, add a user or change an attribute of some entry. ○ On the secondary DS, verify that the same information exists. ○ Repeat the above two steps in the opposite direction. • Check to see how often the DS’s are configured to replicate to each other. In other words, see if they are configured to replicate to each other continuously, or if they are to share their data at pre-determined intervals. Verify that this was the agreed-upon configuration.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience Sun ONE Directory Server 5.2 Product Brief [24] Server Management Guide: Sun™ ONE Server Console [20]

3.13 Item #13 – Password Security Policy

Purpose	To determine whether the DS is configured to appropriately enforce the company’s password policies. This could include locking a user out after a certain period of inactivity, expiring a user’s password after so many days, and keeping a history of the users’ previous passwords.
----------------	--

Risk	By not enforcing a strict password security policy, the administrators increase the chances of a compromised password. Forcing users to use “strong passwords” (see the criteria under Item #10), in combination with a password lockout policy, can increase the overall security of the network by making it difficult for a malicious user to crack or obtain passwords.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • In the DS GUI, under the Configuration tab, inspect the settings for the data entry. Ensure that they match the company’s password security policy. This policy is as follows: <ul style="list-style-type: none"> ○ Allow users to change their passwords after 3 days. ○ Keep a history of the last 5 passwords for each user. ○ Force a password change every 180 days. ○ Lockout a user after 3 failed password attempts. ○ Unlock a user after 30 minutes if 3 bad passwords were entered. ○ Send a warning 15 days before a password is about to expire.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience Focus on Windows: Password Policies [4]

3.14 Item #14 – Lockdown of DS-specific Directories

Purpose	To determine whether the directories where the DS application is installed is locked down so that only the DS administrator and root can access them.
Risk	By not placing strict restrictions on who can access the DS-specific directories, the administrators significantly increase the chances of data compromise and exploitation
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Inspect the permissions and ownerships of the directories where the DS application is installed. Verify that they are owned by either the DS administrator or by root. Also ensure that the permissions on the directories are 700 or less.
Pass / Fail	

Objective / Subjective	Objective
Reference(s)	Personal experience Sun ONE Directory Server 5.2 Product Brief [24] Server Management Guide: Sun™ ONE Server Console [20]

3.15 Item #15 – Data Backup Plan

Purpose	To determine whether a regular data archive/backup plan is in place and being utilized correctly.
Risk	A lack of a data archive plan significantly increases the amount of time that will be necessary to restore lost data if all DS servers in a network fail.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> Inspect the configuration of the network to verify that some sort of data archive or tape backup system is in place and being properly utilized. Ensure that there is appropriate documentation that captures this backup process.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Personal experience Sun Product Documentation [27]
Comment	This application may not be running directly on the DS server, so it may be necessary to look elsewhere to see if this criterion is met.

3.16 Item #16 – Startup/Shutdown Scripts

Purpose	To determine whether the server has the proper startup scripts so that the DS processes automatically commence whenever the server is restarted. Also, to determine whether scripts are in place to properly stop the DS processes when the server is shutdown.
Risk	Although the risk is small, failure to properly bring down the DS processes on a server shutdown can lead to internal problems with the application. Bringing the processes up at server startup is good practice and requires little human intervention.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> Check the /etc/rc* directories to verify that a startup and shutdown script exists for the DS processes.
Pass / Fail	

Objective / Subjective	Objective
Reference(s)	Personal experience

3.17 Item #17 – Vulnerability Scans

Purpose	To determine if any previously undetected security holes still exist on the system.
Risk	Any open ports or services on a machine can lead to a potential exploit. These need to be detected and fixed as soon as possible.
Testing Procedure / Compliance Criteria	<ul style="list-style-type: none"> • Using a Nessus scan, ensure that all unnecessary services are disabled on the server. • Using an Nmap scan, ensure that no unnecessary ports are left open, and ensure that no potentially damaging information is available to the public.
Pass / Fail	
Objective / Subjective	Objective
Reference(s)	Nessus Open Source Vulnerability Scanner Project [11] Introduction to Nessus [1] Insecure.org [9] Advanced System and Network Auditing [8]

© SANS Institute 2000

4 Conduct the Audit Testing, Evidence and Findings

The checklist that was generated in Section 2 of this report will serve as the basis for the audit of the Solaris Server running Sun ONE DS v5.2. Each item in the checklist will be audited, but the issues addressed in Items 1, 2, 5, 8, 9, 10, 15, and 17 appear to have the highest importance because they address the issues that pose the more severe risks to the system.

Note: The host names, IP addresses, and installation directories in all screen captures and data captures have been modified so as not to reveal any potentially sensitive information.

4.1 Test #1 – Access to Updated Documentation

Comment: Because of the sensitivity of the data being discussed here, and because all of the information below is located on an isolated intranet, screen captures will not be available.

The DS administrators showed me where the DS v5.2 installation instructions are kept. These documents are kept in a controlled area where only a select few users have the privileges of updating the document. This document is also kept in a well-organized and easy-to-find place within the document control area.

The instructions are based on the Server Management Guide: Sun™ ONE Server Console located at <http://docs-pdf.sun.com/816-6704-10/816-6704-10.pdf> [20]. The installation has not been automated as of yet, but the instructions go into explicit detail and spell out everything that needs to be configured for a new DS installation. These instructions are laid out in an easy-to-read format, and the administrators have informed me that multiple people have used the instructions to configure a new DS.

The network diagrams for each system that contains a DS server are also contained in the document control area. Each diagram explicitly shows the DS server's location within the network, all IP addresses associated with it, and all physical connections to the server itself. These diagrams contain all the information that is needed to physically install one of these servers.

Each administrator was also able to tell me where he or she could go to get documentation directly from the vendor. A few of the sources for this report, including [23], [24], [20], and [10] come directly from the vendor's (Sun's) website. The administrators also informed me that there are a couple points of contact on the program that keep records of all contract licenses and software that we use on the system. These points of contact have a vast amount of

information on how to get in contact with Sun customer support in case the online documentation is not sufficient.

The DS administrators proved that a great deal of information on the Sun ONE DS v5.2 application is at their disposal, and they all knew where they could obtain this information.

RESULT: PASS

4.2 Test #2 – Process for Documentation Control

Comment: Because of the sensitivity of the data being discussed here, and because all of the information below is located on an isolated intranet, screen captures will not be available.

I asked the DS administrators if there was a controlled place in the system where “default” LDAP files for new installations of the DS server is contained. They informed me that the “default” LDAP files for the DS servers are controlled by Rational ClearCase, and they showed me where these files were located. There are two main files that are under documentation control:

- First, there is a default data file known as the “Gold Copy” that contains pretty much all information that a new DS installation would need. The only thing that was excluded from this “Gold Copy” was any user information, which is ok since specific user information is going to be different across different platforms.
- Secondly, there is a custom-defined schema file called 99user.ldif. This file contains customized attributes that are not provided by the DS itself. More information about how the 99user.ldif file can be used is located at this link: <http://docs.sun.com/source/816-5599-10/schema.htm> [10].

I then asked if there was any written documentation that corresponded with this default information. They showed me the controlled place where the internal DS-specific documentation is stored. The first thing I noticed was that there was no documentation that corresponded with the information stored in the 99user.ldif file. Further inquiries revealed that changes to this file are done on an ad hoc basis, and any documentation that discusses updates to this file is scattered across the system.

I then inspected the documentation that corresponds with the “Gold Copy” data files. A close inspection revealed that the data file and the documentation were close, but there were still a few inconsistencies between the two.

There is a process that can be used to update both the documentation and the “Gold Copy” files, but there are areas for disconnection. Anytime a modification

is requested, discussions are conducted via e-mail and ad hoc meetings to discuss whether or not the change is necessary and practical. Once an agreement is reached, the modification is then presented to an internal review board for approval. After they grant approval for this change, a task is assigned to the people that control the documentation so that the modification can be made there first. Once this is in place, another task can be assigned to the DS administrator for implementation into the “Gold Copy”.

The process itself is not a bad one; however, I noticed that there is no formal control over how the modification tasks are passed out to the administrators. The approval board does not assign these tasks. Instead, it is up to the administrators to ensure that any approved changes are implemented in the “Gold Copy” and on all DS servers in the system. This could explain the inconsistencies between the controlled data files and the documentation.

There are many aspects of this document-control process that are commendable; however, there are quite a few issues that need to be addressed in the near future. Failure to do so will result in wasted time and effort trying to get all information consistent and put in to the system’s baseline.

RESULT: FAIL

4.3 Test #3 – Physical Access to the Server

The server itself is located inside a secure room at a rather secure facility. A person needs either a permanent badge or some type of pre-approved visitor badge before they can even get past the perimeter of the facility. The permanent badges have a picture of the person to whom it belongs, and each person is assigned a numerical code that must be used in conjunction with the badge to gain access to the facility. Unless visitors have been given the proper approvals, they are not allowed to travel around the facility without an escort.

Once inside the secure area, a person must have an additional set of accesses and permissions before being allowed into the room where the server is housed. A badge reader also controls access to this room, and the room is clearly marked as a restricted area. Visitors and personnel who have not obtained the additional accesses are not allowed into the room without an escort. The only other entrance into the room is through a set of double doors – used mainly for the bigger pieces of equipment – which is strictly controlled by on-site security.

The proper controls have been put into place to ensure that the DS server (and all of the other servers in the network) is physically secure. Everyone involved in the audit was also cognizant of this security procedure.

RESULT: PASS

4.4 Test #4 – Physical Safety Controls

The room in which the DS server resides has been equipped to handle a majority of environmental dangers. First off, a sprinkler system has been installed to prevent any major fire outbreaks. The installation of a non-water based fire extinguishing system may be worth investigating because of the damage that water could do to all the expensive equipment in the server room. However, the room is so big that this effort may not be cost effective.

There are fire extinguishers at regular intervals throughout the room, and each of them are clearly marked and charged properly. An alarm system is in place in the server room as well, and on-site security has informed me that they test the alarm system in the building at least twice every year. Gigantic air handlers are in place in the server room to continuously cycle air and cool the room. Perforated tiles are in place at regular intervals on the server room floor to ensure an even distribution of the circulated air. The server rack in which the DS server is installed has been properly equipped to handle any unforeseen surges of electricity.

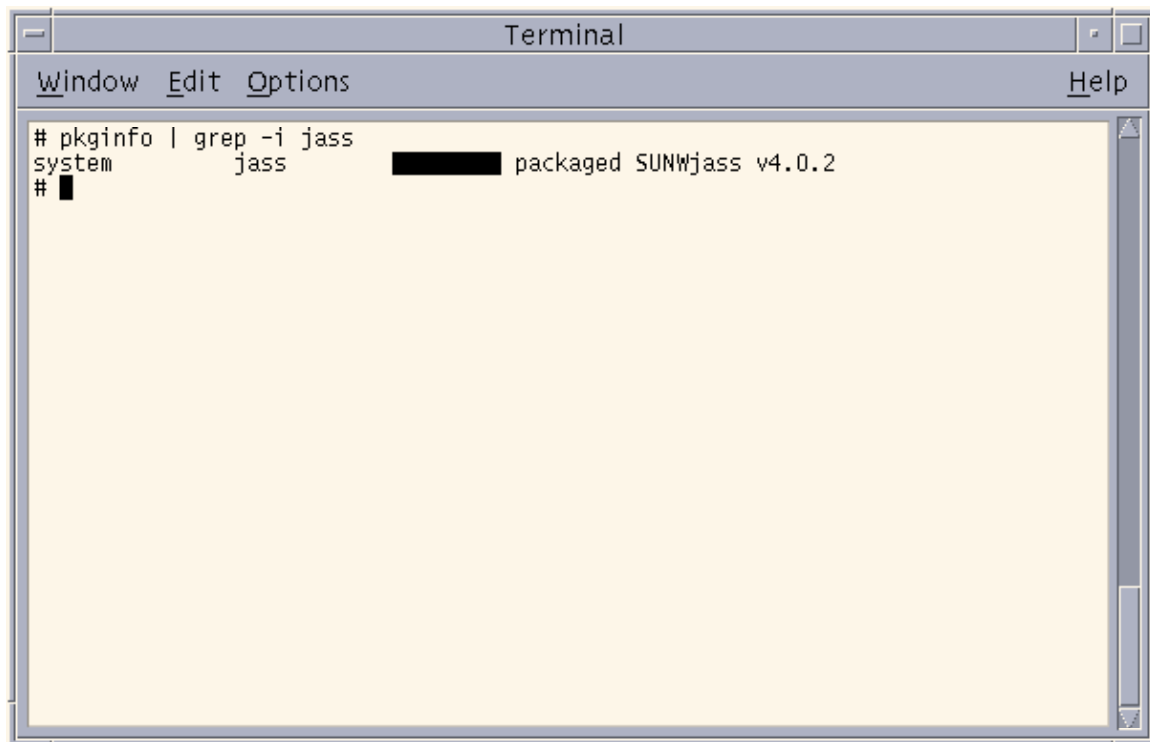
All exits in the room are clearly marked with lit signs on the ceiling. At each exit, there is a map of the building that shows how to completely get out of the building in case of an emergency. Telephones are available in various places throughout the room, and all emergency numbers, including on-site security, are clearly written on each phone.

All in all, the room in which the server is stored is prepared for most major types of environmental dangers.

RESULT: PASS

4.5 Test #5 – Installation of a Solaris Hardening Package

The first thing I checked was to ensure that a Solaris hardening package had been installed on the DS server. Figure 2 shows that a customized version of the Sun JASS package v4.0.2 [13] has been installed. Again, to protect sensitive information, part of the description of the package has been omitted.



```
Terminal
Window Edit Options Help
# pkginfo | grep -i jass
system      jass      [REDACTED] packaged SUNWjass v4.0.2
#
```

Figure 2 – JASS installation

The file “gsna-be-ldap2.SOL.20050312”, which is the output of all the .fin scripts that were run during the JASS installation, is shown in Appendix A. These .fin scripts are responsible for locking down the server by performing a variety of tasks.

- In most cases, the .fin scripts will rename some of the files in the /etc/rc*d directories so that they are not called during startup or shutdown. For example, here is the output from the “disable-devfsadm.fin” script

```
=====
=====
SOLsecure.driver: Finish script: disable-devfsadm.fin
=====
=====

Disabling the devfsadm service.
[NOTE] Renaming /etc/rc0.d/K83devfsadm to
/etc/rc0.d/_K83devfsadm.JASS.20050312022438
[NOTE] Renaming /etc/rcS.d/S50devfsadm to
/etc/rcS.d/_S50devfsadm.JASS.20050312022438
```

- In some cases, a configuration file is either modified to contain new information, or it will be simply renamed so that its service will not recognize it. For example, here is the output from the “disable-vold.fin” script:

```

=====
=====
SOLsecure.driver: Finish script: disable-vold.fin
=====
=====

Disabling the service: Volume Management (VOLD)

[NOTE] Renaming /etc/vold.conf to
/etc/_vold.conf.JASS.20050312022500

```

- Finally, a script called “update-inetd-conf.fin” is run so that it can comment out all unnecessary services in the /etc/inetd.conf file. Here is part of the output of this script:

```

=====
=====
SOLsecure.driver: Finish script: update-inetd-conf.fin
=====
=====

Updating status of network services in
/etc/inet/inetd.conf.

Disabling those services listed in JASS_SVCS_DISABLE.

[NOTE] Copying /etc/inet/inetd.conf to
/etc/inet/inetd.conf.JASS.20050312022509

Disabling service, chargen (internal).
Disabling service, comsat (/usr/sbin/in.comsat).
Disabling service, daytime (internal).
Disabling service, discard (internal).
Disabling service, dtspc (/usr/dt/bin/dtspcd).
Disabling service, echo (internal).
Disabling service, exec (/usr/sbin/in.rexecd).
Disabling service, finger (/usr/sbin/in.fingerd).

```

Whenever JASS renames or copies off a file, it will put a “.JASS.<timestamp>” extension on the file name. This is to ensure that the original file on the server will be replaced if JASS is ever uninstalled or backed out.

The next part of this test was to check the /etc/inetd.conf file to ensure that all unnecessary services are commented out by the JASS installation. The /etc/inetd.conf file from the DS server is shown in Appendix A. There are a couple of things to note about this file. First off, everything listed in the checklist in Item 2.5 is either commented out of the file or it is not even present in the file. Certain services, such as “ypupdated”, “uucp”, “imap”, and “pop3” are not found in the file. The “ftp” service is also missing from the inetd.conf file. This is because, as part of the JASS installation, the SUNWftpr and SUNWftpu packages are removed from the server. Lastly, there are four custom-defined

services located at the end of the `/etc/inetd.conf` file. These are for the purposes of NetBackup.

```
bpcd    stream    tcp    nowait    root
        /usr/opensv/netbackup/bin/bpcd    bpcd
vnetd   stream    tcp    nowait    root
        /usr/opensv/bin/vnetd    vnetd
voiped  stream    tcp    nowait    root
        /usr/opensv/bin/voiped    voiped
bpjava-msvc stream    tcp    nowait    root
        /usr/opensv/netbackup/bin/bpjava-msvc    bpjava-msvc
```

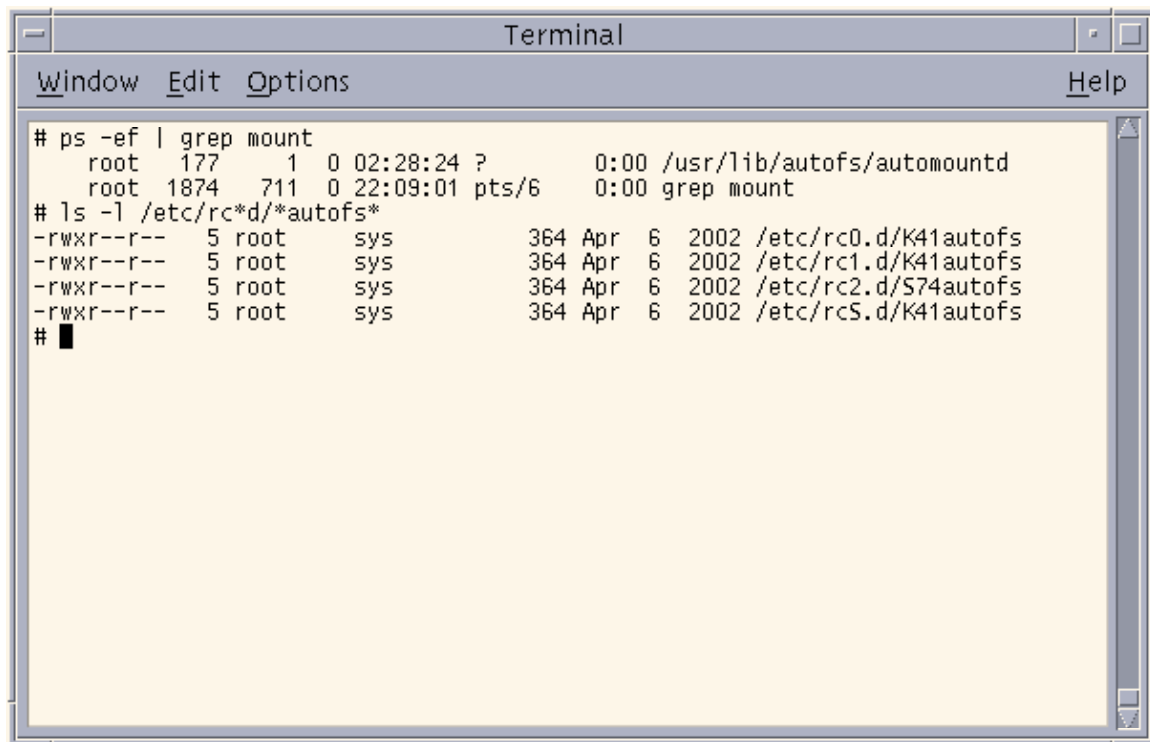
The `/etc/system` and `/etc/services` files are also located in Appendix A. The `/etc/system` file is the base file that comes with a normal Solaris installation. No extra information has been put into this file, and no extraneous services are being started from here. The `/etc/services` file is also the base file that comes with Solaris, with one slight modification. The NetBackup ports have been appended to the end of this file. For the purposes of this server, this is ok.

```
#
# NetBackup services
#
bprd    13720/tcp    bprd
bpjava-msvc 13722/tcp    bpjava-msvc
bpcd    13782/tcp    bpcd
vnetd   13724/tcp    vnetd
voiped  13783/tcp    voiped
```

I then performed a check of some of the files that should have been disabled in the `/etc/rc*d` directories. In the checklist above, it says that the following items need to be checked:

- Automounter
- Sendmail
- RPC
- SNMP
- NFS Client
- NFS Server

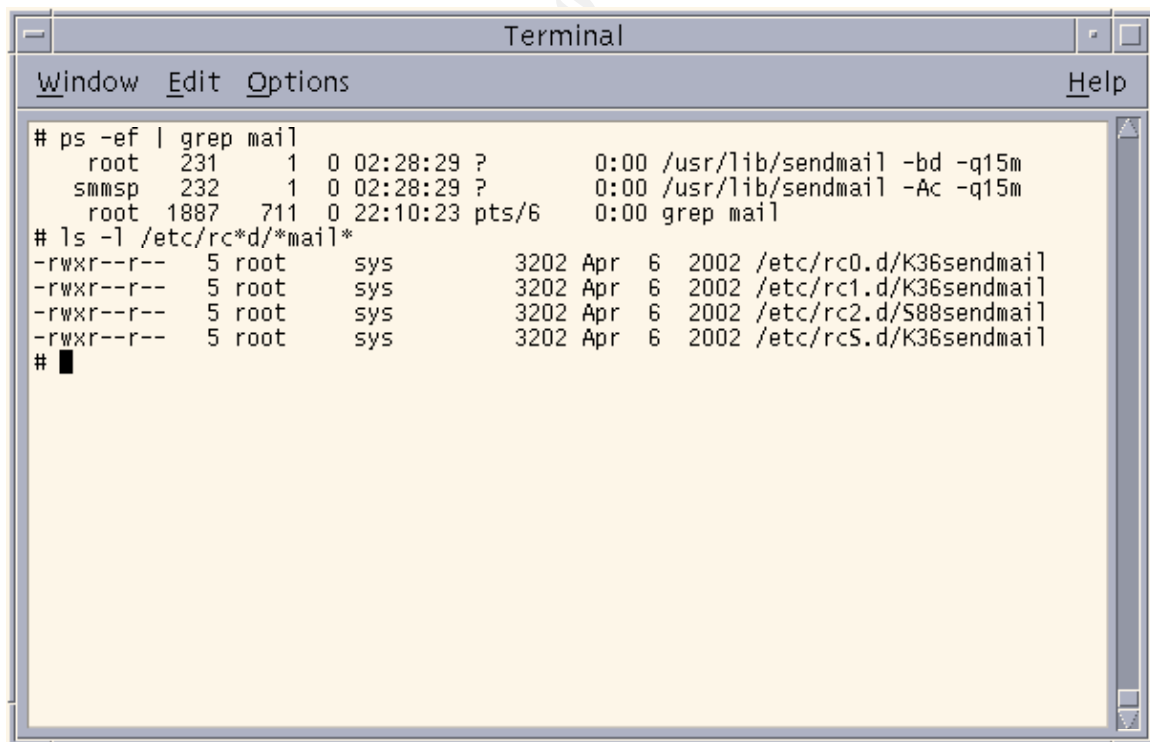
The following figures show screen capture of the items listed above and their corresponding entries in the `/etc/rc*d` directories:



A terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the output of two commands. The first command, `# ps -ef | grep mount`, shows two processes: `root 177 1 0 02:28:24 ? 0:00 /usr/lib/autofs/automountd` and `root 1874 711 0 22:09:01 pts/6 0:00 grep mount`. The second command, `# ls -l /etc/rc*d/*autofs*`, lists four files in the `/etc/rc.d` directory, all owned by `root` and `sys` with permissions `-rwxr--r--` and size `5`. The files are `K41autofs`, `K41autofs`, `S74autofs`, and `K41autofs`, all dated `Apr 6 2002`. The prompt `#` is followed by a cursor.

```
# ps -ef | grep mount
root 177 1 0 02:28:24 ? 0:00 /usr/lib/autofs/automountd
root 1874 711 0 22:09:01 pts/6 0:00 grep mount
# ls -l /etc/rc*d/*autofs*
-rwxr--r-- 5 root sys 364 Apr 6 2002 /etc/rc0.d/K41autofs
-rwxr--r-- 5 root sys 364 Apr 6 2002 /etc/rc1.d/K41autofs
-rwxr--r-- 5 root sys 364 Apr 6 2002 /etc/rc2.d/S74autofs
-rwxr--r-- 5 root sys 364 Apr 6 2002 /etc/rcS.d/K41autofs
#
```

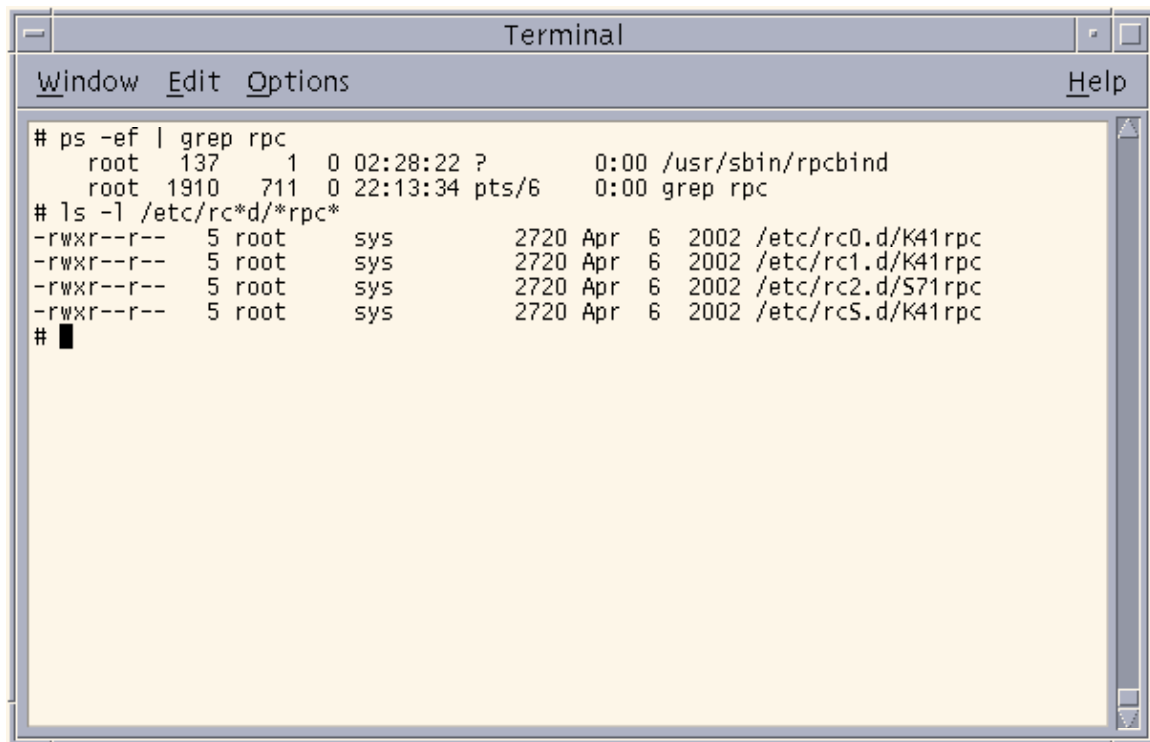
Figure 3 – Automounter



A terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the output of two commands. The first command, `# ps -ef | grep mail`, shows three processes: `root 231 1 0 02:28:29 ? 0:00 /usr/lib/sendmail -bd -q15m`, `smmsp 232 1 0 02:28:29 ? 0:00 /usr/lib/sendmail -Ac -q15m`, and `root 1887 711 0 22:10:23 pts/6 0:00 grep mail`. The second command, `# ls -l /etc/rc*d/*mail*`, lists four files in the `/etc/rc.d` directory, all owned by `root` and `sys` with permissions `-rwxr--r--` and size `5`. The files are `K36sendmail`, `K36sendmail`, `S88sendmail`, and `K36sendmail`, all dated `Apr 6 2002`. The prompt `#` is followed by a cursor.

```
# ps -ef | grep mail
root 231 1 0 02:28:29 ? 0:00 /usr/lib/sendmail -bd -q15m
smmsp 232 1 0 02:28:29 ? 0:00 /usr/lib/sendmail -Ac -q15m
root 1887 711 0 22:10:23 pts/6 0:00 grep mail
# ls -l /etc/rc*d/*mail*
-rwxr--r-- 5 root sys 3202 Apr 6 2002 /etc/rc0.d/K36sendmail
-rwxr--r-- 5 root sys 3202 Apr 6 2002 /etc/rc1.d/K36sendmail
-rwxr--r-- 5 root sys 3202 Apr 6 2002 /etc/rc2.d/S88sendmail
-rwxr--r-- 5 root sys 3202 Apr 6 2002 /etc/rcS.d/K36sendmail
#
```

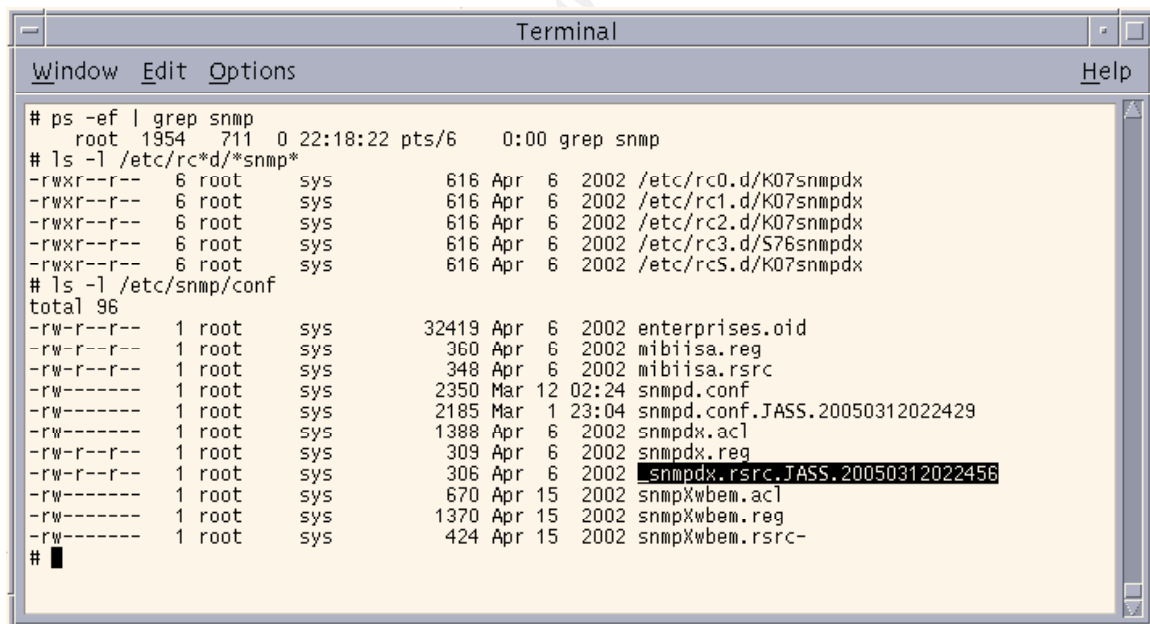
Figure 4 – Sendmail



A terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the output of two commands. The first command, `# ps -ef | grep rpc`, shows two processes: `root 137 1 0 02:28:22 ? 0:00 /usr/sbin/rpcbind` and `root 1910 711 0 22:13:34 pts/6 0:00 grep rpc`. The second command, `# ls -l /etc/rc*d/*rpc*`, lists four files in the `/etc/rc.d` directory, all owned by `root` and `sys` with permissions `-rwxr--r--` and size `5`. The files are `K41rpc`, `K41rpc`, `S71rpc`, and `K41rpc`, all dated `2720 Apr 6 2002`. The prompt `#` is followed by a cursor.

```
# ps -ef | grep rpc
root 137 1 0 02:28:22 ? 0:00 /usr/sbin/rpcbind
root 1910 711 0 22:13:34 pts/6 0:00 grep rpc
# ls -l /etc/rc*d/*rpc*
-rwxr--r-- 5 root sys 2720 Apr 6 2002 /etc/rc0.d/K41rpc
-rwxr--r-- 5 root sys 2720 Apr 6 2002 /etc/rc1.d/K41rpc
-rwxr--r-- 5 root sys 2720 Apr 6 2002 /etc/rc2.d/S71rpc
-rwxr--r-- 5 root sys 2720 Apr 6 2002 /etc/rcS.d/K41rpc
#
```

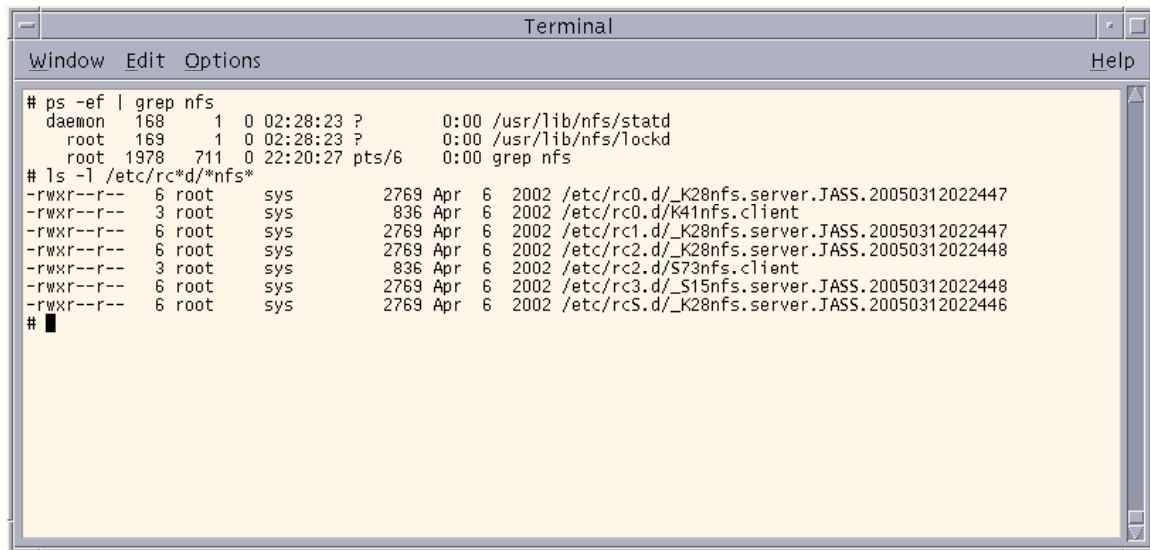
Figure 5 – RPC



A terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the output of two commands. The first command, `# ps -ef | grep snmp`, shows one process: `root 1954 711 0 22:18:22 pts/6 0:00 grep snmp`. The second command, `# ls -l /etc/rc*d/*snmp*`, lists five files in the `/etc/rc.d` directory, all owned by `root` and `sys` with permissions `-rwxr--r--` and size `6`. The files are `K07snmpdx`, `K07snmpdx`, `K07snmpdx`, `S76snmpdx`, and `K07snmpdx`, all dated `616 Apr 6 2002`. The third command, `# ls -l /etc/snmp/conf`, lists 16 files in the `/etc/snmp/conf` directory, all owned by `root` and `sys` with permissions `-rw-r--r--` or `-rw-----`. The files include `enterprises.oid`, `mib1isa.reg`, `mib1isa.rsrc`, `snmpd.conf`, `snmpd.conf.JASS.20050312022429`, `snmpdx.ac1`, `snmpdx.reg`, `snmpdx.rsrc.JASS.20050312022456`, `snmpXwbem.ac1`, `snmpXwbem.reg`, and `snmpXwbem.rsrc-`. The prompt `#` is followed by a cursor.

```
# ps -ef | grep snmp
root 1954 711 0 22:18:22 pts/6 0:00 grep snmp
# ls -l /etc/rc*d/*snmp*
-rwxr--r-- 6 root sys 616 Apr 6 2002 /etc/rc0.d/K07snmpdx
-rwxr--r-- 6 root sys 616 Apr 6 2002 /etc/rc1.d/K07snmpdx
-rwxr--r-- 6 root sys 616 Apr 6 2002 /etc/rc2.d/K07snmpdx
-rwxr--r-- 6 root sys 616 Apr 6 2002 /etc/rc3.d/S76snmpdx
-rwxr--r-- 6 root sys 616 Apr 6 2002 /etc/rcS.d/K07snmpdx
# ls -l /etc/snmp/conf
total 96
-rw-r--r-- 1 root sys 32419 Apr 6 2002 enterprises.oid
-rw-r--r-- 1 root sys 360 Apr 6 2002 mib1isa.reg
-rw-r--r-- 1 root sys 348 Apr 6 2002 mib1isa.rsrc
-rw----- 1 root sys 2350 Mar 12 02:24 snmpd.conf
-rw----- 1 root sys 2185 Mar 1 23:04 snmpd.conf.JASS.20050312022429
-rw----- 1 root sys 1388 Apr 6 2002 snmpdx.ac1
-rw-r--r-- 1 root sys 309 Apr 6 2002 snmpdx.reg
-rw-r--r-- 1 root sys 306 Apr 6 2002 snmpdx.rsrc.JASS.20050312022456
-rw----- 1 root sys 670 Apr 15 2002 snmpXwbem.ac1
-rw----- 1 root sys 1370 Apr 15 2002 snmpXwbem.reg
-rw----- 1 root sys 424 Apr 15 2002 snmpXwbem.rsrc-
#
```

Figure 6 – SNMP

A terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the output of two commands. The first command is "# ps -ef | grep nfs", which shows three lines of process information: "daemon 168 1 0 02:28:23 ? 0:00 /usr/lib/nfs/statd", "root 169 1 0 02:28:23 ? 0:00 /usr/lib/nfs/lockd", and "root 1978 711 0 22:20:27 pts/6 0:00 grep nfs". The second command is "# ls -l /etc/rc*d/*nfs*", which lists several files with permissions, owner, group, size, date, and filename. The files are: "-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc0.d/_K28nfs.server.JASS.20050312022447", "-rwxr--r-- 3 root sys 836 Apr 6 2002 /etc/rc0.d/K41nfs.client", "-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc1.d/_K28nfs.server.JASS.20050312022447", "-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc2.d/_K28nfs.server.JASS.20050312022448", "-rwxr--r-- 3 root sys 836 Apr 6 2002 /etc/rc2.d/S73nfs.client", "-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc3.d/_S15nfs.server.JASS.20050312022448", and "-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc5.d/_K28nfs.server.JASS.20050312022446". The prompt "# " is visible at the bottom of the terminal.

```
# ps -ef | grep nfs
daemon 168 1 0 02:28:23 ? 0:00 /usr/lib/nfs/statd
root 169 1 0 02:28:23 ? 0:00 /usr/lib/nfs/lockd
root 1978 711 0 22:20:27 pts/6 0:00 grep nfs
# ls -l /etc/rc*d/*nfs*
-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc0.d/_K28nfs.server.JASS.20050312022447
-rwxr--r-- 3 root sys 836 Apr 6 2002 /etc/rc0.d/K41nfs.client
-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc1.d/_K28nfs.server.JASS.20050312022447
-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc2.d/_K28nfs.server.JASS.20050312022448
-rwxr--r-- 3 root sys 836 Apr 6 2002 /etc/rc2.d/S73nfs.client
-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc3.d/_S15nfs.server.JASS.20050312022448
-rwxr--r-- 6 root sys 2769 Apr 6 2002 /etc/rc5.d/_K28nfs.server.JASS.20050312022446
#
```

Figure 7 – NFS Client and Server

Figures 3, 4, and 5 show that the automounter, sendmail, and RPC processes are running on the server, and JASS did not properly shut them down. An analysis of the JASS output file located in Appendix A shows that JASS did not attempt to disable the automounter or RPC services. The script “disable-sendmail.fin” was run, but it did not attempt to rename any of the /etc/rc*d directories. Instead, it attempted to copy in a new version of the /etc/mail/sendmail.cf file, but this did not appear to be successful.

Figure 6 shows that SNMP is disabled because the /etc/snmp/conf/snmpdx.rsrc file has been moved, and without this file, SNMP will not properly start. Figure 7 shows that the NFS client services are still running while the NFS server services are not. According to the configuration of this network, this is ok because there is a centralized NFS server on the backend of this system.

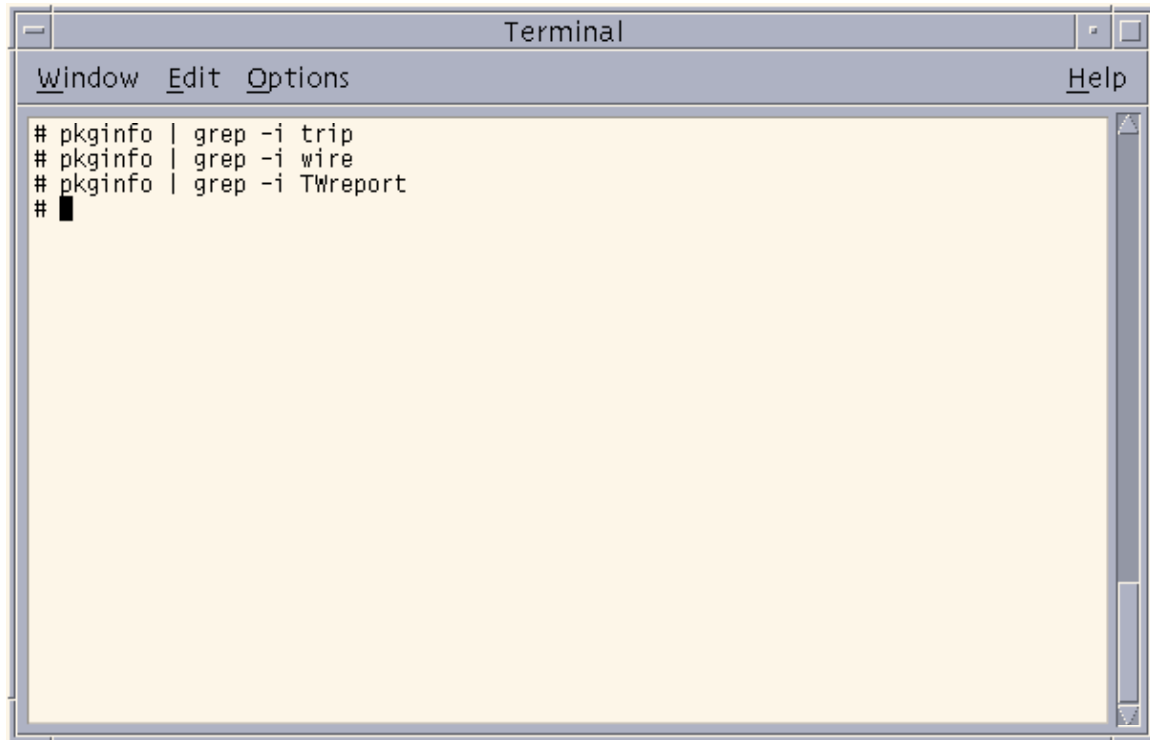
Overall, the system appears to be thoroughly hardened with an appropriate Solaris hardening package. There is still a bit of an issue with a couple of the services that are still running (namely, automounter and sendmail), but with a minimal amount of effort, these minor problems can be rectified. A note of this will be made in the “Findings and Recommendations” portion of Section 4, but these problems are not serious enough to call this test a failure.

RESULT: PASS (with comments)

4.6 Test #6 – Tripwire Installation and Configuration

In this test, we want to show that a Tripwire package has been installed and properly configured on the DS server. When the “pkginfo” command was run on the DS server, the results showed that no Tripwire package had been installed

(see Figure 8).



```
Terminal
Window Edit Options Help
# pkginfo | grep -i trip
# pkginfo | grep -i wire
# pkginfo | grep -i TWreport
#
```

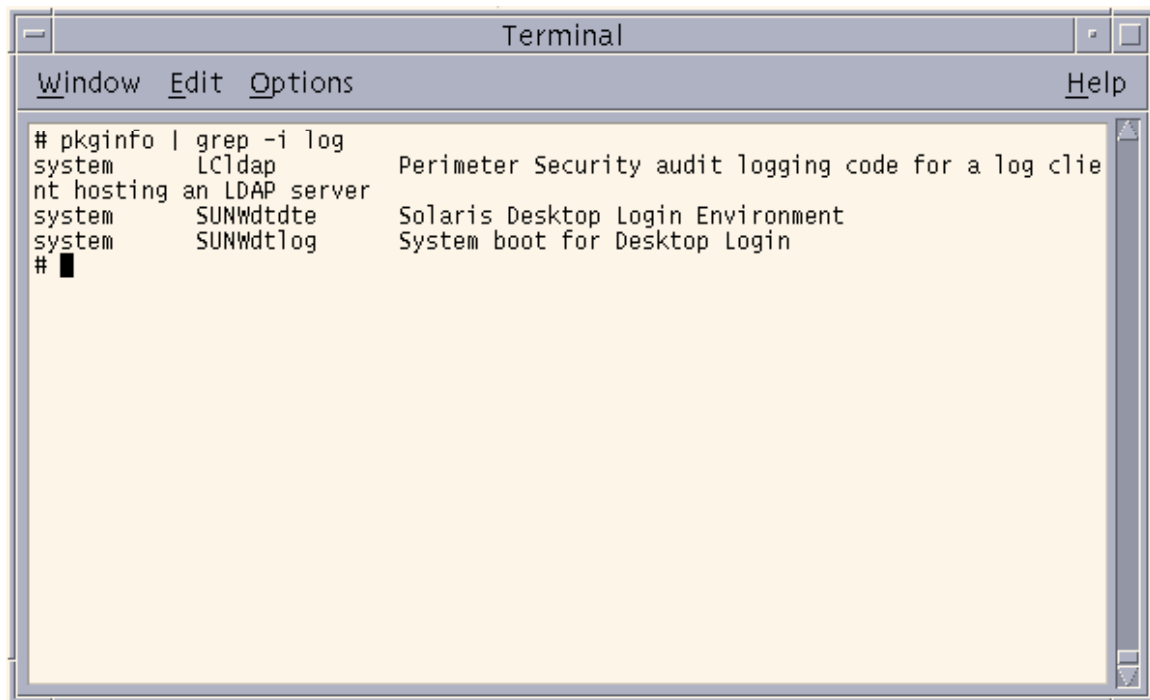
Figure 8 – Tripwire

Because of the fact that no Tripwire package has been installed, there is no need to see if it has been properly initialized and configured. The lack of a file tracking piece of software like Tripwire will make it extremely difficult to track down who when files important files have been modified.

RESULT: FAIL

4.7 Test #7 – Syslog Setup

The “pkginfo” command was run to determine if any kind of logging package had been installed on this DS server (see Figure 9).

A terminal window titled "Terminal" with a menu bar containing "Window", "Edit", "Options", and "Help". The terminal displays the output of the command "# pkginfo | grep -i log". The output shows three lines of package information: "system LCldap Perimeter Security audit logging code for a log client hosting an LDAP server", "system SUNWdtde Solaris Desktop Login Environment", and "system SUNWdtlog System boot for Desktop Login". The prompt "# " is followed by a cursor.

```
# pkginfo | grep -i log
system LCldap Perimeter Security audit logging code for a log client
nt hosting an LDAP server
system SUNWdtde Solaris Desktop Login Environment
system SUNWdtlog System boot for Desktop Login
#
```

Figure 9 – Logging package

A customized LDAP-specific logging package (LCldap) has been installed on this server. The administrator informed me that, in addition to writing all local logs to its own /var/adm/messages file, there are a couple of extra daemons running on the server to parse out specific messages and send them to the central log server.

First, there is an OS-specific daemon (named SEC_PS_bsm_os_daemon) that captures all system events that occur on the DS server. These log messages are then sent to the central log server, which, according to the /etc/hosts file, is defined as:

```
10.10.10.170 gsna-be-logs1 loghost
```

A special directory structure has been configured in the /var partition on the central log server to store the logs for the OS-specific system events that occur on the DS server. These syslog messages are sent to a file called OS_logs. The following text is an example of some of the messages that appear in this file.

```
Mar 15 17:22:37 gsna-be-ldap2 SEC_PS_bsm_os_daemon.pl[8386]:
header,140,2,execve(2),,Tue Mar 15 23:23:01 GMT 2005, + 71
msec,path,/usr/bin/su,attribute,104555,root,sys,136,280861,0,ex
ec_args,3,su,-
,dsuser,subject,root,root,other,root,other,10280,656,0 0 gsna-
be-ldap2,return,success,0

Mar 15 17:22:52 gsna-be-ldap2 SEC_PS_bsm_os_daemon.pl[8386]:
```

```
header,135,2,execve(2),,Tue Mar 15 23:23:15 GMT 2005, + 489
msec,path,/usr/bin/ls,attribute,100555,root,bin,136,280812,0,ex
ec_args,2,ls,-al,subject,root,root,other,root,other,10336,656,0
0 gsna-be-ldap2,return,success,0
```

```
Mar 15 17:22:58 gsna-be-ldap2 SEC_PS_bsm_os_daemon.pl[8386]:
header,150,2,execve(2),,Tue Mar 15 23:23:21 GMT 2005, + 324
msec,path,/usr/bin/chmod,attribute,100555,root,bin,136,280727,0
,exec_args,3,chmod,644,messages,subject,root,root,other,root,ot
her,10361,656,0 0 gsna-be-ldap2,return,success,0
```

The three syslog messages shown above originated on the DS server (gsna-be-ldap2) and were written to the central log server. Each line contains a timestamp of when the system event occurred, the server on which the event occurred, the daemon that captured this log (SEC_PS_bsm_os_daemon.pl), and the event itself (in bold).

The second daemon that is running on the DS server captures the information that is written to the access, error, and audit logs for the DS application (Section 3.11 provides more details about these DS-specific log files). This daemon, called SEC_PS_ldap_daemon, reads a configuration file that is stored in the /products directory. This configuration file contains the path(s) where the DS-specific logs are located on the DS server. The daemon then parses the access, errors, and audit files in this directory, and it sends them to the central log server. The logs are stored here for a period of time before they are rotated and saved off to tape. The following text shows the files where the DS information is written on the log server:

```
# ls -al *LDAP*
-rw----- 1 root      other          363296 Mar 12 03:10
LDAP_AUD_logs
-rw----- 1 root      other          542212 Mar 12 03:10
LDAP_ERR_logs
-rw----- 1 root      other        12318938 Mar 12 03:10 LDAP_logs
# pwd
/var/adm/audit_logs/logs
```

The following lines are examples of the output captured by the SEC_PS_ldap_daemon. These logs are exactly what you will find in the access, errors, and audit logs on the DS server itself:

```
Mar 15 17:19:33 gsna-be-ldap2 SEC_PS_ldap_daemon.pl[7972]:
LDAP_ACC: /sun1ds-v5.2/ds_install_gsna: [15/Mar/2005:23:14:48
+0000] conn=809 op=4 msgId=5 - UNBIND\n
[15/Mar/2005:23:14:48 +0000] conn=809 op=4 msgId=-1 - closing -
U1\n [15/Mar/2005:23:14:48 +0000] conn=810 op=-1 msgId=-1 -
fd=28 slot=28 LDAP connection from 10.10.10.140 to
10.10.10.150\n [15/Mar/2005:23:14:48 +0000] conn=809 op=-1
msgId=-1 - closed.
```

```
Mar 15 17:19:33 gsna-be-ldap2 SEC_PS_ldap_daemon.pl[7972]:
LDAP_ACC: /sun1ds-v5.2/ds_install_gsna: [15/Mar/2005:23:14:48
```

```
+0000] conn=810 op=0 msgId=1 - BIND dn="cn=replication manager,
cn=replication, cn=config" method=128 version=3\n
[15/Mar/2005:23:14:48 +0000] conn=810 op=0 msgId=1 - RESULT
err=0 tag=97 nentries=0 etime=0 dn="cn=replication
manager,cn=replication,cn=config"
```

```
Mar 15 17:19:33 gsna-be-ldap2 SEC_PS_ldap_daemon.pl[7972]:
LDAP_ACC: /sunlds-v5.2/ds_install_gsna: [15/Mar/2005:23:14:48
+0000] conn=810 op=1 msgId=2 - SRCH base="" scope=0
filter="(objectClass=*)" attrs="supportedControl
supportedExtension"\n [15/Mar/2005:23:14:48 +0000] conn=810
op=1 msgId=2 - RESULT err=0 tag=101 nentries=1 etime=0
```

We then checked the `/etc/syslog.conf` file to ensure that messages with a minimum priority of “error” are being properly logged.

```
#ident      "@(#)syslog.conf 1.5   98/12/14 SMI"      /* SunOS 5.0 */
#
# Copyright (c) 1991-1998 by Sun Microsystems, Inc.
# All rights reserved.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words. Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice          /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages

*.alert;kern.err;daemon.err            operator
*.alert                                root

*.emerg                                *

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
#auth.notice                          ifdef(`LOGHOST', /var/log/authlog,
@loghost)

mail.debug                             ifdef(`LOGHOST', /var/log/syslog, @loghost)

#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err                               /dev/sysmsg
user.err                               /var/adm/messages
user.alert                             `root, operator'
user.emerg                             *
)
```

As you can see, everything with an “error” priority is written to both `/dev/sysmsg`

and /var/adm/messages. Syslog messages with other priorities, such as “kern.debug” and “daemon.notice”, are also written to /var/adm/messages. The administrators have ensured that a good number of syslog messages are written locally, which makes debugging and troubleshooting server problems much easier.

Lastly, we observed how the DS server logs user login attempts. For the first test, a user named “testusr1” attempted to SSH into the DS server. The following log was written to /var/adm/messages:

```
Mar 13 01:22:37 gsna-be-ldap2 sshd[28948]: [ID 800047 auth.info]
Accepted password for testusr1 from 10.10.10.130 port 53270 ssh2
```

Next, “testusr1” attempted to login with the wrong password. After two attempts, he hit Ctrl-C to close the connection.

```
Mar 13 01:23:08 gsna-be-ldap2 sshd[28955]: [ID 800047 auth.info]
Failed password for testusr1 from 10.10.10.130 port 53274 ssh2
Mar 13 01:23:10 gsna-be-ldap2 last message repeated 1 time
Mar 13 01:23:13 gsna-be-ldap2 sshd[28955]: [ID 800047 auth.info]
Connection closed by 10.10.10.130
```

“Testusr1” then successfully logged in again. This time, he attempted to use the “su” command to become root. The first attempt was a success, and the following log was generated:

```
Mar 13 01:23:31 gsna-be-ldap2 su: [ID 366847 auth.notice] 'su
root' succeeded for testusr1 on /dev/pts/7
```

The second time “testusr1” tried to become root, he typed in the wrong password.

```
Mar 13 01:23:37 gsna-be-ldap2 su: [ID 810491 auth.crit] 'su
root' failed for testusr1 on /dev/pts/7
```

In addition to the logs in /var/adm/messages, the DS server creates an additional log in the /var/adm/sulog file every time someone attempts to use the “su” command. The following logs were created on the DS server. The first line shows that “testusr1” tried to “su” to root, and the “+” sign indicates that it was a success. The second line is similar to the first, except the “-” indicates that it was a failed attempt.

```
SU 03/13 01:23 + pts/7 testusr1-root
SU 03/13 01:23 - pts/7 testusr1-root
```

This server has been configured to capture all pertinent syslog information and then some. This setup is more than adequate for the purposes of this server.

RESULT: PASS

4.8 Test #8 – Solaris Patch Updates

In order to check the status of the patches on the DS server, I downloaded the Sun Patch Check v1.2 application from the SunSolve website [28]. This utility compares the patch set on a server against the most up-to-date “Recommended and Security patch list” provided by Sun. This application produces an HTML output file that is easy to read, and it informs the administrator whether any critical patches need to be installed.

The results of the Patch Check v1.2 application against the DS server are shown in Appendix B. The output shows that almost all patches are current, and no critical updates need to be installed. The administrator informed me that the patch set was updated three weeks before this audit.

Because the server is on an internal network with no direct access to Sun’s website, it is impossible for the DS server to automatically download patch updates as they are made available. The administrator informed me that this is a manual process with no set schedule for patch updates. In this respect, there is a lack of documented process, and this issue needs to be addressed.

RESULT: PASS (with comments)

4.9 Test #9 – Configuration of DS Access Controls

The best way to control who has access to the information in the DS database is through customized Access Control Instructions (ACIs). When an administrator creates an ACI, he can specify which users can manage a resource as well as when and how access is granted [20]. Figure 10 demonstrates how to access the ACI list for a specific container.

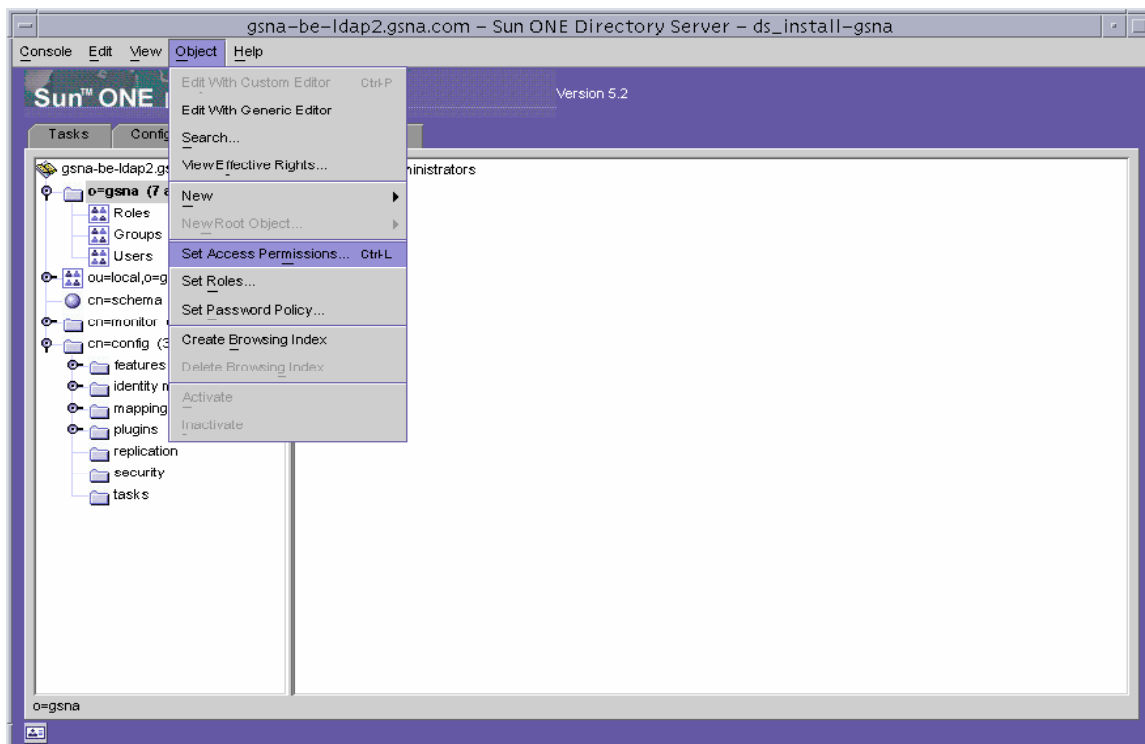


Figure 10 – Accessing an ACI

On this particular DS instance, seven ACIs have been defined for the o=gsna database, as shown in Figure 11.

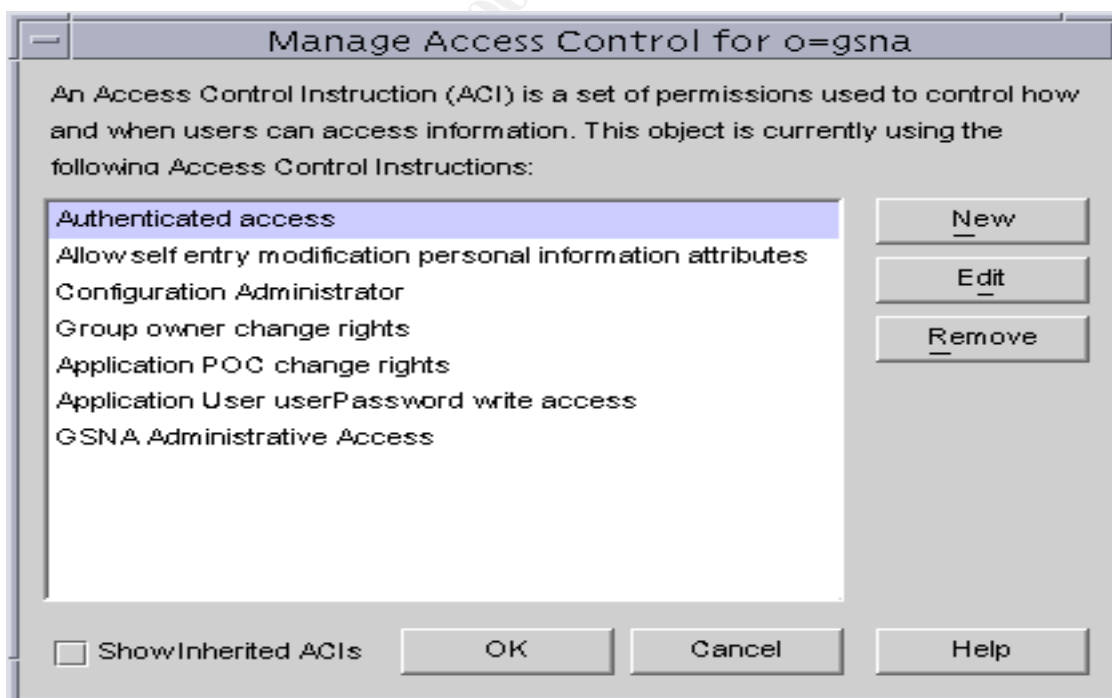


Figure 11 – ACI List for o=gsna

The most important ACL on this list is the one for “Configuration Administrator”. This ACL defines which user can make administrative changes to the information in the DS database (including modifications of the ACLs for the database). This ACL needs to be limited to as few users as possible. In the case of this particular DS server, this privilege is granted only to the original DS Administrator that was set up during the creation of this instance and to a select few users in the “Directory Administrators” container. It’s a good idea for DS Administrators to have their own separate user names so that there is traceability for any modifications that is made to the database. Figure 12 shows the syntax of the “Configuration Administrator” ACL.

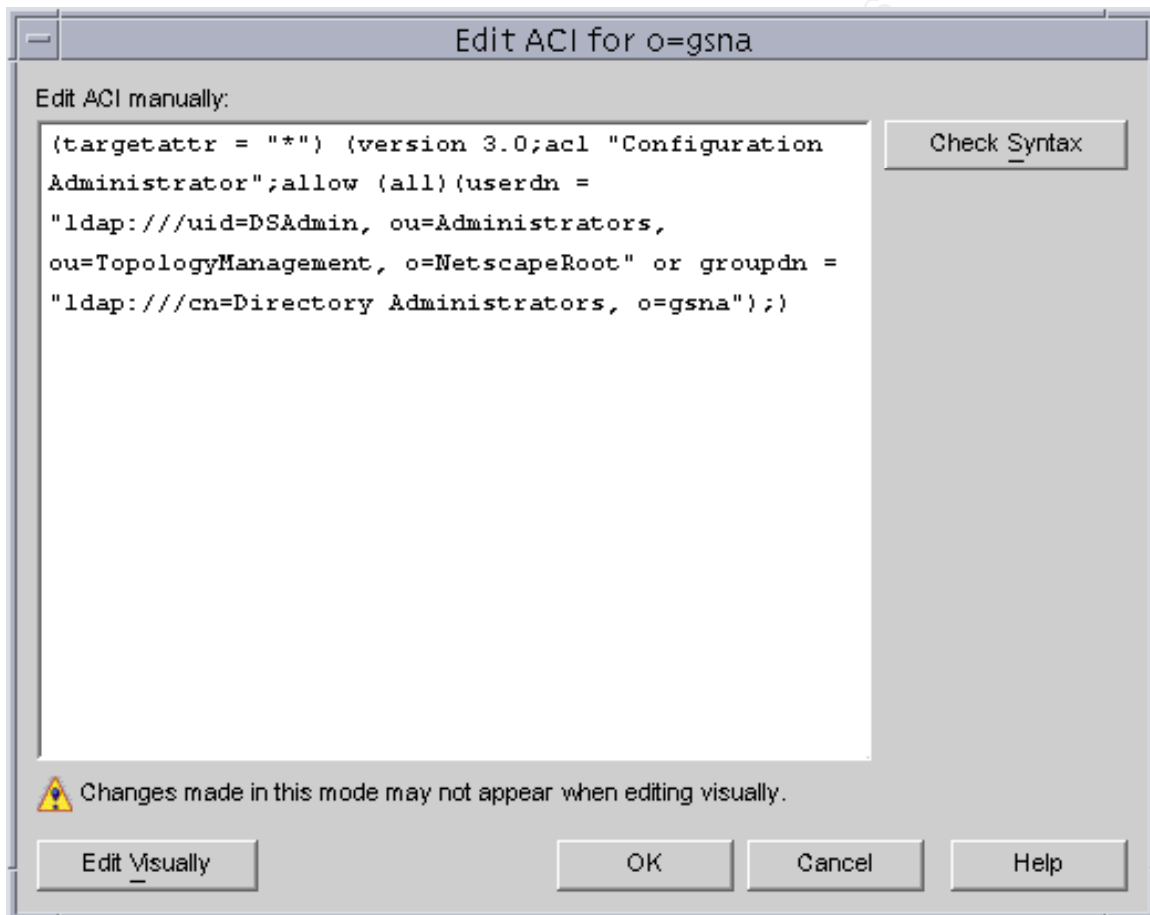


Figure 12 – Configuration Administrator ACL

The other ACLs on the list are much more restrictive in the information that they allow certain users to modify. For example, one of the ACLs mentioned in Figure 11 is called “Allow self entry modification personal information attributes”. This ACL allows individual users who are authenticated in through this DS server to modify certain attributes about themselves. This cannot be done directly through the DS GUI, however, because individual users are not allowed to log in administratively into the DS GUI. Instead, these modifications can be made while a user is logged in to one of the servers on the back-end of the network

that requires LDAP-based authentication. Even though a user may make changes to his own information, there are many attributes that he may not modify, such as the password expiration time, his user ID (i.e., "uid"), and his password history, to name a few. The entire ACI is shown in Figure 13.

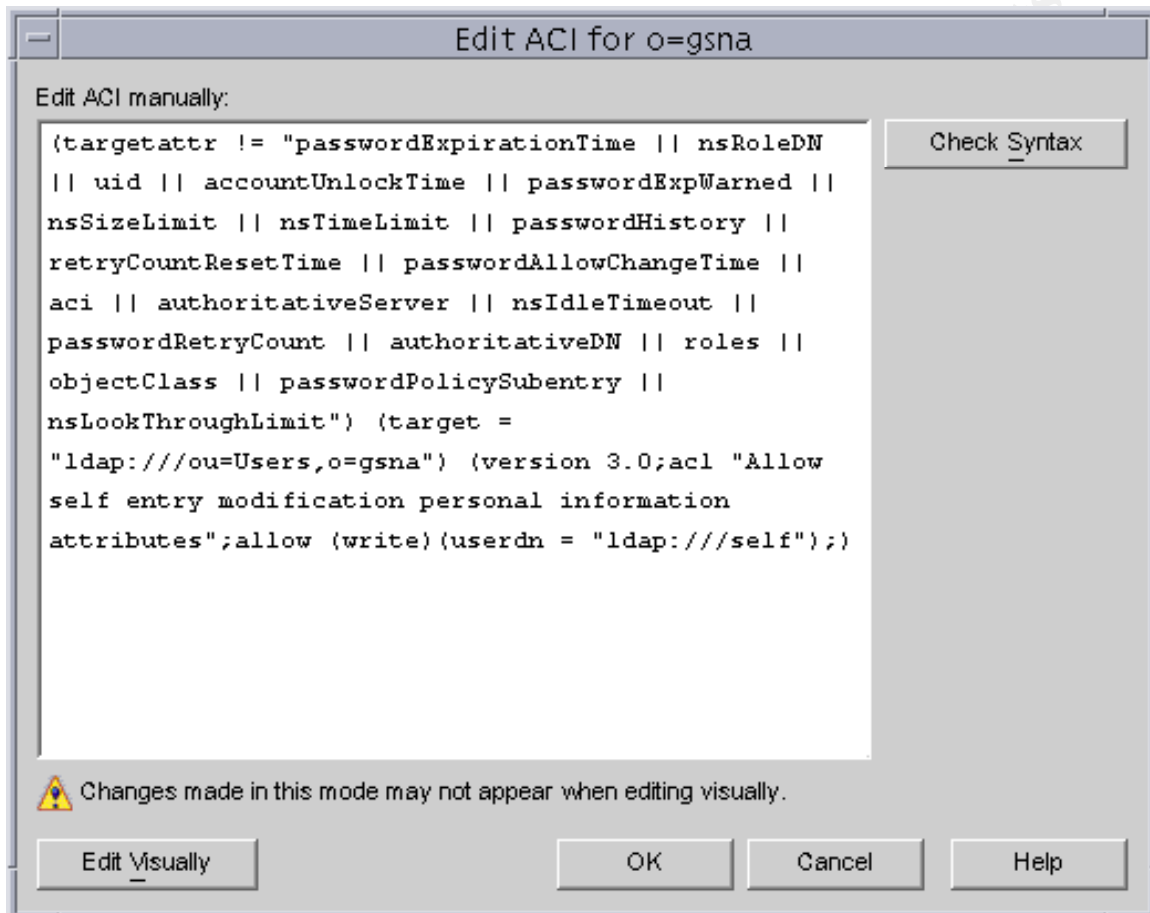


Figure 13 – Allow Self Modification ACI

An inspection of the other ACIs in the list showed similar restrictions to users that have access to other information in the database. The ACIs on this DS server are well defined, and they allow users to access all the information that they will need without giving them too many privileges.

RESULT: PASS

4.10 Test #10 – Password Strength

I asked the administrators of the DS server if a "strong" password had been chosen for the DS Administrator account. In order to qualify as a strong password, it had to adhere to the following standards listed in the company's internal documentation:

- Password must be at least 8 characters long
- Password must include at least 3 of the following types of characters: uppercase, lowercase, numbers, special characters, or symbols.
- Password cannot match any 8-character dictionary word.
- Password cannot contain any part of the username.
- Password must be changed every 180 days.

Without giving away what the password is, the administrators informed me that the password they chose for the DS Administrator did not meet all of the above criteria. In fact, the password only adhered to 2 of the items listed above.

I then asked the administrators about the password that was set up for the owner of the DS directories (on this system, the owner is “dsuser”, and he belongs to the group “dsgroup”). Again, this password only adhered to 2 of the criteria listed above. The fact that this password is weak should cause some concern as well because a determined malicious user could log in or “su” to that username and be able to access all the DS directories.

Although the DS server is located in a secure area with “trusted” personnel, the fact that the DS Administrator and DS owner have weak passwords is something that should be addressed immediately. A stronger password may be more difficult to remember, but it would be a small price to pay to ensure that there is one more line of defense between the data and a malicious intruder.

RESULT: FAIL

4.11 Test #11 – DS Logging Setup

The next three Figures show the configuration for the access, errors, and audit logs for the DS server.

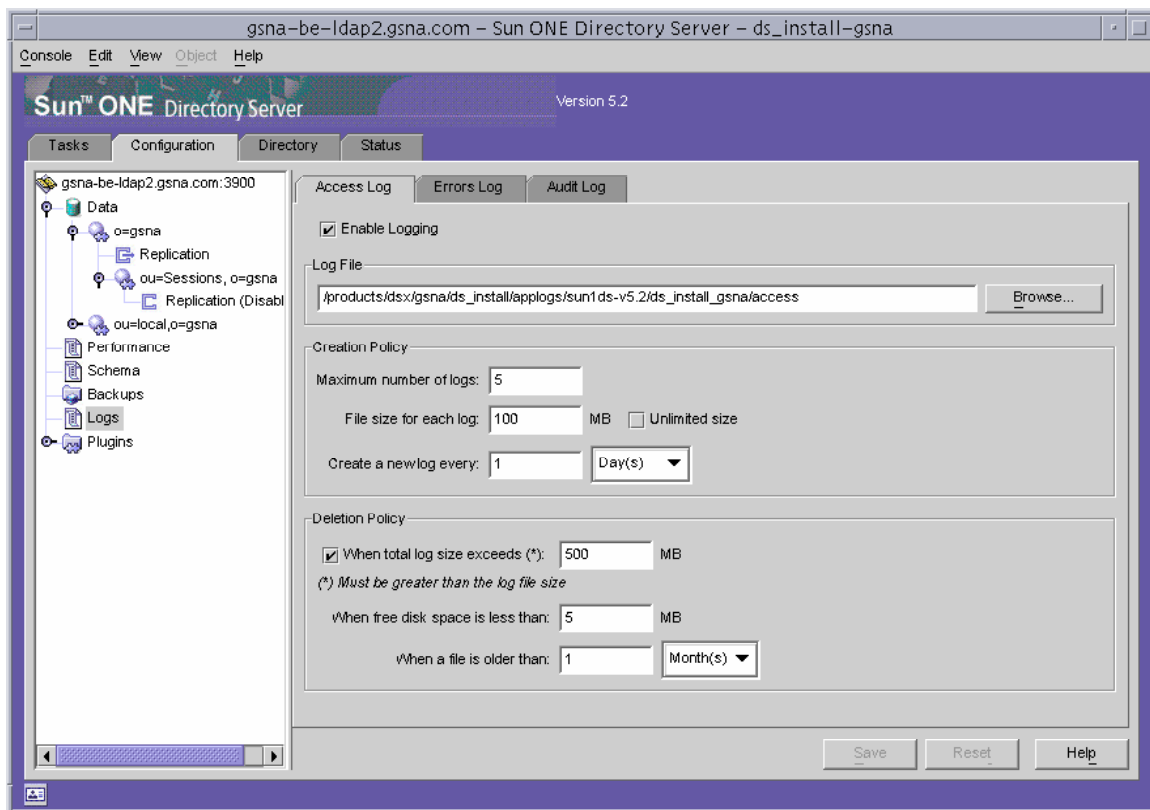


Figure 14 – Access Logs Configuration

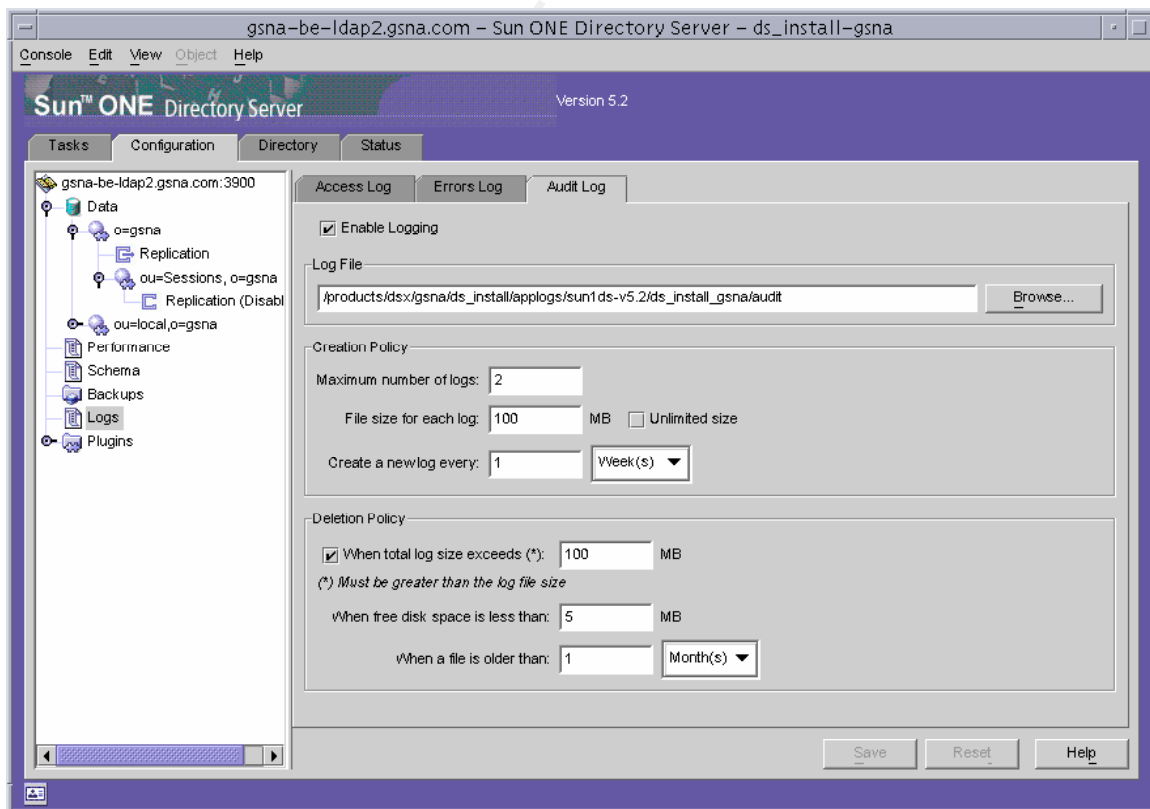


Figure 15 – Audit Logs Configuration

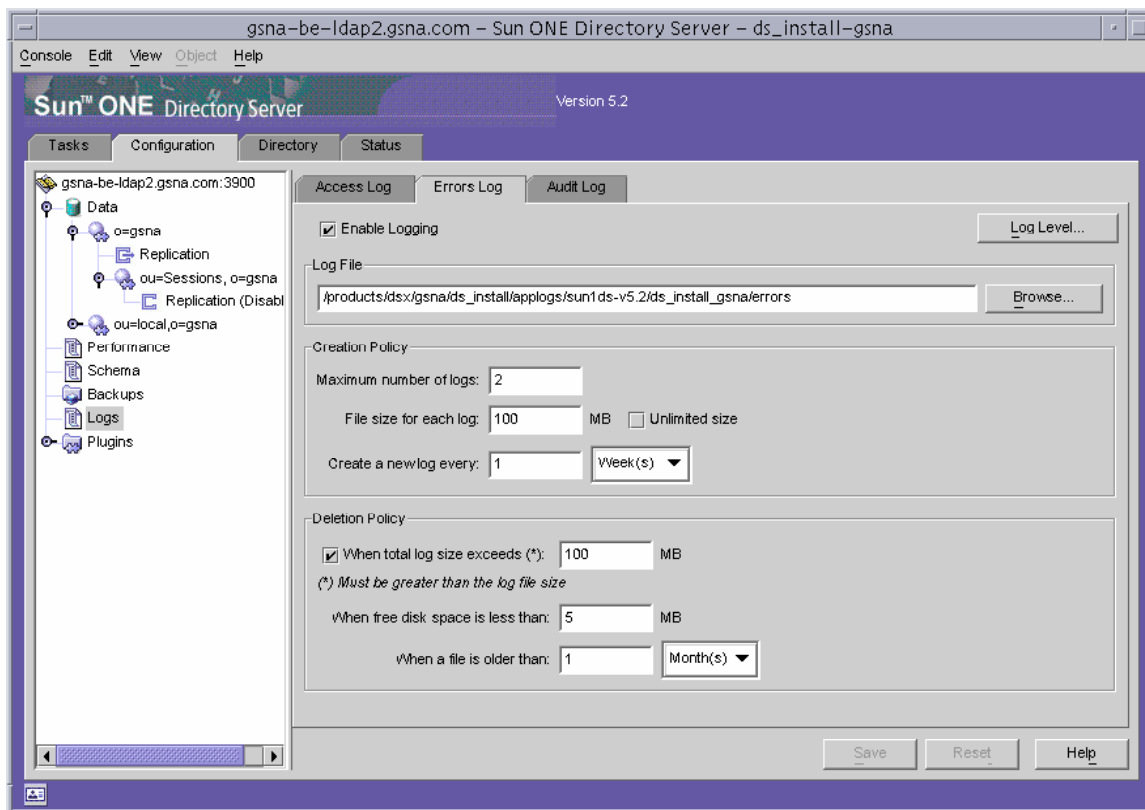


Figure 16 – Errors Logs Configuration

These screen shots show that the access, audit, and errors files are all being written to the same directory. The administrators have ensured that the “Maximum number of logs:” value has been set to at least 2 for each log. This ensures a proper rotation scheme when any of these files get too big.

The administrators have changed the default directory structure for these logs because they wanted better organization of all the log files. The access, errors, and audit files are located under the `/products/dsx/gsna/ds_install/applogs` directory. The administrators also wanted this same type of organization for the replication logs (changelogs), the DB cache logs (dbcache), and the Transaction logs (txnlogs). These directories are shown in Figure 17.

The next screenshot also shows that the access, audit, and errors logs are being properly written to the directory that was defined in the three previous screenshots. At the end of Figure 17, we see that the partition in which the logs are being stored has plenty of room to allow for the rapid growth of these files.

```

Terminal
Window Edit Options Help

# pwd
/products/dsx/gsna/ds_install
# ls -al
total 14
drwx----- 7 dsuser  dsgroup  512 Mar 11 22:44 .
drwxr-xr-x  3 root    other    512 Mar 11 22:43 ..
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:43 applogs
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:44 changelogs
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:44 dbcach
drwxr-xr-x 20 dsuser  dsgroup 1024 Mar 12 19:21 sun1ds-v5.2
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:44 txnlogs
# ls -altR applogs
applogs:
total 6
drwx----- 7 dsuser  dsgroup  512 Mar 11 22:44 ..
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:43 .
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:43 sun1ds-v5.2

applogs/sun1ds-v5.2:
total 6
drwx----- 2 dsuser  dsgroup  512 Mar 12 19:40 ds_install_gsna
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:43 .
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:43 ..

applogs/sun1ds-v5.2/ds_install_gsna:
total 1128
-rw----- 1 dsuser  dsgroup 489685 Mar 13 02:50 access
-rw----- 1 dsuser  dsgroup 30708  Mar 13 02:50 errors
-rw----- 1 dsuser  dsgroup 41023  Mar 13 02:25 audit
drwx----- 2 dsuser  dsgroup  512 Mar 12 19:40 .
-rw----- 1 dsuser  dsgroup  63 Mar 12 19:40 audit.rotationinfo
-rw----- 1 dsuser  dsgroup  63 Mar 12 19:39 errors.rotationinfo
-rw----- 1 dsuser  dsgroup  63 Mar 12 19:39 access.rotationinfo
drwx----- 3 dsuser  dsgroup  512 Mar 11 22:43 ..
# cd applogs/sun1ds-v5.2/ds_install_gsna
# df -k .
Filesystem      kbytes  used  avail capacity  Mounted on
/dev/dsk/c0t0d0s0 4156926 977161 3138196    24%    /
# █

```

Figure 17 – DS Log Directories

The administrators have done a good job in ensuring that the DS logging schemes have been properly configured.

RESULT: PASS

4.12 Test #12 – Replication Setup

In order to verify that replication is configured correctly between the two DS servers on the system, we first need to inspect the settings of the replication agreements on both servers. Before replication can be configured, however, the settings for the replication logs and the Replication Manager (a special account that controls replication between two DS servers) must be correct. Figure 18

shows that a password for the Replication Manager has been set, and the administrators have set up the directory structure for the replication logs.

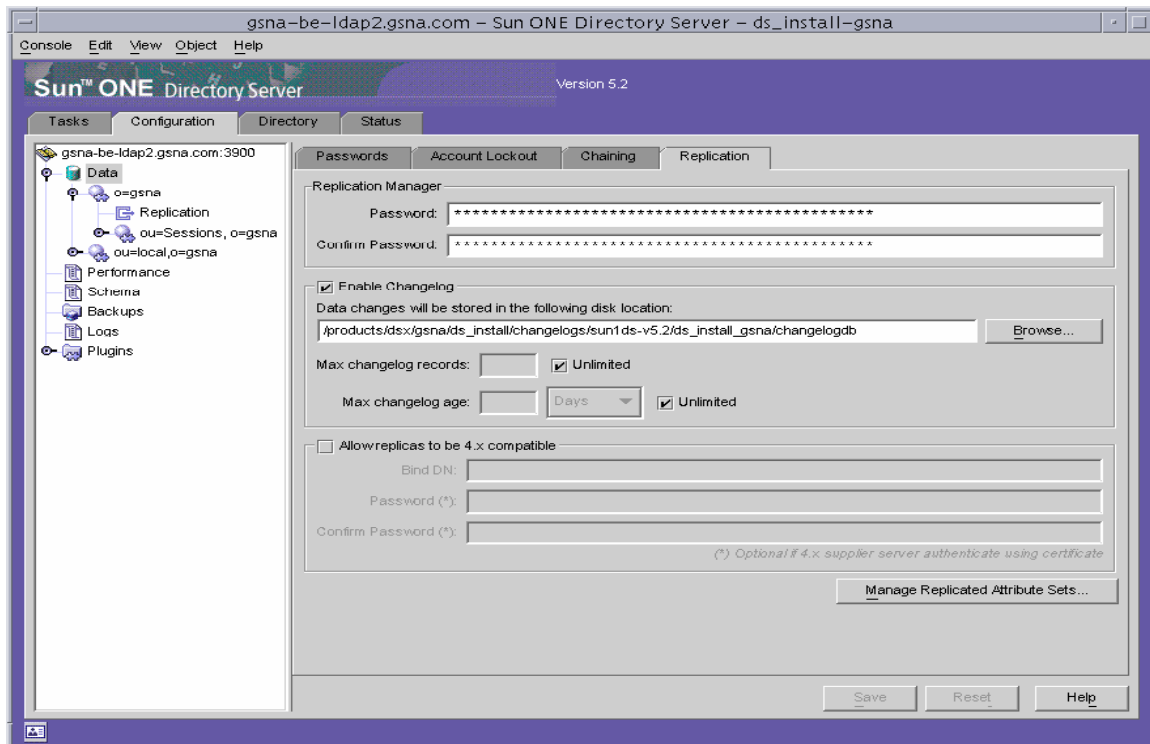


Figure 18 – Replication Configuration

Figure 19 shows that the directory structure on the server has been set up properly, and the replication information file is stored in the proper directory.

© SANS Institute 2000 - 2005

```

Terminal
Window Edit Options Help

# pwd
/products/ds/gsna/ds_install
# ls -al
total 14
drwx----- 7 dsuser dsgroup 512 Mar 11 22:44 .
drwxr-xr-x 3 root other 512 Mar 11 22:43 ..
drwx----- 3 dsuser dsgroup 512 Mar 11 22:43 applogs
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 changelogs
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 dbcache
drwxr-xr-x 20 dsuser dsgroup 1024 Mar 12 19:21 sun1ds-v5.2
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 txnlogs
# ls -altR changelogs
changelogs:
total 6
drwx----- 7 dsuser dsgroup 512 Mar 11 22:44 ..
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 .
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 sun1ds-v5.2
changelogs/sun1ds-v5.2:
total 6
drwx----- 3 dsuser dsgroup 512 Mar 12 20:12 ds_install_gsna
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 .
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 ..
changelogs/sun1ds-v5.2/ds_install_gsna:
total 6
drwx----- 2 dsuser dsgroup 512 Mar 12 21:01 changelogdb
drwx----- 3 dsuser dsgroup 512 Mar 12 20:12 .
drwx----- 3 dsuser dsgroup 512 Mar 11 22:44 ..
changelogs/sun1ds-v5.2/ds_install_gsna/changelogdb:
total 36
-rw----- 1 dsuser dsgroup 16384 Mar 13 02:25 o_gsna42334d11000000370000.
db3
drwx----- 2 dsuser dsgroup 512 Mar 12 21:01 .
drwx----- 3 dsuser dsgroup 512 Mar 12 20:12 ..
# █

```

Figure 19 – Replication Directory Structure

Next, we want to verify that the replication agreements between the two servers have been properly configured based on the company's baselines. Since either of the two DS servers could be acting as the primary server at any given time, we want both LDAP instances to be configured as a master of the other. This means that any changes made in one of the servers will be replicated over to the other server. This is known as a "multiple master" configuration.

Figure 20 shows the replication configuration on the primary DS server (i.e., the focus of this audit). Its IP address is 10.10.10.150. According to the screenshot, this server is replicating its information to the secondary DS server, IP address of 10.10.10.140.

© SANS Institute

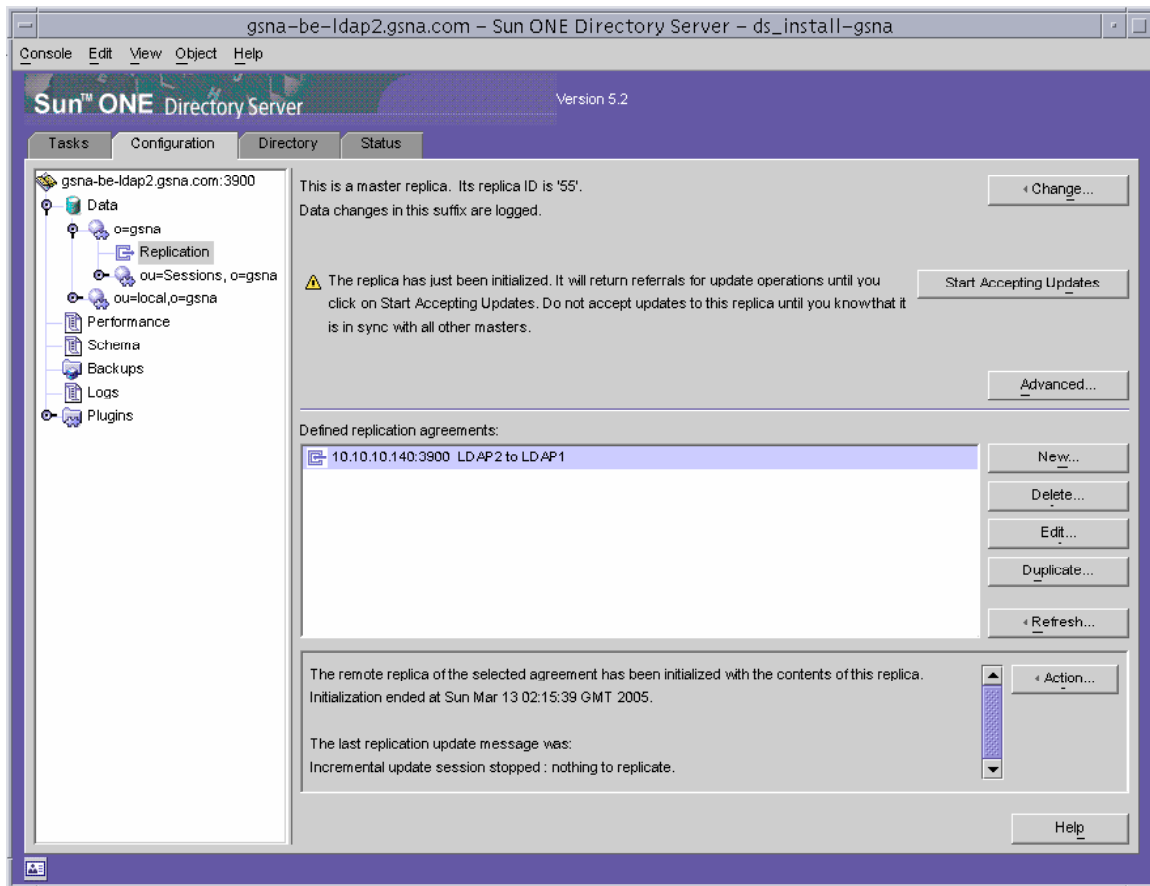


Figure 20 – Primary DS Server Replication Configuration

If we highlight the name of the replication agreement and click the “Edit...” button, we can see more details about this configuration. The window shown in Figure 21 gives details about the IP address and port number to which this server is replicating, and it allows the administrator to modify the settings of the Replication Manager.

© SANS Institute 2000 - 2005

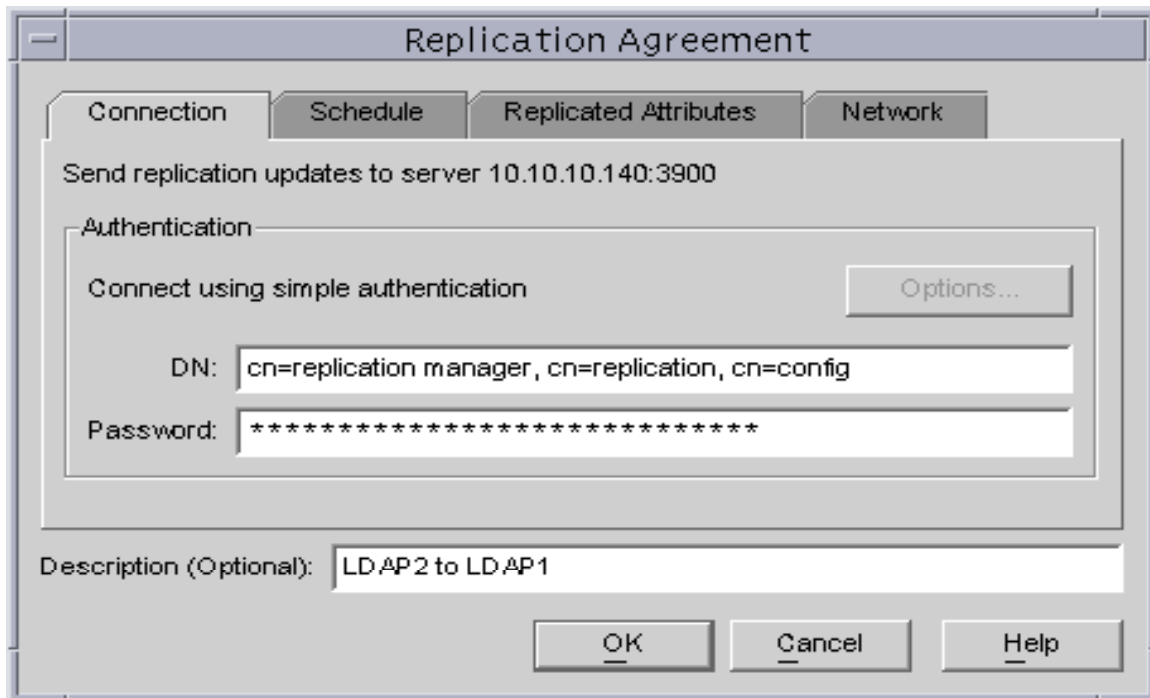


Figure 21 – Replication Agreement (Connection)

Because of the nature of the network, the databases always need to be kept in sync with each other, as demonstrated in Figure 22.

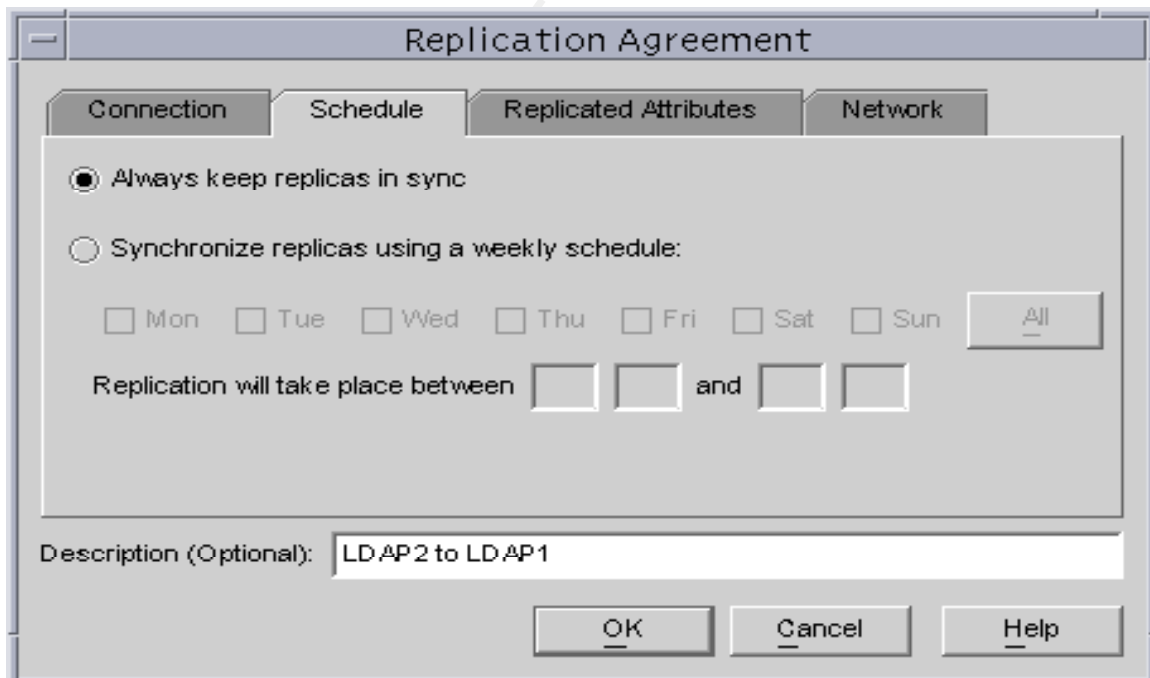


Figure 22 – Replication Agreement (Schedule)

An inspection of the secondary DS server shows similar settings and configurations. In this respect, the agreements between the two DS servers

have been properly set up.

A simple test was run to ensure that the replication agreement between the two DS servers was working properly, and this is demonstrated in the following 8 screenshots. First, we inspected the “ou=Users,o=gsna” container on both servers. Each of them contained the users shown in Figure 23.

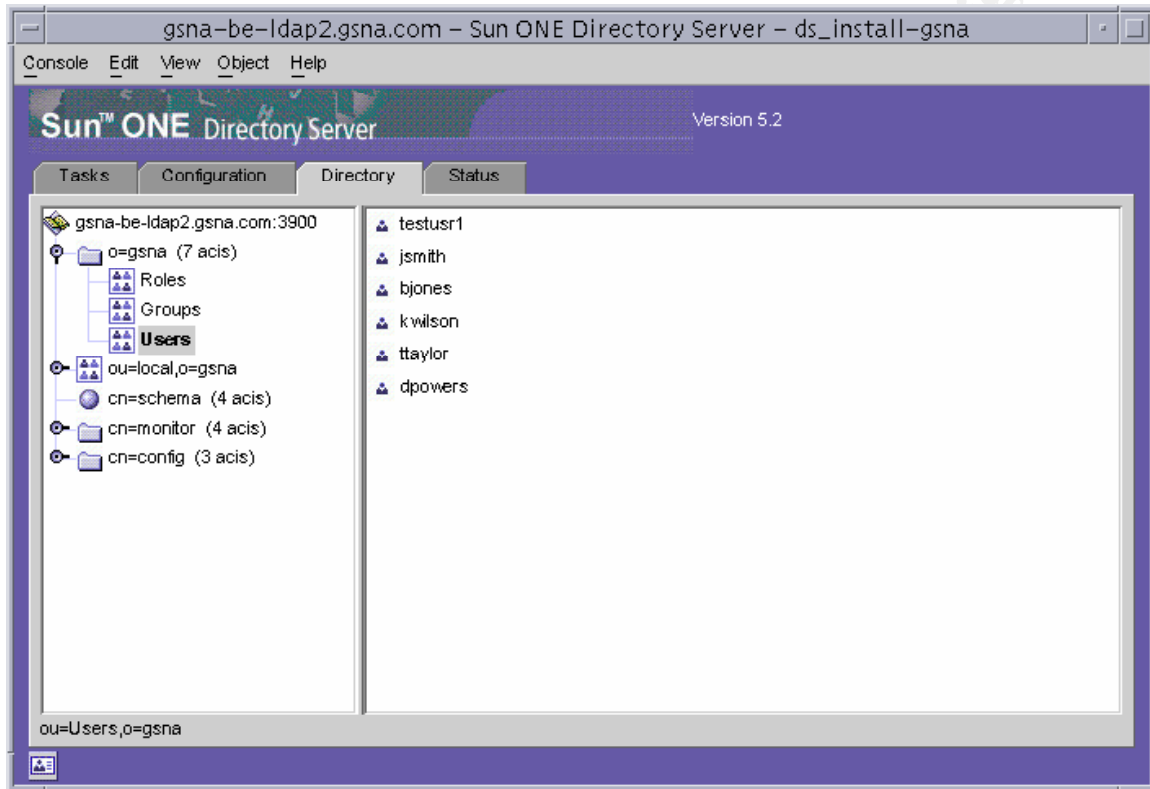


Figure 23 – ou=Users,o=gsна

The next step was to create a new user within this container. This can be done by selecting “Object -> New -> User” from the drop-down menu at the top of the window.

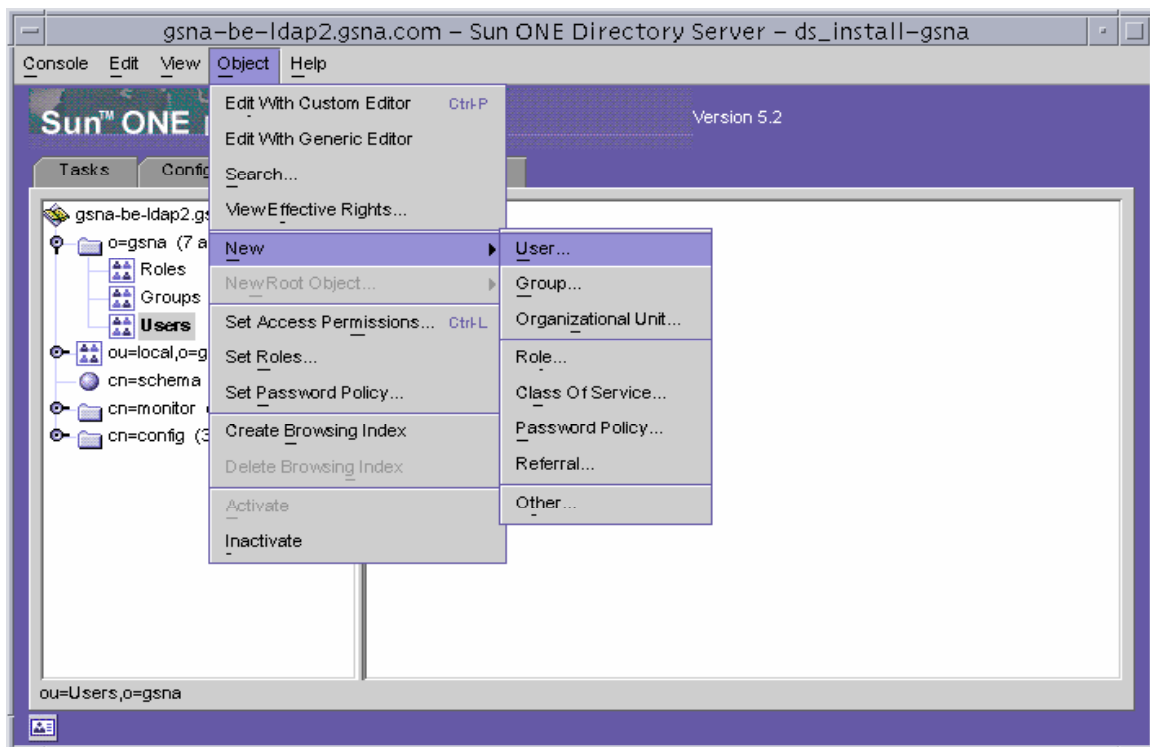


Figure 24 – Create a New User

When the “Create New User” window popped up, we entered information for a new user named “Steve Butler” (whose user ID will be “sbutler”).

 The screenshot shows the "Create New User" dialog box. On the left is a sidebar with "User" selected. The main area contains the following fields:

- * First Name: steve
- * Last Name: butler
- * Common Name(s): steve butler
- User ID: sbutler
- Password: *****
- Confirm Password: *****
- E-Mail: (empty field) (e.g., user@company.com)
- Phone: (empty field)
- Fax: (empty field)

 At the bottom, there is a note: "* Indicates a required field". The dialog has "Access Permissions Help", "OK", "Cancel", and "Help" buttons.

Figure 25 – Creating Steve Butler

Once the proper information was entered, we observe that the new user (sbutler) now exists in the “Users” database.

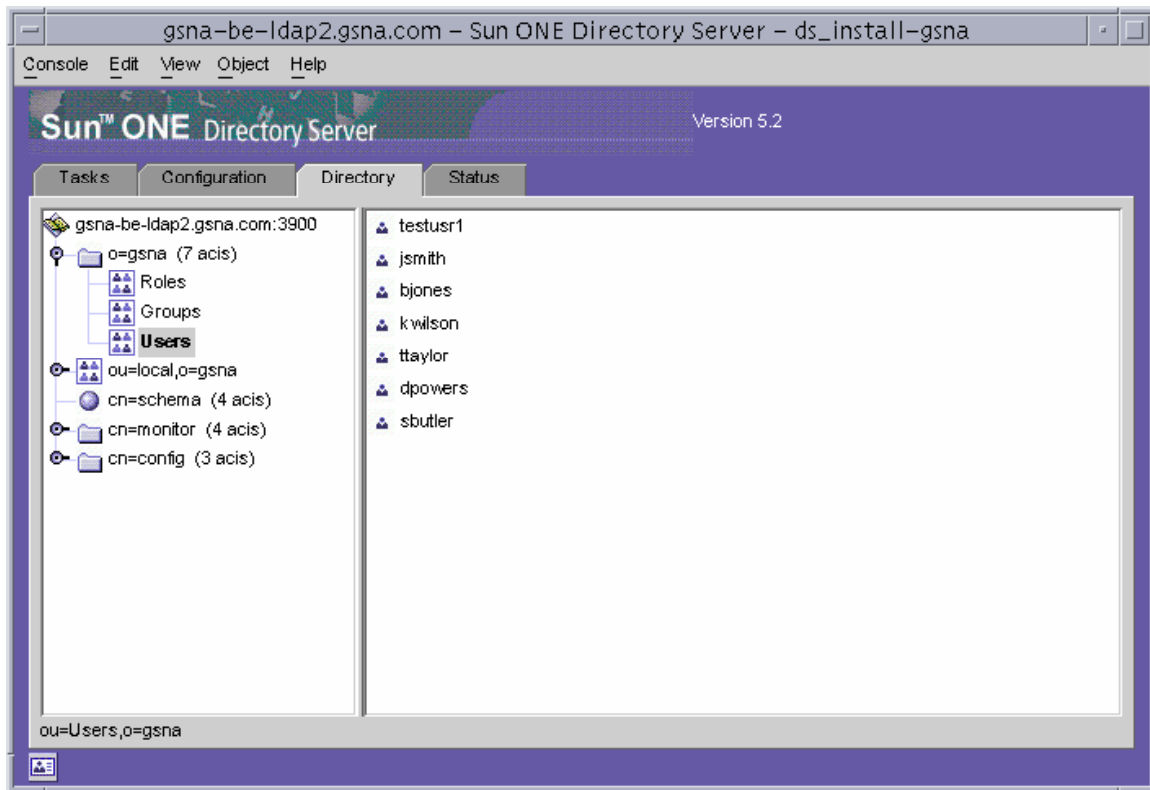


Figure 26 – Users Database with Steve Butler

Once Steve’s information had been entered on the primary DS server, we then checked the DS instance that exists on the secondary DS server. The following Figure shows that this was indeed the case.

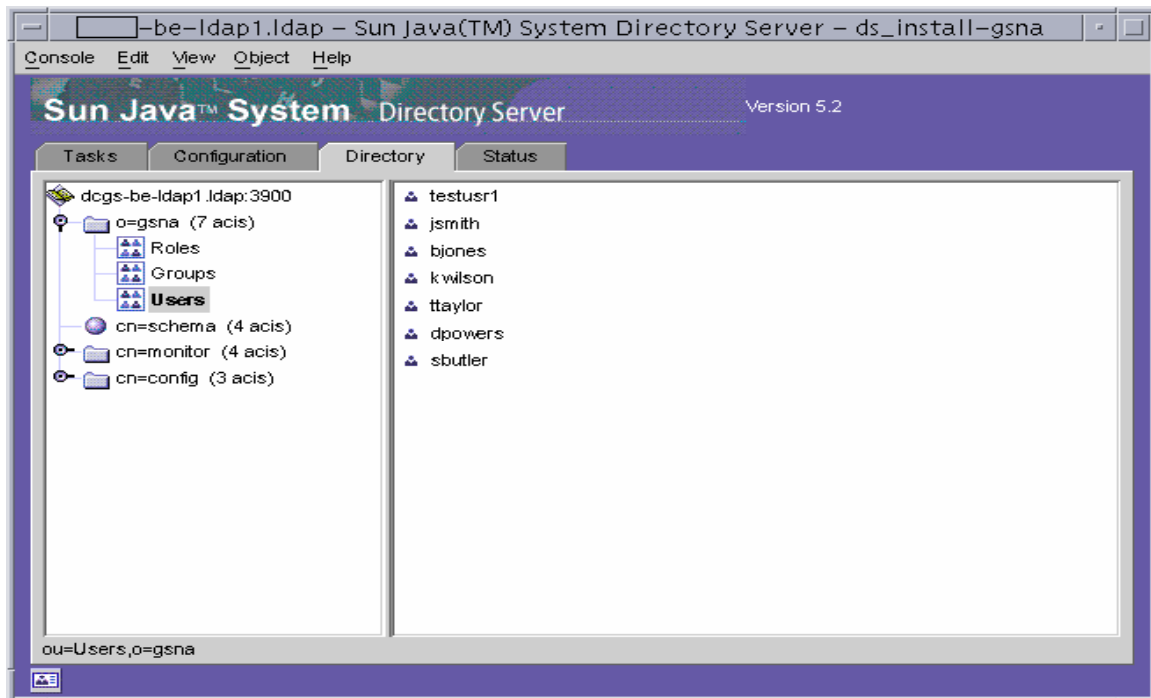


Figure 27 – Secondary Server with Steve's Information

This proves that replication is working properly from the primary DS server to the secondary DS server. In order to prove that replication is working in the opposite direction, we deleted one of the users (kwilson) from the secondary server, as shown in Figure 28.

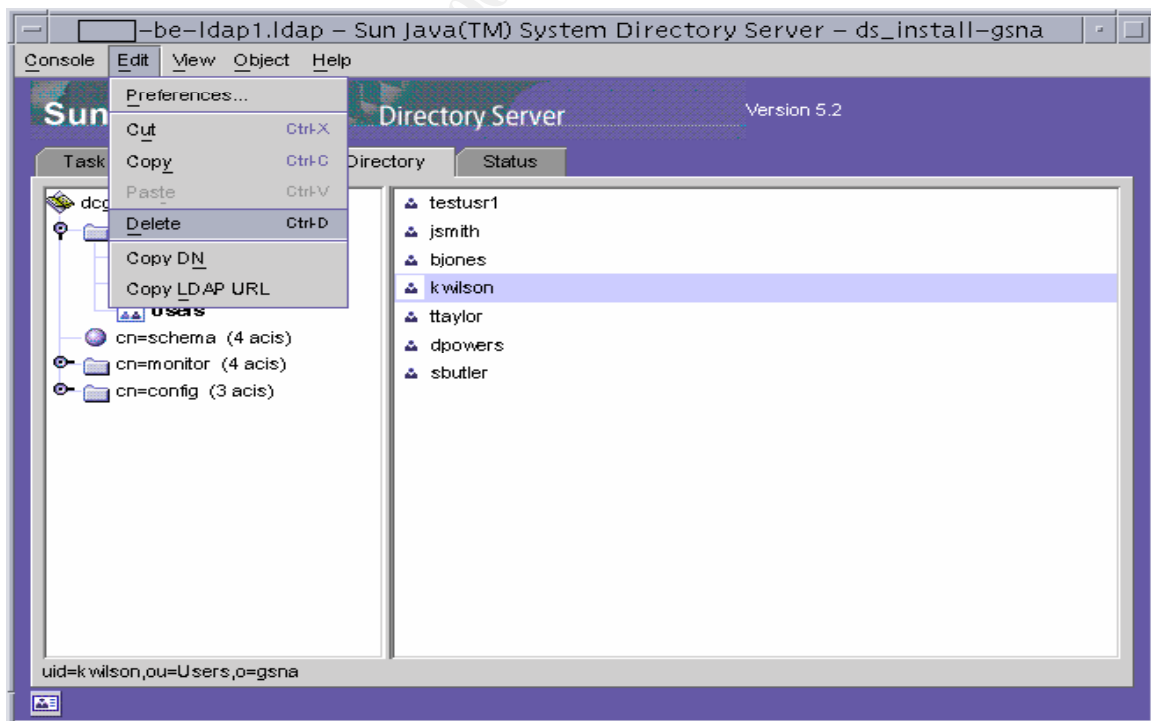


Figure 28 – Deleting kwilson from the Secondary Server

As we see in the next screenshot, kwilson is gone.

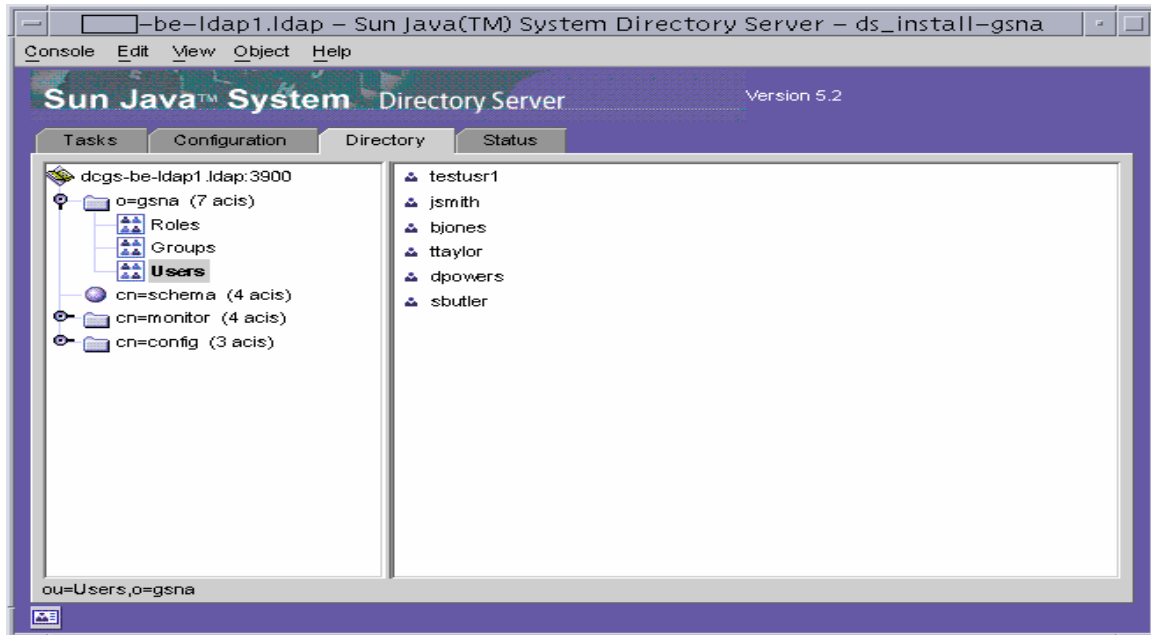


Figure 29 – Updated Secondary Database

The final screenshot shows the updated information in the primary DS server. The “ou=Users,o=gsna” containers are identical to each other, which proves that replication is working in both directions.

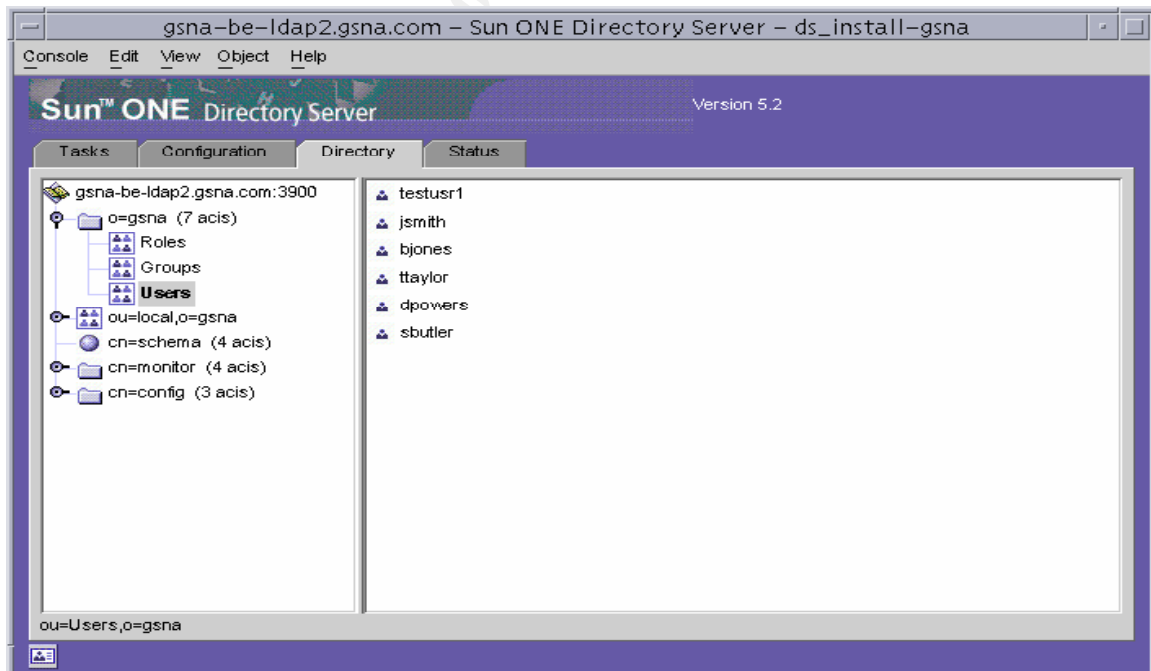


Figure 30 – Updated Primary Database

All aspects of the replication agreements checked out, and this functionality appears to be working properly on both DS servers.

RESULT: PASS

4.13 Test #13 – Password Security Policy

According to the company's password policy, the following criteria must be met:

- Allow users to change their passwords after 3 days.
- Keep a history of the last 5 passwords for each user.
- Force a password change every 180 days.
- Lockout a user after 3 failed password attempts.
- Unlock a user after 30 minutes if 3 bad passwords were entered.
- Send a warning 15 days before a password is about to expire.

Figures 31 and 32 show the Account Lockout and Password policy configurations in the DS server.

© SANS Institute 2000 - 2005, Author retains full rights.

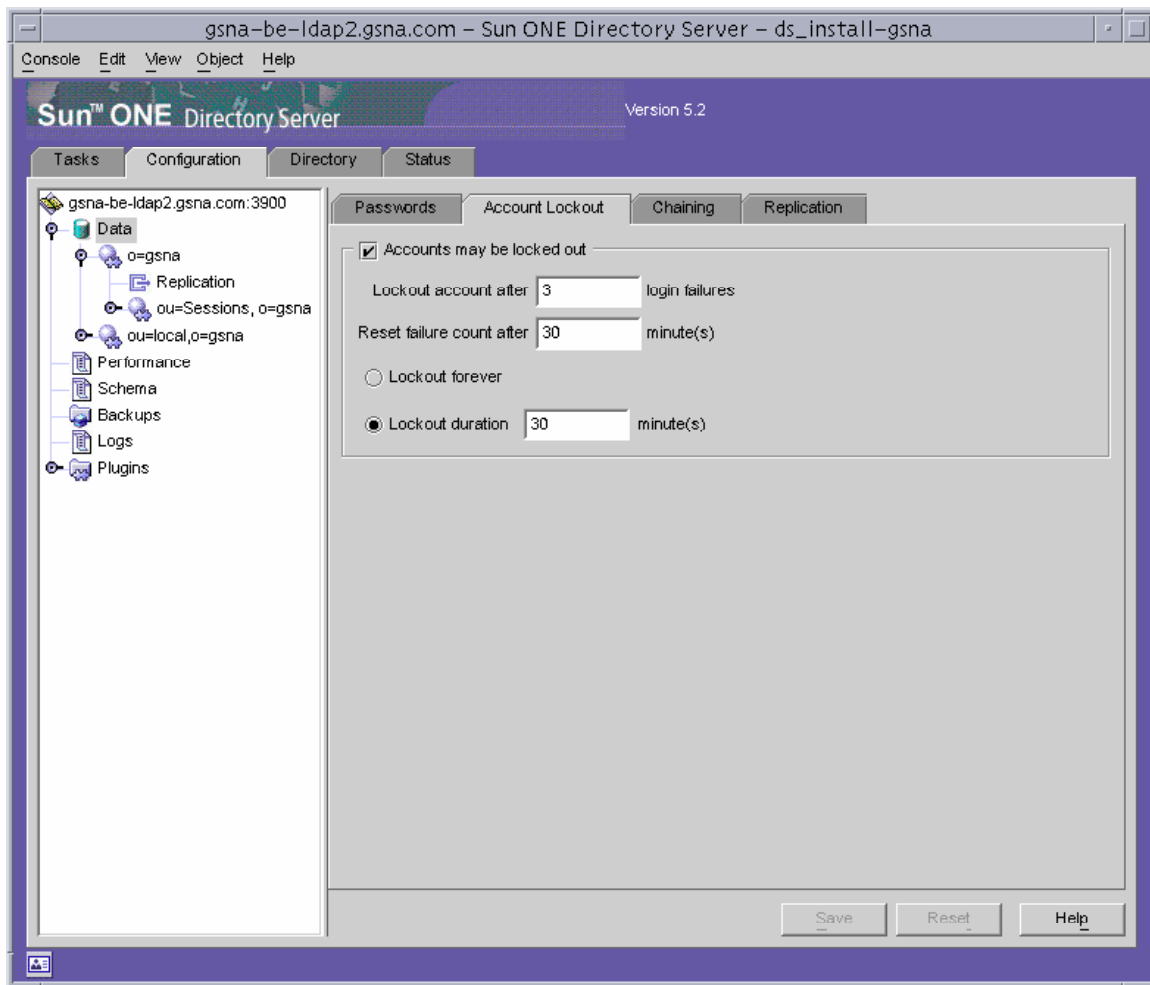


Figure 31 – Account lockout policy

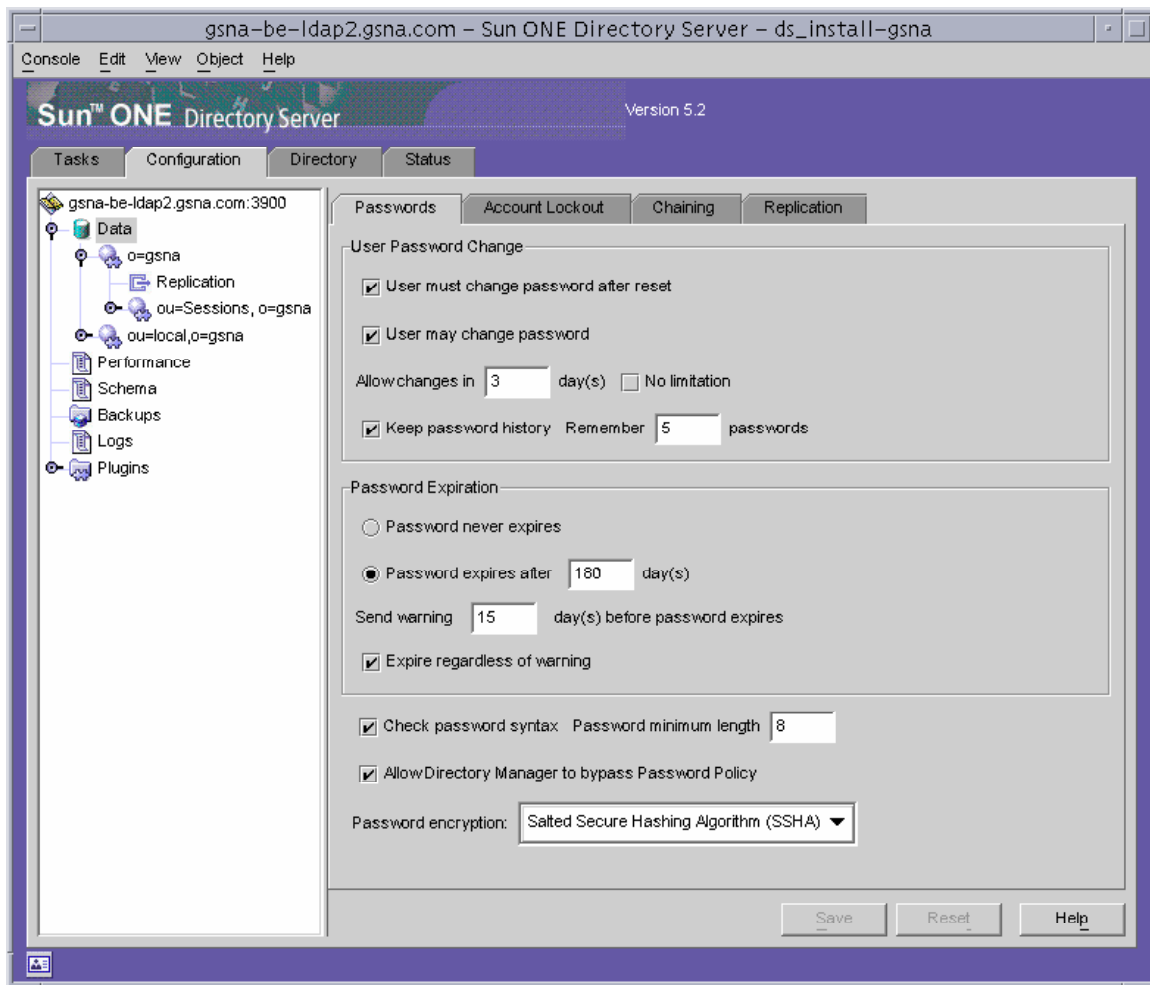


Figure 32 – Password policy

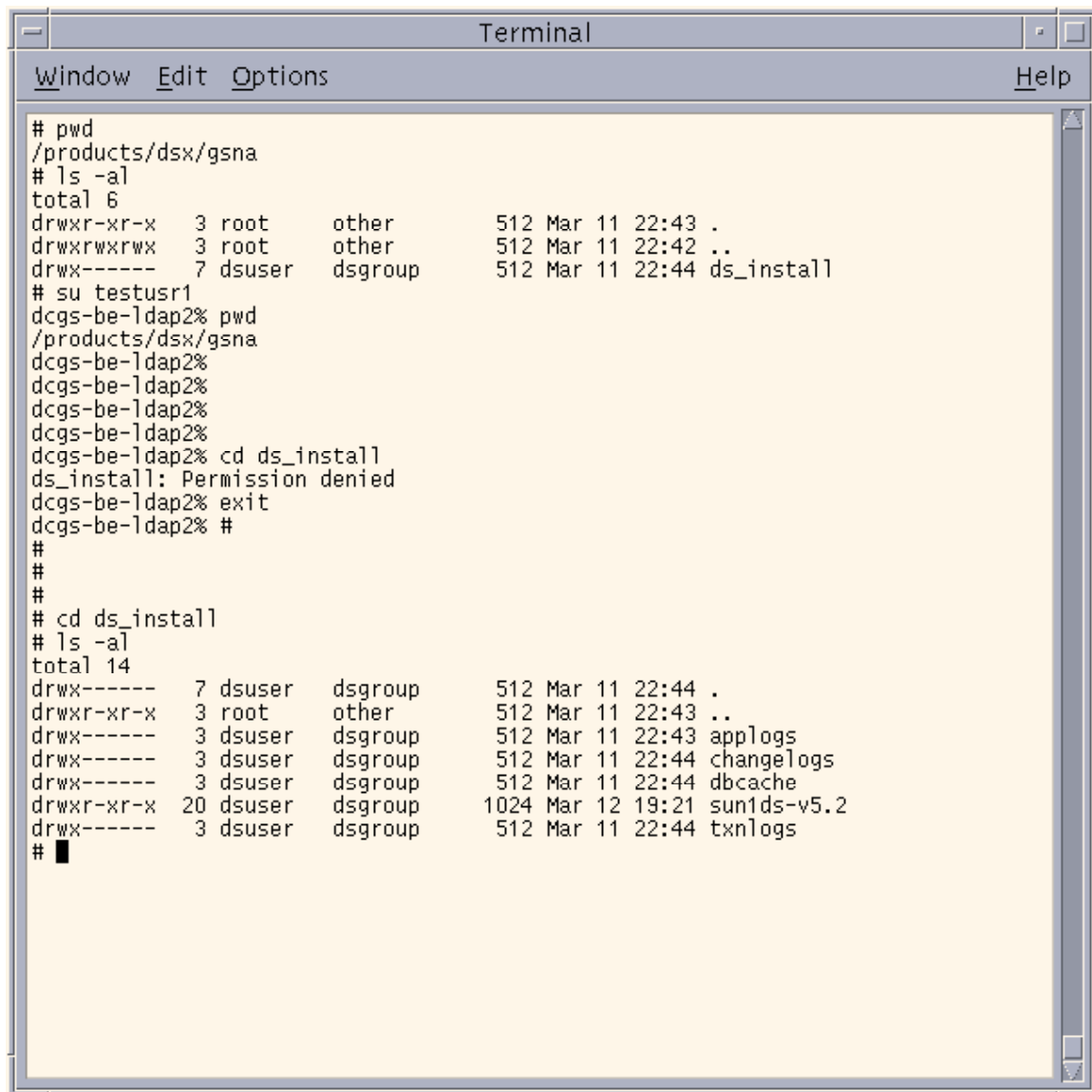
The settings in the user instance of the DS server have been properly configured to meet the company's security requirements.

RESULT: PASS

4.14 Test #14 – Lockdown of DS-specific Directories

For the purposes of this audit, the Sun ONE DS application has been stored in the /products/dsx/gsna/ds_install/sun1ds-v5.2 directory on the DS server. Figure 33 provides a demonstration of what happens when a user who is not the DS owner (dsuser) or root attempt to access these directories.

According to Figure 33, the permissions have been set at 700 at the "ds_install" subdirectory. Also, the permissions of all the customized logging directories have been set to 700. "Testusr1" attempted to access the "ds_install" directory, but was denied access.



```
# pwd
/products/ds/gsna
# ls -al
total 6
drwxr-xr-x  3 root    other      512 Mar 11 22:43 .
drwxrwxrwx  3 root    other      512 Mar 11 22:42 ..
drwx----- 7 dsuser  dsgroup   512 Mar 11 22:44 ds_install
# su testusr1
dcgs-be-ldap2% pwd
/products/ds/gsna
dcgs-be-ldap2%
dcgs-be-ldap2%
dcgs-be-ldap2%
dcgs-be-ldap2%
dcgs-be-ldap2% cd ds_install
ds_install: Permission denied
dcgs-be-ldap2% exit
dcgs-be-ldap2% #
#
#
#
# cd ds_install
# ls -al
total 14
drwx----- 7 dsuser  dsgroup   512 Mar 11 22:44 .
drwxr-xr-x  3 root    other      512 Mar 11 22:43 ..
drwx----- 3 dsuser  dsgroup   512 Mar 11 22:43 applogs
drwx----- 3 dsuser  dsgroup   512 Mar 11 22:44 changelogs
drwx----- 3 dsuser  dsgroup   512 Mar 11 22:44 dbcach
drwxr-xr-x 20 dsuser  dsgroup  1024 Mar 12 19:21 sun1ds-v5.2
drwx----- 3 dsuser  dsgroup   512 Mar 11 22:44 txnlogs
# █
```

Figure 33 – DS directory permissions

The permissions on the DS directories have been properly locked down at a point where nobody except root or dsuser can access the internal information.

RESULT: PASS

4.15 Test #15 – Data Backup Plan

According to internal documentation provided by the administrators, the DS database is backed up using a combination of DS-provided scripts and Veritas NetBackup [12] on a nightly basis. Within the NetBackup directory on the DS server, a couple of shell scripts – bptest.sh and bpend.sh – are used to create the DS backups and prepare for backup to tape.

The bpstart.sh script basically runs the db2bak.pl script [27] on each Directory Server instance that has been created on the server. This Perl script generates a series of files with a “.db3” extension that contain all information captured within the DS database. These files are then stored in a temporary directory (/var/tmp/ldap_backup) on the DS server. Once the Veritas NetBackup application has finished saving everything off to tape, the bpend.sh script cleans up the temporary directory and performs some other “housekeeping” tasks.

The documentation provides steps on how to manually initiate the backup of the DS database. The authors of the document did an excellent job of providing details on how to initiate the NetBackup GUI, which policy to use, and how to properly initiate the backup.

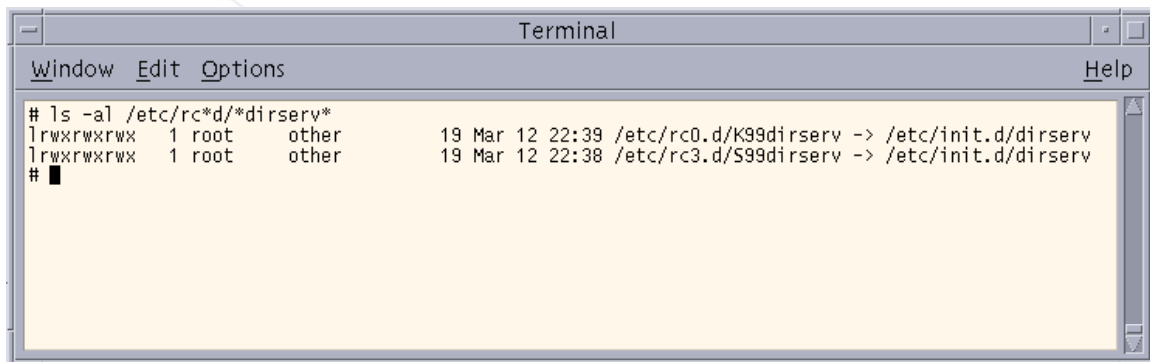
Along with a manual backup, the documentation provides details on how to restore the information to the DS database. This is a two-step process. First, the administrator uses NetBackup to restore the most recent backup to a temporary directory on the DS server. Then, using the bak2db command [26], the information can be restored into the LDAP database.

A plan is in place to ensure that the information in the DS databases is backed up frequently, and there is sufficient documentation that provides background and instruction on this process.

RESULT: PASS

4.16 Test #16 – Startup/Shutdown Scripts

In order to verify that the appropriate startup scripts are in place on the DS server, we first need to look in the /etc/rc*d directories to ensure that some kind of script is called at startup and shutdown. Figure 34 shows that two files are in place to start and stop the DS processes at startup and shutdown.



```
Terminal
Window Edit Options Help
# ls -al /etc/rc*d/*dirserv*
lrwxrwxrwx 1 root other 19 Mar 12 22:39 /etc/rc0.d/K99dirserv -> /etc/init.d/dirserv
lrwxrwxrwx 1 root other 19 Mar 12 22:38 /etc/rc3.d/S99dirserv -> /etc/init.d/dirserv
#
```

Figure 34 - /etc/rc*d/*dirserv*

These links point to the file /etc/init.d/dirserv. This script has been designed to start and stop the DS processes in the correct order, depending on what argument is given to it. The dirserv file is shown below:

```
#!/bin/sh
#
# Directory Server startup script
#

basePath=/products/dsx/gsna/ds_install/sunlds-v5.2

case "$1" in
    start)
        # Start servers
        echo ""
        echo "Starting GSNA Directory Servers ..."
        echo "    Starting slapd-GSNA-config Directory Server ..."
        $basePath/slapd-ds_install-gsna-config/start-slapd
        echo "    Starting administration server ..."
        $basePath/start-admin
        echo "    Starting slapd-GSNA-user Directory Server ..."
        $basePath/slapd-ds_install-gsna/start-slapd
        echo "Done ..."
        echo ""
        ;;

    stop)
        # Stop servers
        echo ""
        echo "Stopping GSNA Directory Servers ..."
        echo "    Stopping slapd-GSNA-user Directory Server ..."
        $basePath/slapd-ds_install-gsna/stop-slapd
        echo "    Stopping administration server ..."
        $basePath/stop-admin
        echo "    Stopping slapd-GSNA-config Directory Server ..."
        $basePath/slapd-ds_install-gsna-config/stop-slapd
        echo "Done ..."
        echo ""
        ;;

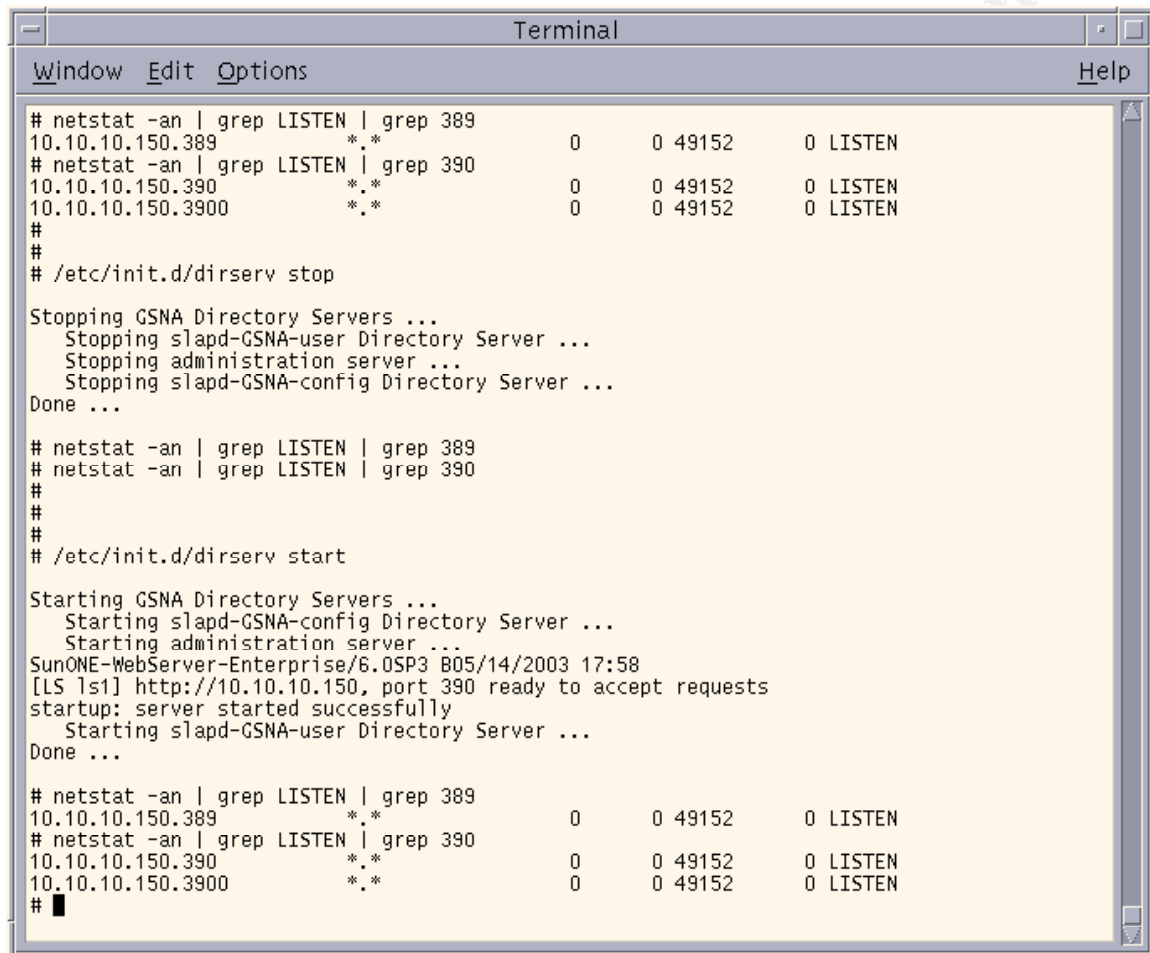
    restart)
        $0 stop
        $0 start
        ;;

    *)
        echo "Usage: dirserv {start|stop|restart}"
        exit 1
esac

exit 0
```

Figure 35 shows the results of stopping and starting these processes by hand using the dirserv script. First, the netstat command has been run to show that

the Config instance (port 389), the administration instance (port 390), and the user instance (port 3900) are all up and listening. Running the command “/etc/init.d/dirserv stop” brings down all these processes, and the ensuing netstat commands prove this. Finally, we ran the “/etc/init.d/dirserv start” command, and all processes were brought up again.



```
Terminal
Window Edit Options Help

# netstat -an | grep LISTEN | grep 389
10.10.10.150.389      *.*                0      0 49152      0 LISTEN
# netstat -an | grep LISTEN | grep 390
10.10.10.150.390     *.*                0      0 49152      0 LISTEN
10.10.10.150.3900    *.*                0      0 49152      0 LISTEN
#
#
# /etc/init.d/dirserv stop

Stopping GSNA Directory Servers ...
  Stopping slapd-GSNA-user Directory Server ...
  Stopping administration server ...
  Stopping slapd-GSNA-config Directory Server ...
Done ...

# netstat -an | grep LISTEN | grep 389
# netstat -an | grep LISTEN | grep 390
#
#
#
# /etc/init.d/dirserv start

Starting GSNA Directory Servers ...
  Starting slapd-GSNA-config Directory Server ...
  Starting administration server ...
SunONE-WebServer-Enterprise/6.0SP3 B05/14/2003 17:58
[LS ls1] http://10.10.10.150, port 390 ready to accept requests
startup: server started successfully
  Starting slapd-GSNA-user Directory Server ...
Done ...

# netstat -an | grep LISTEN | grep 389
10.10.10.150.389      *.*                0      0 49152      0 LISTEN
# netstat -an | grep LISTEN | grep 390
10.10.10.150.390     *.*                0      0 49152      0 LISTEN
10.10.10.150.3900    *.*                0      0 49152      0 LISTEN
# █
```

Figure 35 – Dirserv output

This script and the links in the /etc/rc*d directories have been properly configured to start/stop the DS instances at the appropriate times.

RESULT: PASS

4.17 Test #17 – Vulnerability Scans

A Nessus scan was run to determine which ports are open on the DS server that could lead to potential exploits. The Nessus application, which has a built-in Nmap server, was run from one of the other servers on the back end of this network [11, 9]. The final report showed which ports were open on the DS

server and the potential risk in keeping these ports open.

- *telnet (23/tcp) (Security warnings found)*
- *ssh (22/tcp) (Security notes found)*
- *ftp (21/tcp) (Security notes found)*
- *rpcbind (111/tcp) (Security notes found)*
- *uis (390/tcp) (Security notes found)*
- *ldap (389/tcp) (Security hole found)*
- *shell (514/tcp) (Security warnings found)*
- *udt_os (3900/tcp)*
- *lockd (4045/tcp) (Security notes found)*
- *X11 (6000/tcp)*
- *sometimes-rpc7 (32772/tcp) (Security notes found)*
- *sometimes-rpc5 (32771/tcp) (Security notes found)*
- *general/tcp (Security warnings found)*
- *sunrpc (111/udp) (Security notes found)*
- *lockd (4045/udp) (Security warnings found)*
- *sometimes-rpc8 (32772/udp) (Security hole found)*
- *general/udp (Security notes found)*
- *general/icmp (Security warnings found)*

For each port that is open, Nessus returns any information that it found while scanning on that port. Based on this information, it lets the user know the severity of the issue that was discovered. A “security hole” represents an issue that needs to be addressed as soon as possible. A “security warning” means that the risk is usually low, but the issue should ideally be resolved. When Nessus returns a “security note”, it means that the scan discovered some information that does not immediately pose a threat to the system (e.g., what version of SSH or Operating System a server is running), but an attacker could still use this to his/her advantage to gain entry to the system.

This scan found two security holes. The first one is on port 389, which is the LDAP port. The vulnerability is listed as:

Improperly configured LDAP servers will allow the directory BASE to be set to NULL. This allows information to be culled without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user can query your LDAP server using a tool such as 'LdapMiner'

Solution: Disable NULL BASE queries on your LDAP server

According to Microsoft's Support web site, unauthenticated (NULL) connections must be permitted to connect to root DSA-specific Entries (DSE) in order to comply with RFC 2251 [18]. More information about RFC 2251 can be found

here: <http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2251.html>. This is not a problem that is specific to this particular application. Because the ACLs of this particular server are locked down (see Section 3.9), an attacker should not be able to obtain any sensitive information.

The second security hole was on UDP port 32772. The vulnerability analysis is as follows:

The remote statd service may be vulnerable to a format string attack. This means that an attacker may execute arbitrary code thanks to a bug in this daemon.

As noted in Test #5, the RPC services were not disabled by JASS. Once this cleanup is complete, this issue will be resolved.

A few other security-related issues were found by the Nessus scan, but most of them present a low risk to the system. The full Nessus output is located in Appendix C. The issues that pose the largest risk to the system are issues that will be addressed by the comments from Test #5 in Section 3.5. Since no other major issues were discovered, this test is considered a success.

RESULT: PASS (with comments)

© SANS Institute 2000 - 2005, Author retains full rights.

5 Audit Report

5.1 Executive Summary

The following table is a summary of the results of the checklist provided in Section 2 of this report:

Audit Summary		
Item #	Title of Test	Result
1	Access to Updated Documentation	PASS
2	Process for Documentation Control	FAIL
3	Physical Access to the Server	PASS
4	Physical Safety Controls	PASS
5	Installation of a Solaris Hardening Package	PASS (with comments)
6	Tripwire Installation and Configuration	FAIL
7	Syslog Setup	PASS
8	Solaris Patch Updates	PASS (with comments)
9	Configuration of DS Access Controls	PASS
10	Password Strength	FAIL
11	DS Logging Setup	PASS
12	Replication Setup	PASS
13	Password Security Policy	PASS
14	Lockdown of DS-specific Directories	PASS
15	Data Backup Plan	PASS
16	Startup/Shutdown Scripts	PASS
17	Vulnerability Scans	PASS (with comments)

Of the 17 tests that were run, 14 of them passed the audit. Note that Tests #5, 8, and 17 are marked as “pass”, but the auditor took note of some issues that need to be addressed in order to ensure that problems can be avoided in the future.

Based on the auditor’s findings, the Sun ONE DS application has been properly configured to handle all user information that it contains while maintaining its internal security. The administrators have taken full advantage of the DS’s replication and logging capabilities, and they have implemented a backup and recovery plan in case a disaster occurs. However, there are a few issues with the security of the server on which the application is installed. No file traceability software has been installed on the server, and some additional work is needed to ensure that the server is more thoroughly hardened. Most of the

physical security issues have been addressed, but there are still a couple of places where this could be improved. Perhaps the biggest concern with this server is its documentation and the process by which it is controlled. While this may not have an immediate impact on the server, this could cost precious time and money over the long run.

Because of the cooperation of everyone involved, all of the original objectives of the audit were met. It is the auditor's opinion that the audit was a success.

5.2 Audit Findings and Recommendations

In this audit, we conducted a series of tests to determine what threats and vulnerabilities exist on a Sun ONE Directory Server. These threats and vulnerabilities can be broken down into four categories: documentation/training, physical security, Solaris security/system hardening, and application setup. After conducting the audit, we have generated our findings with regards to each of these categories. In the cases that didn't fully pass the audit, we will offer our recommendations for fixing the problem, and we will estimate the costs for implementing these fixes.

5.2.1 Documentation/Training

Positives

An organizational system for keeping track of all DS-related documentation is being implemented on the program, and the administrators proved that they are utilizing this system to its fullest, as described in Test #1. They also proved that they have a vast number of resources, including the vendor's web site and customer support, at their disposal.

Despite the fact that Test #2 failed, there were still some positives that came out of the test. A formal process, although flawed, is in place to document and administer changes to the DS servers, and there is a document control system in place for storing and maintaining all pertinent DS-related files.

Negatives

Test #2 proved that the formal process that is in place for approving, documenting, and implementing changes to the DS server does not have a single point of control, which can result in multiple potential failure points. The committee in charge of approving any changes does a good job of documenting all approvals, but they do not issue any formal tasks in order for the changes to be implemented. This responsibility is left up to the administrators, which could lead to a communication gap if no formal announcement is made about the approved changes.

If this process is allowed to continue, there is a risk of allowing discrepancies between the documentation and the implementation of the application. My recommendation is that the approval board, along with other management on the program, need to determine a plan for centralizing the tasking assignments for any approved changes. I estimate that the total time for this effort is 20 man-hours.

The files stored in the source controlled area and their respective documentation are out of sync with each other, possibly because of the issue listed above. The administrators need to take the time to perform a scrub of the documentation (or, in certain cases, create the documentation) to ensure consistency between the two. Failure to do so could result in inconsistencies in the system along with wasted time and effort. I estimate that this would take about 8 man-hours.

5.2.2 Physical Security

Positives

As shown in Tests #3 and #4, the physical security of the DS server is extremely good. Electronic and human controls are in place to ensure that the server remains safe, and the administrators showed that they were aware of the access procedures in place. The proper precautions have been taken to ensure that a variety of environmental dangers can be prevented and avoided.

Negatives

As mentioned in Test #4, a water sprinkler system is installed in case of a fire. While this may be effective, it may also cause physical damage to the DS server and the other servers in the storage room. The administrators may want to investigate the cost of installing a non-water-based fire extinguishing system. This effort should take about 2-4 hours. However, the size of the room in which the servers are stored may make it financially impossible to install such a system.

5.2.3 Solaris Security/System Hardening

Positives

The administrators did an excellent job of ensuring that the DS server is capturing all pertinent syslog information. The information shown in Test #7 proves that the logging processes are configured correctly, and the excerpts from the logs themselves are proof that the server passed this section of the audit. The patches on the system, as shown in Test #8 and Appendix B, have been updated recently. A Solaris hardening package has also been installed on the DS server, and the administrators configured the package to attempt to remove all unnecessary services and processes on the server. The output in

Appendix A shows that all of the appropriate “Finish” scripts were run in order to make the server as secure as possible.

Negatives

Test #6 was a failure because no file integrity software, such as Tripwire, is installed on the DS server. Utilizing a tool like Tripwire helps avoid the risk of not being able to trace the modification of important files on the server. My recommendation is that Tripwire be installed on this server, and the website www.tripwire.org can provide a template for the administrators to use. This effort should take about 2 hours.

Although the installation of JASS was a success for the most part, there are still a few services running on the server that could lead to potential exploits. According to Test #5, a couple of the services that were still running after the JASS installation were “automounter” and “sendmail”. None of the JASS “Finish” scripts attempted to disable the “automounter” process. Even though the “disable-sendmail” Finish script was run, the “sendmail” process started up when the server was rebooted. The administrators need to modify their JASS package to ensure that these processes are suppressed during the next JASS installation. The estimated time for this effort is 2-4 man-hours.

The vulnerability scan in Test #17 showed that a couple of ports that could lead to security exploits were open on the server. One of the open ports was TCP port 389 (the LDAP port). An investigation showed that this security hole is not specific to the Sun ONE Directory Server; however, the administrators need to ensure that the ACIs and the root password on the LDAP application are thoroughly hardened. They also need to run some of the tests listed in reference [18] to ensure that they are not revealing any sensitive information.

The second potential security hole was found on UDP port 32772. This port can lead to an exploit using RPC. Figure 5 shows that JASS did not successfully turn off the RPC services on the server. The administrators need to investigate this issue along with the other warnings that the Nessus scan revealed (see Appendix C). The total time to address all these issues should be 5-10 man-hours.

Test #8 showed that the patches had been updated recently; however, there is no well-defined system in place to ensure that the patch sets on the server are consistently updated. Since the server does not have direct access to Sun’s website, this will have to be a manual process, but a process should be in place nonetheless to ensure that the proper security patches are installed on the server. The estimated time to devise and document a plan should be 2-4 man-hours.

5.2.4 Application Setup

Positives

For the most part, the configuration of the DS application was carried out well. All of the DS-related logs are being captured and sent to the central log server on the network, as shown in Figures 14-17. An examination of the Access Control Instructions in Test #9 showed that the administrators and users have all necessary privileges and restrictions when it comes to accessing the LDAP information. Figures 31 and 32 show that the application is set up to enforce the company's password and account lockout policies, and Figure 33 proved that access to the DS installation directories is restricted authorized users only. Backup and recovery plans are in effect on the server, and these procedures are well documented. The information in Test #16 shows that no manual intervention is needed in terms of starting or stopping the DS-specific processes when the server is rebooted. Most importantly, the administrators are taking full advantage of the replication features offered by the DS application. The replication agreements have been set so that all information on the primary and secondary DS servers remain in sync with each other, and Figures 23-30 show that replication is working.

Negatives

The administrators have taken a huge risk by not using a strong password for the DS Administrator. Although password-cracking tools are not allowed on the internal side of the network, there is still a risk for data compromise by using an easy-to-guess password. Further investigation has shown that various groups on the network connect to the DS application using an encrypted form of the DS Administrator password. Although it may be inconvenient, this password needs to be strengthened. Total time for this effort should be no more than one hour.

Although there are procedures in place for data recovery, the administrators have admitted that they are unfamiliar with the procedures, and they have not attempted to practice them. The risk here is small, but valuable time can be lost if the administrators cannot restore the information in the DS application in a timely manner after a disaster. The administrators need to spend 1-2 hours reviewing this documentation and becoming more familiar with the procedures.

References

- [1] Anderson, Harry. "Introduction to Nessus." 1999-2005, SecurityFocus. URL: <http://www.securityfocus.com/infocus/1741>. (5 March 2005)
- [2] "Audit of Solaris 8 Platform." Azim Ferchichi, GSNA Practical, January 2002. URL: http://www.giac.org/certified_professionals/practicals/gsna/0035.php. (26 February 2005)
- [3] "Auditing Unix – Solaris." SANS Security Consensus Operational Readiness Evaluation (S.C.O.R.E.) URL: <http://www.sans.org/score/checklists/AuditingUnix.pdf>. (1 March 2005)
- [4] "Focus on Windows: Password Policies." 2005, About, Inc. URL: <http://windows.about.com/od/security//aa000910a.htm>. (6 March 2005)
- [5] Hayes, Bill. "Conducting a Security Audit: An Introductory Overview." 26 May 2003. URL: <http://www.securityfocus.com/printable/infocus/1697>. (27 February 2005)
- [6] Heare, Sean. "Data Center Physical Security Checklist." 1 December 2001. URL: <http://sans.org/rr/whitepapers/awareness/416.php>. (2 March 2005)
- [7] "High Technology Crime – Computer Forensics and Digital Evidence." 03 November 2004. URL: <http://www.tecrime.com/0secure.htm>. (28 February 2005)
- [8] Hoelzer, David. "Advanced System and Network Auditing." 2004, The SANS Institute. (26 February 2005)
- [9] Insecure.org. URL: <http://www.insecure.org>. (5 March 2005)
- [10] "iPlanet Directory Server Deployment Guide: How to Design the Schema." 2001, Sun Microsystems, Inc. URL: <http://docs.sun.com/source/816-5599-10/schema.htm>. (8 March 2005)
- [11] Nessus Open Source Vulnerability Scanner Project. 2004, Tenable Network Security™. URL: <http://www.nessus.org>. (5 March 2005)
- [12] "NetBackup™ Enterprise Server." 2005, VERITAS Software Corporation. URL: <http://www.veritas.com/Products/www?c=product&refId=2>. (9 March 2005)
- [13] Noodergraaf, Alex and Brunette, Glenn. "Auditing System Security." May 2003, Sun BluePrints™ OnLine. URL:

- <http://www.sun.com/blueprints/0503/817-2881.pdf>. (28 February 2005)
- [14] Noodergraaf, Alex and Watson, Keith. "Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology." December 1999, Sun BluePrints™ OnLine. URL: <http://www.sun.com/blueprints/1299/minimization.pdf>. (27 February 2005)
- [15] OpenLDAP: Community developed by LDAP software. 2005, OpenLDAP Foundation. URL: <http://www.openldap.org>. (1 March 2005)
- [16] "RU Secure: Security Checklist." 2003, Rutgers, The State University of New Jersey. URL: http://rusecure.rutgers.edu/sec_plan/checklist.php. (2 March 2005)
- [17] "Security Audit of a Network Associates Gauntlet 6.0 Firewall: An Auditor's Perspective." Ronald Jeppson, GSNA Practical, September 2002. URL: http://www.giac.org/certified_professionals/practicals/gsna/0056.php. (26 February 2005)
- [18] "Security Issues with LDAP Null Base Connections." 2005, Microsoft Corporation. URL: <http://support.microsoft.com/default.aspx?scid=kb;en-us;837964>. (16 March 2005)
- [19] "Secure Directory Solutions: A Nexor White Paper." November 2002, Nexor. URL: <http://www.nexor.com/media/whitepapers/directory%20solutions.pdf>. (1 March 2005)
- [20] "Server Management Guide: Sun™ ONE Server Console." June 2003. URL: <http://docs-pdf.sun.com/816-6704-10/816-6704-10.pdf>. (26 February 2005)
- [21] "Solaris Hardening Checklist." URL: <http://www.securitytribe.com/~roamer/whitepapers/checklist.doc>. (28 February 2005)
- [22] "Sourcefire Intrusion Detection System Deployment: An Auditor's Perspective." Don Weber, GSNA Practical, September 24, 2003. URL: http://www.giac.org/certified_professionals/practicals/gsna/0092.php. (26 February 2005)
- [23] "Sun Java System Directory Server 5.2." 1994-2005, Sun Microsystems. URL: http://www.sun.com/software/products/directory_srvr/home_directory.xml. (26 February 2005)

- [24] "Sun ONE Directory Server 5.2 Product Brief." 2003, Sun Microsystems, Inc. URL: <http://docs.sun.com/source/816-6733-10/index.html>. (26 February 2005)
- [25] "Sun ONE Directory Server v5.2 Reference Manual." 2003, Sun Microsystems, Inc. URL: <http://docs.sun.com/source/816-6699-10/contents.html>. (1 March 2005)
- [26] "Sun Product Documentation: bak2db.pl(1M)." January 2005, Sun Microsystems, Inc. URL: <http://docs.sun.com/app/docs/doc/817-7620/6mmu6mn9m?a=view>. (9 March 2005)
- [27] "Sun Product Documentation: db2bak.pl(1M)." January 2005, Sun Microsystems, Inc. URL: <http://docs.sun.com/app/docs/doc/817-7620/6mmu6mn9r?a=view>. (9 March 2005)
- [28] "Sun™ Patch Check, Version 1.2." 2005, Sun Microsystems, Inc. URL: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk>. (15 March 2005)
- [29] Tripwire.org – Home of the Tripwire Open Source Project. URL: <http://www.tripwire.org>. (5 March 2005)
- [30] "UNIX Security Checklist v2.0." 2001, AusCERT. URL: http://www.cert.org/tech_tips/usc20_full.html, (1 March 2005)
- [31] "VA Security Standard Compliance Checklist." 2005, Virginia Alliance for Secure Computing and Networking (VA SCAN). URL: http://www.vascan.org/checklist/physical_security_check.html. (1 March 2005)

Appendix A

This appendix contains file information that is pertinent to Test #5 located in Section 3.5 of this paper.

gsna-be-ldap2.SOL.20050312

```
=====
=====
SOLsecure.driver: Driver started.
=====
=====
```

```
=====
=====
Toolkit Version: 4.0.2
Node name:      gsna-be-ldap2.gsna.com
Host ID:        80c68f48
Host address:   10.10.10.150
MAC address:    8:0:20:c6:8f:48
OS version:     5.9
Date:          Sat Mar 12 02:23:44 GMT 2005
=====
=====
```

```
=====
=====
SOLsecure.driver: Finish script: install-templates.fin
=====
=====
```

Copying personalized files (templates).

```
[NOTE] Copying /.cshrc from /opt/jass/Files/.cshrc.
[NOTE] Copying /.profile from /opt/jass/Files/.profile.
```

```
=====
=====
SOLsecure.driver: Finish script: set-root-password.fin
=====
=====
```

Setting the password for the "root" account.

```
[NOTE] The system is not booted from mini-root, no changes made.
```

```
=====
=====
SOLsecure.driver: Finish script: set-term-type.fin
=====
=====
```

Setting the default terminal type to 'vt100'.

[NOTE] Copying /etc/profile to /etc/profile.JASS.20050312022413

Adding "TERM=vt100" to /etc/profile.

[NOTE] Copying /etc/.login to /etc/.login.JASS.20050312022413

Adding "setenv TERM vt100" to /etc/.login.

```
=====
=====
SQLsecure.driver: Driver finished.
=====
=====
```

```
=====
=====
SQLsecure.driver: Driver started.
=====
=====
```

```
=====
=====
Toolkit Version: 4.0.2
Node name:      gsna-be-ldap2.gsna.com
Host ID:       80c68f48
Host address:  10.10.10.150
MAC address:   8:0:20:c6:8f:48
OS version:    5.9
Date:         Sat Mar 12 02:24:15 GMT 2005
=====
=====
```

```
=====
=====
SQLsecure.driver: Finish script: install-templates.fin
=====
=====
```

Copying personalized files (templates).

[NOTE] Creating a new directory, /etc/dt.
[NOTE] Creating a new directory, /etc/dt/config.
[NOTE] Copying /etc/dt/config/Xaccess from
/opt/jass/Files/etc/dt/config/Xaccess.
[NOTE] Copying /etc/init.d/set-tmp-permissions from
/opt/jass/Files/etc/init.d/set-tmp-permissions.
[NOTE] Copying /etc/issue from /opt/jass/Files/etc/issue.
[NOTE] Copying /etc/motd to /etc/motd.JASS.20050312022421
[NOTE] Copying /etc/motd from /opt/jass/Files/etc/motd.
[NOTE] Copying /etc/notrouter from /opt/jass/Files/etc/notrouter.
[NOTE] Linking /etc/rc2.d/S00set-tmp-permissions from

```
/opt/jass/Files/etc/rc2.d/S00set-tmp-permissions.  
[NOTE] Linking /etc/rc2.d/S07set-tmp-permissions from  
/opt/jass/Files/etc/rc2.d/S07set-tmp-permissions.  
[NOTE] Copying /etc/security/audit_class to  
/etc/security/audit_class.JASS.20050312022425  
[NOTE] Copying /etc/security/audit_class from  
/opt/jass/Files/etc/security/audit_class.  
[NOTE] Copying /etc/security/audit_control to  
/etc/security/audit_control.JASS.20050312022426  
[NOTE] Copying /etc/security/audit_control from  
/opt/jass/Files/etc/security/audit_control.  
[NOTE] Copying /etc/security/audit_event to  
/etc/security/audit_event.JASS.20050312022427  
[NOTE] Copying /etc/security/audit_event from  
/opt/jass/Files/etc/security/audit_event.  
[NOTE] Copying /etc/security/audit_startup from  
/opt/jass/Files/etc/security/audit_startup.  
[NOTE] Copying /etc/security/audit_user to  
/etc/security/audit_user.JASS.20050312022428  
[NOTE] Copying /etc/security/audit_user from  
/opt/jass/Files/etc/security/audit_user.  
[NOTE] Copying /etc/snmp/conf/snmpd.conf to  
/etc/snmp/conf/snmpd.conf.JASS.20050312022429  
[NOTE] Copying /etc/snmp/conf/snmpd.conf from  
/opt/jass/Files/etc/snmp/conf/snmpd.conf.
```

```
=====  
=====
```

SOLsecure.driver: Finish script: disable-apache.fin

```
=====  
=====
```

Disabling the service: Apache

```
=====  
=====
```

SOLsecure.driver: Finish script: disable-asppp.fin

```
=====  
=====
```

Disabling the service: Asynchronous Point-to-Point Protocol (ASPPP)

[NOTE] This script is only applicable for Solaris version 5.5.1-5.8.

```
=====  
=====
```

SOLsecure.driver: Finish script: disable-autoinst.fin

```
=====  
=====
```

Disabling the function: Automatic system reconfiguration

[WARN] This script will prevent the successful use of the 'sys-unconfig'
program to restore a system's configuration to an 'as-manufactured'
state.

[NOTE] Renaming /etc/rc2.d/S30sysid.net to
/etc/rc2.d/_S30sysid.net.JASS.20050312022434
[NOTE] Renaming /etc/rc2.d/S71sysid.sys to
/etc/rc2.d/_S71sysid.sys.JASS.20050312022435
[NOTE] Renaming /etc/rc2.d/S72autoinstall to
/etc/rc2.d/_S72autoinstall.JASS.20050312022435

=====
=====

```
SOLsecure.driver: Finish script: disable-cachedaemons.fin
```

=====
=====

Disabling the cachedaemon service.
[NOTE] Renaming /etc/rcS.d/S35cacheos.sh to
/etc/rcS.d/_S35cacheos.sh.JASS.20050312022436
[NOTE] Renaming /etc/rc2.d/S73cachefs.daemon to
/etc/rc2.d/_S73cachefs.daemon.JASS.20050312022437
[NOTE] Renaming /etc/rc2.d/S93cacheos.finish to
/etc/rc2.d/_S93cacheos.finish.JASS.20050312022437

=====
=====

```
SOLsecure.driver: Finish script: disable-devfsadm.fin
```

=====
=====

Disabling the devfsadm service.
[NOTE] Renaming /etc/rc0.d/K83devfsadm to
/etc/rc0.d/_K83devfsadm.JASS.20050312022438
[NOTE] Renaming /etc/rcS.d/S50devfsadm to
/etc/rcS.d/_S50devfsadm.JASS.20050312022438

=====
=====

```
SOLsecure.driver: Finish script: disable-dhcpd.fin
```

=====
=====

Disabling the service: Dynamic Host Configuration Protocol (DHCP)

[NOTE] This script only prevents a system from being a DHCP server.
DHCP
client services are not impacted by this script.

=====
=====

```
SOLsecure.driver: Finish script: disable-dmi.fin
```

=====
=====

Disabling the service: Desktop Management Interface (DMI)

[NOTE] Renaming /etc/dmi/conf/dmispd.conf to
/etc/dmi/conf/_dmispd.conf.JASS.20050312022440
[NOTE] Renaming /etc/dmi/conf/snmpXdmid.conf to
/etc/dmi/conf/_snmpXdmid.conf.JASS.20050312022440

[NOTE] Renaming /etc/dmi/ciagent/ciinvoke to
/etc/dmi/ciagent/_ciinvoke.JASS.20050312022441

```
=====
=====
SOLsecure.driver: Finish script: disable-dtlogin.fin
=====
=====
```

Disabling the service: Common Desktop Environment (CDE)

done
desktop auto-start disabled.

```
=====
=====
SOLsecure.driver: Finish script: disable-lp.fin
=====
=====
```

Disabling the service: Line printer (LP)

[NOTE] Renaming /etc/rcS.d/K39lp to
/etc/rcS.d/_K39lp.JASS.20050312022442
[NOTE] Renaming /etc/rc0.d/K39lp to
/etc/rc0.d/_K39lp.JASS.20050312022442
[NOTE] Renaming /etc/rc1.d/K39lp to
/etc/rc1.d/_K39lp.JASS.20050312022443
[NOTE] Renaming /etc/rc2.d/S80lp to
/etc/rc2.d/_S80lp.JASS.20050312022444

[NOTE] Copying /etc/cron.d/cron.deny to
/etc/cron.d/cron.deny.JASS.20050312022444

Adding the "lp" account to /etc/cron.d/cron.deny.

Disabling the "lp" user crontab entry.

[NOTE] Creating backup directory, /var/spool/cron/crontabs.JASS
[NOTE] Creating a new directory, /var/spool/cron/crontabs.JASS.
[NOTE] Moving /var/spool/cron/crontabs/lp to
/var/spool/cron/crontabs.JASS/lp.JASS.20050312022445

```
=====
=====
SOLsecure.driver: Finish script: disable-nfs-server.fin
=====
=====
```

Disabling the service: Networked File System (NFS) Server

[NOTE] Renaming /etc/rcS.d/K28nfs.server to
/etc/rcS.d/_K28nfs.server.JASS.20050312022446
[NOTE] Renaming /etc/rc0.d/K28nfs.server to
/etc/rc0.d/_K28nfs.server.JASS.20050312022447
[NOTE] Renaming /etc/rc1.d/K28nfs.server to
/etc/rc1.d/_K28nfs.server.JASS.20050312022447
[NOTE] Renaming /etc/rc2.d/K28nfs.server to

```

/etc/rc2.d/_K28nfs.server.JASS.20050312022448
[NOTE] Renaming /etc/rc3.d/S15nfs.server to
/etc/rc3.d/_S15nfs.server.JASS.20050312022448

=====
=====
SOLsecure.driver: Finish script: disable-nscd-caching.fin
=====
=====

Disabling the function: Name Service Cache Daemon (NSCD)

Changing the positive-time-to-live and negative-time-to-live entries
to "0" for the "passwd", "group", "hosts" and "ipnodes" entries
in /etc/nscd.conf.

[NOTE] Copying /etc/nscd.conf to /etc/nscd.conf.JASS.20050312022449

=====
=====
SOLsecure.driver: Finish script: disable-preserve.fin
=====
=====

Disabling the function: Preserve Edited Files (PRESERVE)

[NOTE] Renaming /etc/rc2.d/S89PRESERVE to
/etc/rc2.d/_S89PRESERVE.JASS.20050312022450

=====
=====
SOLsecure.driver: Finish script: disable-remote-root-login.fin
=====
=====

Disabling the function: Direct, remote login as the "root" account

[NOTE] Copying /etc/default/login to
/etc/default/login.JASS.20050312022451

Setting the "CONSOLE" parameter in /etc/default/login.

=====
=====
SOLsecure.driver: Finish script: disable-rhosts.fin
=====
=====

Disabling the function: "rhosts" Authentication

[NOTE] Copying /etc/pam.conf to /etc/pam.conf.JASS.20050312022452

Commenting the "pam_rhosts_auth" entries in /etc/pam.conf.

=====
=====
SOLsecure.driver: Finish script: disable-sendmail.fin

```



```

=====
=====

Disabling the service: sendmail (for mail receipt)

[NOTE] Copying /etc/mail/sendmail.cf to
/etc/mail/sendmail.cf.JASS.20050312022454
[NOTE] Copying /etc/mail/sendmail.cf from
local.JASS.20050312022453.cf.

=====
=====

SOLsecure.driver: Finish script: disable-snmpp.fin
=====
=====

Disabling the service: Simple Network Management Protocol (SNMP)

[NOTE] Renaming /etc/snmp/conf/snmpdx.rsrc to
/etc/snmp/conf/_snmpdx.rsrc.JASS.20050312022456

=====
=====

SOLsecure.driver: Finish script: disable-spc.fin
=====
=====

Disabling the service: SunSoft Print Service (SPC)

[NOTE] Renaming /etc/rcS.d/K39spc to
/etc/rcS.d/_K39spc.JASS.20050312022456
[NOTE] Renaming /etc/rc0.d/K39spc to
/etc/rc0.d/_K39spc.JASS.20050312022457
[NOTE] Renaming /etc/rc1.d/K39spc to
/etc/rc1.d/_K39spc.JASS.20050312022457
[NOTE] Renaming /etc/rc2.d/S80spc to
/etc/rc2.d/_S80spc.JASS.20050312022458

=====
=====

SOLsecure.driver: Finish script: disable-syslogd-listen.fin
=====
=====

Disabling the function: SYSLOG (for external log receipt)

[NOTE] Preventing the SYSLOG service from logging remote connections.
[NOTE] The service will no longer accept log messages from other
systems.

[NOTE] Copying /etc/default/syslogd to
/etc/default/syslogd.JASS.20050312022459

Setting the "LOG_FROM_REMOTE" parameter to "NO" in
/etc/default/syslogd.

=====
=====

```

```

SOLsecure.driver: Finish script: disable-uucp.fin
=====
=====

Disabling the service: Unix-to-Unix Copy (UUCP)

=====
=====
SOLsecure.driver: Finish script: disable-vold.fin
=====
=====

Disabling the service: Volume Management (VOLD)

[NOTE] Renaming /etc/vold.conf to /etc/_vold.conf.JASS.20050312022500

=====
=====
SOLsecure.driver: Finish script: disable-xntpd.fin
=====
=====

Disabling the xntpd service.
[NOTE] Renaming /etc/rc0.d/K40xntpd to
/etc/rc0.d/_K40xntpd.JASS.20050312022502
[NOTE] Renaming /etc/rc1.d/K40xntpd to
/etc/rc1.d/_K40xntpd.JASS.20050312022502
[NOTE] Renaming /etc/rcS.d/K40xntpd to
/etc/rcS.d/_K40xntpd.JASS.20050312022503
[NOTE] Renaming /etc/rc2.d/S74xntpd to
/etc/rc2.d/_S74xntpd.JASS.20050312022503

=====
=====
SOLsecure.driver: Finish script: install-shells.fin
=====
=====

Defining valid shells for this system.

[NOTE] Creating a new file, /etc/shells.

[NOTE] Copying /etc/shells to /etc/shells.JASS.20050312022505

Adding /bin/csh to /etc/shells.
Adding /bin/false to /etc/shells.
Adding /bin/jsh to /etc/shells.
Adding /bin/ksh to /etc/shells.
Adding /bin/sh to /etc/shells.
[NOTE] File /bin/tcsh was not found.
Adding /sbin/jsh to /etc/shells.
[NOTE] File /sbin/noshell was not found.
Adding /sbin/sh to /etc/shells.
Adding /usr/bin/csh to /etc/shells.
Adding /usr/bin/jsh to /etc/shells.
Adding /usr/bin/ksh to /etc/shells.
Adding /usr/bin/sh to /etc/shells.

```

```
=====
=====
SOLsecure.driver: Finish script: set-rmmount-nosuid.fin
=====
=====
```

Preventing remove media types from being mounted set-uid.

```
=====
=====
SOLsecure.driver: Finish script: set-system-umask.fin
=====
=====
```

Setting system-wide default file creation mask.

```
=====
=====
SOLsecure.driver: Finish script: update-inetd-conf.fin
=====
=====
```

Updating status of network services in /etc/inet/inetd.conf.

Disabling those services listed in JASS_SVCS_DISABLE.

[NOTE] Copying /etc/inet/inetd.conf to
/etc/inet/inetd.conf.JASS.20050312022509

Disabling service, 100068/2-5 (/usr/dt/bin/rpc.cmsd).
Disabling service, 100083/1 (/usr/dt/bin/rpc.ttdbserverd).
Disabling service, 100134/1 (/usr/lib/krb5/ktkt_warnd).
Disabling service, 100150/1 (/usr/sbin/ocfserve).
Disabling service, 100155/1 (/usr/lib/smedia/rpc.smsserverd).
Disabling service, 100221/1 (/usr/openwin/bin/kcms_server).
Disabling service, 100229/1-2 (/usr/sbin/rpc.metad).
Disabling service, 100230/1 (/usr/sbin/rpc.metamhd).
Disabling service, 100232/10 (/usr/sbin/sadmind).
Disabling service, 100234/1 (/usr/lib/gss/gssd).
Disabling service, 100235/1 (/usr/lib/fs/cachefs/cachefs).
Disabling service, 100242/1 (/usr/sbin/rpc.metamedd).
Disabling service, chargen (internal).
Disabling service, comsat (/usr/sbin/in.comsat).
Disabling service, daytime (internal).
Disabling service, discard (internal).
Disabling service, dtspc (/usr/dt/bin/dtspcd).
Disabling service, echo (internal).
Disabling service, exec (/usr/sbin/in.rexecd).
Disabling service, finger (/usr/sbin/in.fingerd).
Disabling service, fs (/usr/openwin/lib/fs.auto).
Disabling service, login (/usr/sbin/in.rlogind).
Disabling service, name (/usr/sbin/in.tnamed).
Disabling service, printer (/usr/lib/print/in.lpd).
Disabling service, rquotad/1 (/usr/lib/nfs/rquotad).
Disabling service, rstatd/2-4 (/usr/lib/netsvc/rstat/rpc.rstatd).

```
Disabling service, rusersd/2-3 (/usr/lib/netshvc/rusers/rpc.rusersd).
Disabling service, sprayd/1 (/usr/lib/netshvc/spray/rpc.sprayd).
Disabling service, talk (/usr/sbin/in.talkd).
Disabling service, time (internal).
Disabling service, walld/1 (/usr/lib/netshvc/rwall/rpc.rwalld).
```

Enabling those services listed in JASS_SVCS_ENABLE.

```
=====
=====
SOLsecure.driver: Finish script: install-fix-modes.fin
=====
=====
```

Installing Software: fix-modes

[NOTE] The installation directory, /opt/SUNWbefm, does not exist.

```
=====
=====
SOLsecure.driver: Driver finished.
=====
=====
```

/etc/inetd.conf

```
#ident      "@(#)inetd.conf  1.51  02/11/19 SMI"
#
# Copyright 1989-2002 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#
# Configuration file for inetd(1M).  See inetd.conf(4).
#
# To re-configure the running inetd process, edit this file, then
# send the inetd process a SIGHUP.
#
# Syntax for socket-based Internet services:
#  <service_name> <socket_type> <proto> <flags> <user>
#  <server_pathname> <args>
#
# Syntax for TLI-based Internet services:
#
#  <service_name> tli <proto> <flags> <user> <server_pathname> <args>
#
# IPv6 and inetd.conf
# By specifying a <proto> value of tcp6 or udp6 for a service, inetd
# will
# pass the given daemon an AF_INET6 socket.  The following daemons
# have
```

```

# been modified to be able to accept AF_INET6 sockets
#
#      ftp telnet shell login exec tftp finger printer
#
# and service connection requests coming from either IPv4 or IPv6-
based
# transports. Such modified services do not normally require
separate
# configuration lines for tcp or udp. For documentation on how to do
this
# for other services, see the Solaris System Administration Guide.
#
# You must verify that a service supports IPv6 before specifying
<proto> as
# tcp6 or udp6. Also, all inetd built-in commands (time, echo,
discard,
# daytime, chargen) require the specification of <proto> as tcp6 or
udp6
#
# The remote shell server (shell) and the remote execution server
# (exec) must have an entry for both the "tcp" and "tcp6" <proto>
values.
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers." Many sites choose to
disable
# some or all of these services to improve security.
#
#systat      stream      tcp  nowait      root  /usr/bin/ps      ps -
ef
#netstat     stream      tcp  nowait      root  /usr/bin/netstat
netstat -f inet
#
# Time service is used for clock synchronization.
#
# time       stream      tcp6 nowait      root  internal
# time       dgram udp6  wait  root  internal
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
# echo       stream      tcp6 nowait      root  internal
# echo       dgram udp6  wait  root  internal
# discard    stream      tcp6 nowait      root  internal
# discard    dgram udp6  wait  root  internal
# daytime    stream      tcp6 nowait      root  internal
# daytime    dgram udp6  wait  root  internal
# chargen    stream      tcp6 nowait      root  internal
# chargen    dgram udp6  wait  root  internal
#
#
# RPC services syntax:
# <rpc_prog>/<vers> <endpoint-type> rpc/<proto> <flags> <user> \
# <pathname> <args>
#
# <endpoint-type> can be either "tli" or "stream" or "dgram".
# For "stream" and "dgram" assume that the endpoint is a socket
descriptor.
# <proto> can be either a nettype or a netid or a "*". The value is

```

```

# first treated as a nettype. If it is not a valid nettype then it is
# treated as a netid. The "*" is a short-hand way of saying all the
# transports supported by this system, ie. it equates to the
"visible"
# nettype. The syntax for <proto> is:
#      *|<nettype|netid>|<nettype|netid>{[,<nettype|netid>]}
# For example:
# dummy/1 tli rpc/circuit_v,udpwait root /tmp/test_svc
# test_svc
#
# Solstice system and network administration class agent server
# 100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind
#
# rpc.cmsd is a data base daemon which manages calendar data backed
# by files in /var/spool/calendar
#
#
# Sun ToolTalk Database Server
#
# 100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd
rpc.ttdbserverd
#
# Sun KCMS Profile Server
#
# 100221/1 tli rpc/tcp wait root /usr/openwin/bin/kcms_server
kcms_server
#
# Sun Font Server
#
# fs stream tcp6 wait nobody /usr/openwin/lib/fs.auto
fs
#
# CacheFS Daemon
#
# 100235/1 tli rpc/ticotsord wait root /usr/lib/fs/cachefs/cachefsd
cachefsd
# OCFSESV - OCF (Smart card) Daemon
# 100150/1 tli rpc/ticotsord wait root /usr/sbin/ocfserv
ocfserv
# dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
# 100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
# METAD - SLVM metadb Daemon
# 100229/1-2 tli rpc/tcp wait root /usr/sbin/rpc.metad
rpc.metad
# METAMHD - SLVM HA Daemon
# 100230/1 tli rpc/tcp wait root /usr/sbin/rpc.metamhd
rpc.metamhd
# METAMEDD - SLVM Mediator Daemon
# 100242/1 tli rpc/tcp wait root /usr/sbin/rpc.metamedd
rpc.metamedd
# LPD - Print Protocol Adaptor (BSD listener)
# printer stream tcp6 nowait root /usr/lib/print/in.lpd
in.lpd
# RSHD - rsh daemon (BSD protocols)
# shell stream tcp nowait root /usr/sbin/in.rshd
in.rshd
# shell stream tcp6 nowait root /usr/sbin/in.rshd
in.rshd

```

```

# RLOGIND - rlogin daemon (BSD protocols)
# login      stream      tcp6  nowait      root  /usr/sbin/in.rlogind
           in.rlogind
# REXECD - rexec daemon (BSD protocols)
# exec       stream      tcp   nowait      root  /usr/sbin/in.rexecd
           in.rexecd
# exec       stream      tcp6  nowait      root  /usr/sbin/in.rexecd
           in.rexecd
# COMSATD - comsat daemon (BSD protocols)
# comsat     dgram udp    wait  root  /usr/sbin/in.comsat  in.comsat
# TALKD - talk daemon (BSD protocols)
# talk       dgram udp    wait  root  /usr/sbin/in.talkd   in.talkd
# FINGERD - finger daemon
# finger     stream      tcp6  nowait      nobody
           /usr/sbin/in.fingerd  in.fingerd
# RSTATD - rstat daemon
# rstatd/2-4 tli    rpc/datagram_v  wait  root
           /usr/lib/netsvc/rstat/rpc.rstatd  rpc.rstatd
# RUSERSD - rusers daemon (gives out user information)
# rusersd/2-3 tli    rpc/datagram_v,circuit_v  wait  root
           /usr/lib/netsvc/rusers/rpc.rusersd  rpc.rusersd
# RWALLD - rwall daemon (allows others to post messages to users)
# walld/1 tli    rpc/datagram_v  wait  root
           /usr/lib/netsvc/rwall/rpc.rwalld  rpc.rwalld
# SPRAYD - spray daemon (used for testing)
# sprayd/1 tli    rpc/datagram_v  wait  root
           /usr/lib/netsvc/spray/rpc.sprayd  rpc.sprayd
# GSSD - GSS Daemon
# 100234/1 tli    rpc/ticotsord  wait  root  /usr/lib/gss/gssd  gssd
# TFTPd - tftp server (primarily used for booting)
#tftpd dgram udp6  wait  root  /usr/sbin/in.tftpd  in.tftpd -s
/tftpdboot
# TNAMED - tname server (it is an obsolete IEN-116 name server
protocol)
# name       dgram udp    wait  root  /usr/sbin/in.tnamed  in.tnamed
# TELNETD - telnet server daemon
# telnet     stream      tcp6  nowait      root  /usr/sbin/in.telnetd
           in.telnetd
# smserverd to support removable media devices
# 100155/1 tli    rpc/ticotsord  wait  root
           /usr/lib/smedia/rpc.smserverd  rpc.smserverd
# REXD - rexd server provides only minimal authentication
#rexnd/1 tli    rpc/tcp  wait  root  /usr/sbin/rpc.rexd  rpc.rexd
# KTKT_WARND - Kerberos V5 Warning Messages Daemon
# 100134/1 tli    rpc/ticotsord  wait  root
           /usr/lib/krb5/ktkt_warnd  ktkt_warnd
# RQUOTAD - rquotad server supports UFS disk quotas for NFS clients
# rquotad/1 tli    rpc/datagram_v  wait  root  /usr/lib/nfs/rquotad
rquotad
# MDMN_COMMD - SVM Multi Node Communication Daemon
# 100422/1 tli    rpc/tcp  wait  root  /usr/sbin/rpc.mdcommd
rpc.mdcommd
bpcd stream      tcp  nowait      root
           /usr/opencv/netbackup/bin/bpcd  bpcd
vnetd stream      tcp  nowait      root  /usr/opencv/bin/vnetd  vnetd
voiped stream      tcp  nowait      root  /usr/opencv/bin/voiped
           voiped
bpjava-msvc stream      tcp  nowait      root

```

/usr/opensv/netbackup/bin/bpjava-msvc bpjava-msvc

/etc/system

```
*ident      "@(#)system 1.18  97/06/27 SMI" /* SVR4 1.5 */
*
*  SYSTEM SPECIFICATION FILE
*
* moddir:
*
*   Set the search path for modules.  This has a format similar to
the
*   csh path variable.  If the module isn't found in the first
directory
*   it tries the second and so on.  The default is /kernel
/usr/kernel
*
*   Example:
*       moddir: /kernel /usr/kernel /other/modules
*
* root device and root filesystem configuration:
*
*   The following may be used to override the defaults provided by
the boot program:
*
*   rootfs:          Set the filesystem type of the root.
*
*   rootdev:         Set the root device.  This should be a fully
expanded physical pathname.  The default is the
physical pathname of the device where the boot
program resides.  The physical pathname is
highly platform and configuration dependent.
*
*   Example:
*       rootfs:ufs
*       rootdev:/sbus@1,f8000000/esp@0,800000/sd@3,0:a
*
*   (Swap device configuration should be specified in /etc/vfstab.)
*
* exclude:
*
*   Modules appearing in the moddir path which are NOT to be
loaded,
*   even if referenced.  Note that `exclude' accepts either a module
name,
*   or a filename which includes the directory.
*
*   Examples:
*       exclude: win
```



```

*          exclude: sys/shmsys

* forceload:
*
*      Cause these modules to be loaded at boot time, (just before
mounting
*      the root filesystem) rather than at first reference. Note that
*      forceload expects a filename which includes the directory. Also
*      note that loading a module does not necessarily imply that it
will
*      be installed.
*
*      Example:
*          forceload: drv/foo

* set:
*
*      Set an integer variable in the kernel or a module to a new
value.
*      This facility should be used with caution. See system(4).
*
*      Examples:
*
*      To set variables in 'unix':
*
*          set nautopush=32
*          set maxusers=40
*
*      To set a variable named 'debug' in the module named
'test_module'
*
*          set test_module:debug = 0x13

```

/etc/services

```

#ident      "@(#)services      1.32  01/11/21 SMI"
#
#
# Copyright (c) 1999-2001 by Sun Microsystems, Inc.
# All rights reserved.
#
# Network services, Internet style
#
tcpmux      1/tcp
echo        7/tcp
echo        7/udp
discard     9/tcp      sink null
discard     9/udp      sink null
systat      11/tcp      users

```

```

daytime          13/tcp
daytime          13/udp
netstat          15/tcp
chargen          19/tcp          ttytst source
chargen          19/udp          ttytst source
ftp-data         20/tcp
ftp              21/tcp
ssh              22/tcp          # Secure Shell
telnet           23/tcp
smtp             25/tcp          mail
time             37/tcp          timserver
time             37/udp          timserver
name             42/udp          nameserver
whois            43/tcp          nicname          # usually to sri-nic
domain           53/udp
domain           53/tcp
bootps           67/udp          # BOOTP/DHCP server
bootpc           68/udp          # BOOTP/DHCP client
kerberos         88/udp          kdc              # Kerberos V5 KDC
kerberos         88/tcp          kdc              # Kerberos V5 KDC
hostnames        101/tcp          hostname          # usually to sri-nic
pop2             109/tcp          pop-2            # Post Office Protocol - V2
pop3             110/tcp          # Post Office Protocol -
Version 3
sunrpc           111/udp          rpcbind
sunrpc           111/tcp          rpcbind
imap             143/tcp          imap2            # Internet Mail Access
Protocol v2
ldap             389/tcp          # Lightweight Directory
Access Protocol
ldap             389/udp          # Lightweight Directory
Access Protocol
submission       587/tcp          # Mail Message Submission
submission       587/udp          # see RFC 2476
ldaps            636/tcp          # LDAP protocol over TLS/SSL
(was sldap)
ldaps            636/udp          # LDAP protocol over TLS/SSL
(was sldap)
#
# Host specific functions
#
tftp             69/udp
rje              77/tcp
finger          79/tcp
link            87/tcp          ttylink
supdup           95/tcp
iso-tsap         102/tcp
x400             103/tcp          # ISO Mail
x400-snd         104/tcp
csnet-ns         105/tcp
pop-2           109/tcp          # Post Office
uucp-path        117/tcp
nntp             119/tcp          usenet           # Network News Transfer
ntp              123/tcp          # Network Time Protocol
ntp              123/udp          # Network Time Protocol
netbios-ns       137/tcp          # NETBIOS Name Service
netbios-ns       137/udp          # NETBIOS Name Service
netbios-dgm      138/tcp          # NETBIOS Datagram Service

```

```

netbios-dgm 138/udp          # NETBIOS Datagram Service
netbios-ssn 139/tcp          # NETBIOS Session Service
netbios-ssn 139/udp          # NETBIOS Session Service
NeWS          144/tcp          news          # Window System
slp           427/tcp          slp           # Service Location Protocol,
V2
slp           427/udp          slp           # Service Location
Protocol, V2
mobile-ip     434/udp          mobile-ip     # Mobile-IP
cvc_hostd     442/tcp          # Network Console
ike           500/udp          ike          # Internet Key Exchange
uuidgen       697/tcp          # UUID Generator
uuidgen       697/udp          # UUID Generator
#
# UNIX specific services
#
# these are NOT officially assigned
#
exec           512/tcp
login          513/tcp
shell         514/tcp          cmd           # no passwords used
printer       515/tcp          spooler       # line printer
spooler
courier        530/tcp          rpc           # experimental
uucp          540/tcp          uucpd         # uucp daemon
biff          512/udp          comsat
who           513/udp          whod
syslog        514/udp
talk          517/udp
route         520/udp          router routed
ripng         521/udp
klogin        543/tcp          # Kerberos
authenticated rlogin
kshell        544/tcp          cmd           # Kerberos
authenticated remote shell
new-rwho      550/udp          new-who       # experimental
rmonitor      560/udp          rmonitord     # experimental
monitor       561/udp          # experimental
pcserver      600/tcp          # ECD Integrated PC board
srvr
sun-dr        665/tcp          # Remote Dynamic
Reconfiguration
kerberos-adm  749/tcp          # Kerberos V5
Administration
kerberos-adm  749/udp          # Kerberos V5
Administration
kerberos-iv   750/udp          # Kerberos V4 key server
krb5_prop     754/tcp          # Kerberos V5 KDC
propagation
ufsd          1008/tcp          ufsd          # UFS-aware server
ufsd          1008/udp          ufsd
cvc           1495/tcp          # Network Console
ingreslock    1524/tcp
www-ldap-gw   1760/tcp          # HTTP to LDAP gateway
www-ldap-gw   1760/udp          # HTTP to LDAP gateway
listen        2766/tcp          # System V listener
port
nfsd          2049/udp          nfs           # NFS server daemon (clts)

```

```
nfsd      2049/tcp    nfs      # NFS server daemon (cots)
eklogin   2105/tcp      # Kerberos encrypted rlogin
lockd     4045/udp     # NFS lock daemon/manager
lockd     4045/tcp
dtspc     6112/tcp    # CDE subprocess control
fs        7100/tcp    # Font server
#
# NetBackup services
#
bprd      13720/tcp    bprd
bpjava-msvc 13722/tcp  bpjava-msvc
bpcd      13782/tcp    bpcd
vnetd     13724/tcp    vnetd
voiped    13783/tcp    voiped
```

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix B

The following table is the information that was captured using the Sun Patch Check v1.2 utility (for Test #8).

Patch ID	Current Revision	Latest Revision	Synopsis
111711	12	CURRENT	SunOS 5.9: 32-bit Shared library patch for C++
111712	12	CURRENT	SunOS 5.9: 64-Bit Shared library patch for C++
112233	12	CURRENT	SunOS 5.9: Kernel Patch
112617	02	CURRENT	CDE 1.5: rpc.cmsd patch
112661	06	CURRENT	SunOS 5.9: IIIM and X Input & Output Method patch
112764	07	CURRENT	SunOS 5.9: Sun Quad FastEthernet qfe driver
112785	46	CURRENT	X11 6.6.1: Xsun patch
112807	13	CURRENT	CDE 1.5: dtlogin patch
112808	06	CURRENT	CDE1.5: Tooltalk patch
112810	06	CURRENT	CDE 1.5: dtmail patch
112817	23	CURRENT	SunOS 5.9: Sun GigaSwift Ethernet 1.0 driver patch
<input type="checkbox"/> 112834	04	06	SunOS 5.9: patch scsi
112874	31	CURRENT	SunOS 5.9: lgroup API libc Patch
112875	01	CURRENT	SunOS 5.9: patch /usr/lib/netsvc/rwall/rpc.rwalld
112907	03	CURRENT	SunOS 5.9: libgss Patch
112908	17	CURRENT	SunOS 5.9: krb5 shared object patch
112911	13	CURRENT	SunOS 5.9: ifconfig Patch
112912	01	CURRENT	SunOS 5.9: libinetcfg Patch
112921	06	CURRENT	SunOS 5.9: libkadm5 Patch
112922	02	CURRENT	SunOS 5.9: krb5 lib Patch
112923	03	CURRENT	SunOS 5.9: krb5 usr/lib Patch
112925	05	CURRENT	SunOS 5.9: ktutil kdb5_util kadmin kadmin.local kadmind Patch
112926	06	CURRENT	SunOS 5.9: smartcard Patch
112945	31	CURRENT	SunOS 5.9: wbem Patch
112951	10	CURRENT	SunOS 5.9: patchadd and patchrm Patch
112954	10	CURRENT	SunOS 5.9: uata Driver Patch
<input type="checkbox"/> 112960	22	24	SunOS 5.9: patch libsldap ldap_cachemgr libldap
112963	18	CURRENT	SunOS 5.9: linker patch
<input type="checkbox"/> 112964	09	11	SunOS 5.9: /usr/bin/ksh Patch
112965	04	CURRENT	SunOS 5.9: patch /kernel/drv/sparcv9/eri
112970	07	CURRENT	SunOS 5.9: patch libresolv
112998	03	CURRENT	SunOS 5.9: patch /usr/sbin/syslogd
113033	05	CURRENT	SunOS 5.9: patch /kernel/drv/isp and /kernel/drv/sparcv9/isp
113068	06	CURRENT	SunOS 5.9: hpc3130 patch
113073	14	CURRENT	SunOS 5.9: ufs and fsck patch
113077	14	CURRENT	SunOS 5.9: /platform/sun4u/kernel/drv/su Patch
113096	03	CURRENT	X11 6.6.1: OWconfig patch

113226	05	CURRENT	SunOS 5.9: hme Driver Patch
113240	11	CURRENT	CDE 1.5: dtsession patch
113273	10	CURRENT	SunOS 5.9: /usr/lib/ssh/sshd Patch
<input type="checkbox"/> 113277	29	32	SunOS 5.9: sd and ssd Patch
113278	09	CURRENT	SunOS 5.9: NFS Daemon, rpcmod Patch
113279	01	CURRENT	SunOS 5.9: klmmod Patch
113319	20	CURRENT	SunOS 5.9: libnsl nispasswd patch
113329	12	CURRENT	SunOS 5.9: lp Patch
113447	25	CURRENT	SunOS 5.9: libprtdiag_psr Patch
113451	09	CURRENT	SunOS 5.9: IKE Patch
113482	02	CURRENT	SunOS 5.9: sbin/sulogin Patch
113575	05	CURRENT	SunOS 5.9: sendmail Patch
113579	07	CURRENT	SunOS 5.9: ypserv/ypxfrd patch
113713	18	CURRENT	SunOS 5.9: pkginstall Patch
<input type="checkbox"/> 113718	02	03	WITHDRAWN PATCH SunOS 5.9: usr/lib/utmp_update Patch
113923	02	CURRENT	X11 6.6.1: security font server patch
114008	01	CURRENT	SunOS 5.9: cachefs Patch
114014	09	CURRENT	SunOS 5.9: libxml, libxslt and Freeware man pages Patch
114125	01	CURRENT	SunOS 5.9: IKE config.sample patch
114127	03	CURRENT	SunOS 5.9: abi_libefi.so.1 and fmthard Patch
114129	02	CURRENT	SunOS 5.9: multi-terabyte disk support -libuuid patch
114133	02	CURRENT	SunOS 5.9: mail Patch
114135	03	CURRENT	SunOS 5.9: at utility Patch
<input type="checkbox"/> 114332	17	18	SunOS 5.9: c2audit & *libbsm.so.1 Patch
114344	09	CURRENT	SunOS 5.9: arp, dlcosmk, ip, and ipgpc Patch
114361	01	CURRENT	SunOS 5.9: /kernel/drv/lofi Patch
114363	02	CURRENT	SunOS 5.9: sort Patch
114482	04	CURRENT	SunOS 5.9: Product Registry CLI Revision
114495	01	CURRENT	CDE 1.5: dtprintinfo patch
114564	04	CURRENT	SunOS 5.9: /usr/sbin/in.ftpd Patch
114569	02	CURRENT	SunOS 5.9: libdbm.so.1 Patch
114571	02	CURRENT	SunOS 5.9: libc.so.*.9/bcp Patch
114684	03	CURRENT	SunOS 5.9: samba Patch
114713	02	CURRENT	SunOS 5.9: newtask Patch
114721	05	CURRENT	SunOS 5.9: ufsrestore and ufsdump Patch
114729	01	CURRENT	SunOS 5.9: usr/sbin/in.telnetd Patch
114861	01	CURRENT	SunOS 5.9: /usr/sbin/wall
114971	02	CURRENT	SunOS 5.9: usr/kernel/fs/namefs Patch
115165	05	CURRENT	SunOS 5.9: usr/lib/libnisdb.so.2 Patch
115172	01	CURRENT	SunOS 5.9: kernel/drv/le Patch
115665	10	CURRENT	SunOS 5.9: Chalupa platform support patch
115683	03	CURRENT	SunOS 5.9: Header files Patch
115689	01	CURRENT	SunOS 5.9: /usr/lib/patch/patchutil Patch
115754	02	CURRENT	SunOS 5.9: zlib security Patch
116237	01	CURRENT	SunOS 5.9: pfexec Patch
116245	01	CURRENT	SunOS 5.9: uncompress Patch

116247	01	CURRENT	SunOS 5.9: audit_warn Patch
116308	01	CURRENT	CDE 1.5: libDtHelp patch
116453	02	CURRENT	SunOS 5.9: sadmind patch
116532	03	CURRENT	SunOS 5.9: mpt Patch
116538	03	CURRENT	SunOS 5.9: SUNW_disk_link.so Patch
116561	04	CURRENT	SunOS 5.9: platmod Patch
116774	03	CURRENT	SunOS 5.9: ping patch
117067	01	CURRENT	SunOS 5.9: awk nawk oawk Patch
117071	01	CURRENT	SunOS 5.9: memory leak in llc1_ioctl()
117114	02	CURRENT	CDE 1.5: sdtwebclient patch
117171	17	CURRENT	SunOS 5.9: Kernel Patch
117455	01	CURRENT	SunOS 5.9: in.rwhod Patch
<input type="checkbox"/> 118558	02	03	SunOS 5.9: Kernel Patch

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix C

The following is the output of the Nessus scan from Section 3.17.

Warning found on port telnet (23/tcp)

The Telnet service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

Solution:

If you are running a Unix-type system, OpenSSH can be used instead of telnet. For Unix systems, you can comment out the 'telnet' line in /etc/inetd.conf. For Unix systems which use xinetd, you will need to modify the telnet services file in the /etc/xinetd.d folder. After making any changes to xinetd or inetd configuration files, you must restart the service in order for the changes to take affect.

In addition, many different router and switch manufacturers support SSH as a telnet replacement. You should contact your vendor for a solution which uses an encrypted session.

Risk factor : Low

CVE : [CAN-1999-0619](#)

Nessus ID : [10280](#)

Information found on port telnet (23/tcp)

A telnet server seems to be running on this port

Nessus ID : [10330](#)

Information found on port telnet (23/tcp)

Remote telnet banner :

SunOS 5.9

Nessus ID : [10281](#)

Information found on port telnet (23/tcp)

Remote telnet banner :

SunOS 5.9

Nessus ID : [10281](#)

Information found on port ssh (22/tcp)

An ssh server is running on this port

Nessus ID : [10330](#)

Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-Sun_SSH_1.0.1

Nessus ID : [10267](#)

Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.99

. 2.0

Nessus ID : [10881](#)

Information found on port ftp (21/tcp)

An FTP server is running on this port.

Here is its banner :

220 gsna-be-lldap2 FTP server ready.

Nessus ID : [10330](#)

Information found on port ftp (21/tcp)

Remote FTP server banner :

220 gsna-be-lldap2 FTP server ready.

Nessus ID : [10092](#)

Information found on port ftp (21/tcp)

Remote FTP server banner :

220 gsna-be-lldap2 FTP server ready.

Nessus ID : [10092](#)

Information found on port rpcbind (111/tcp)

The RPC portmapper is running on this port. An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port.

Risk factor : Low

CVE : [CAN-1999-0632](#), [CVE-1999-0189](#)

BID : [205](#)

Nessus ID : [10223](#)

Information found on port rpcbind (111/tcp)

RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port

RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port

Nessus ID : [11111](#)

Information found on port uis (390/tcp)

A web server is running on this port

Nessus ID : [10330](#)

Information found on port uis (390/tcp)

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/manual/help/help (helpdir [admin] token [framework-legacy-console-info] mapfile [tokens.map])

Nessus ID : [10662](#)

Information found on port uis (390/tcp)

Nessus was not able to reliably identify this server. It might be:

Netscape-Enterprise/6.0

Netscape-Enterprise/4.1

The fingerprint differs from these known signatures on 3 point(s)

Nessus ID : [11919](#)

Information found on port uis (390/tcp)

The remote web server type is :

Netscape-Enterprise/6.0

Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.

Nessus ID : [10107](#)

Vulnerability found on port ldap (389/tcp)

Improperly configured LDAP servers will allow the directory BASE to be set to NULL. This allows information to be culled without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user can query your LDAP server using a tool such as 'LdapMiner'

Solution: Disable NULL BASE queries on your LDAP server

Risk factor : Medium
Nessus ID : [10722](#)

Vulnerability found on port ldap (389/tcp)

Improperly configured LDAP servers will allow any user to connect to the server and query for information.

Solution: Disable NULL BIND on your LDAP server

In addition, the LDAP bind function in Exchange 5.5 has a buffer overflow that allows a user to conduct a denial of service or execute commands in all versions prior to Exchange server SP2. Coupled with a NULL BIND, an anonymous user can mount a remote attack against your server.

Note: no test was done to see what version of Exchange server is running, nor attempt to verify the service pack.

Solution: see <http://www.microsoft.com/technet/security/bulletin/ms99-009.asp>

Risk factor: Medium

CVE : [CVE-1999-0385](#)

BID : [503](#)

Nessus ID : [10723](#)

Warning found on port shell (514/tcp)

The rsh service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

You should disable this service and use ssh instead.

Solution : Comment out the 'rsh' line in /etc/inetd.conf.

Risk factor : Low

CVE : [CAN-1999-0651](#)

Nessus ID : [10245](#)

Information found on port lockd (4045/tcp)

RPC program #100021 version 1 'nlockmgr' is running on this port
RPC program #100021 version 2 'nlockmgr' is running on this port
RPC program #100021 version 3 'nlockmgr' is running on this port
RPC program #100021 version 4 'nlockmgr' is running on this port

Nessus ID : [11111](#)

Information found on port sometimes-rpc9 (32773/tcp)

This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin

Nessus ID : [10919](#)

Information found on port sometimes-rpc7 (32772/tcp)

RPC program #100024 version 1 'status' is running on this port
RPC program #100133 version 1 is running on this port

Nessus ID : [11111](#)

Information found on port sometimes-rpc5 (32771/tcp)

RPC program #100422 version 1 is running on this port

Nessus ID : [11111](#)

Warning found on port general/tcp

The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch

Risk factor : Medium

BID : [7487](#)

Nessus ID : [11618](#)

Information found on port general/tcp

10.10.10.150 resolves as gsna-be-ldap2.

Nessus ID : [12053](#)

Information found on port general/tcp

Nessus was not able to reliably identify the remote operating system. It might be:

Sun Solaris 9 The fingerprint differs from these known signatures on 1 points. If you know what operating system this host is running, please send this signature to os-signatures@nessus.org :

:1:1:1:255:1:255:1:1:255:1:0:255:1:64:255:1:1:1:1:3:1:1:1:1:64:49232:NNTMNW
NNS:0:1:1

Nessus ID : [11936](#)

Information found on port sunrpc (111/udp)

RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is

running on this port

RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is

running on this port

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is

running on this port

Nessus ID : [11111](#)

Warning found on port lockd (4045/udp)

The nlockmgr RPC service is running. If you do not use this service, then disable it as it may become a security threat in the future, if a vulnerability is discovered.

Risk factor : Low

CVE : [CVE-2000-0508](#)

BID : [1372](#)

Nessus ID : [10220](#)

Information found on port lockd (4045/udp)

RPC program #100021 version 1 'nlockmgr' is running on this port

RPC program #100021 version 2 'nlockmgr' is running on this port

RPC program #100021 version 3 'nlockmgr' is running on this port

RPC program #100021 version 4 'nlockmgr' is running on this port

Nessus ID : [11111](#)

Vulnerability found on port sometimes-rpc8 (32772/udp)

The remote statd service may be vulnerable to a format string attack.

This means that an attacker may execute arbitrary code thanks to a bug in this daemon.

*** Nessus reports this vulnerability using only information that was gathered.

*** Use caution when testing without safe checks enabled.

Solution : upgrade to the latest version of rpc.statd

Risk factor : High

CVE : [CVE-2000-0666](#), [CAN-2000-0800](#)

BID : [1480](#)

Nessus ID : [10544](#)

Warning found on port sometimes-rpc8 (32772/udp)

The statd RPC service is running. This service has a long history of security holes, so you should really know what you are doing if you decide to let it run.

*** No security hole regarding this program have been tested, so
*** this might be a false positive.

Solution : We suggest that you disable this service.

Risk factor : High

CVE : [CVE-1999-0018](#), [CVE-1999-0019](#), [CVE-1999-0493](#)

BID : [127](#), [450](#)

Nessus ID : [10235](#)

Information found on port sometimes-rpc8 (32772/udp)

RPC program #100024 version 1 'status' is running on this port

RPC program #100133 version 1 is running on this port

Nessus ID : [11111](#)

Information found on port general/udp

For your information, here is the traceroute to 10.10.10.150 :

10.10.10.130

10.10.10.150

Nessus ID : [10287](#)

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker

to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low

CVE : [CAN-1999-0524](#)

Nessus ID : [10114](#)

Warning found on port general/icmp

The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.255.128). An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters.

Solution : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17.

Risk factor : Low
CVE : [CAN-1999-0524](#)
Nessus ID : [10113](#)

© SANS Institute 2000 - 2005, Author retains full rights.