



# 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.

# **GCUX Practical Assignment Version 2.0**

Option 2 – Consultant's Report from auditing UNIX

## **Security Audit of GIAC Enterprises Sun Solaris UNIX Server**

Submitted By: Mark A. Winship  
Date: March 4 2004

## Abstract

---

GIAC Enterprises has requested that an external audit be completed against a representative sample of the UNIX systems within the GIAC enterprise. GIAC is hiring an external consulting firm in order to identify shortcomings in several aspects of the IT organization. GIAC Enterprises understands that protections need to be put in place in order to effectively maintain an infrastructure that is used to deliver a secure on-line based product. A breach of sensitive customer information could drastically impair GIAC's ability to maintain its online presence in the market place. This audit will examine a UNIX system configuration, staff training levels, security awareness levels, as well as compliance levels within the GIAC organization. Several recommendations will be made to improve the overall security level of GIAC Enterprises.

© SANS Institute 2004, Author retains full rights.

## Table of Contents

---

<b>Abstract .....</b>	<b>i</b>
<b>Table of Contents.....</b>	<b>ii</b>
<b>Executive Summary .....</b>	<b>1</b>
<i>Purpose of the Audit.....</i>	<i>1</i>
<i>Audit Scope .....</i>	<i>1</i>
<i>Conclusions and Recommendations .....</i>	<i>1</i>
<b>Description of System and Audit Methodology .....</b>	<b>3</b>
<i>Description of the Audited System .....</i>	<i>3</i>
<i>Audit Methodology.....</i>	<i>4</i>
<b>Detailed Analysis .....</b>	<b>6</b>
<i>Operating System Vulnerabilities &amp; Patch Management Procedures.....</i>	<i>6</i>
<i>Configuration Vulnerabilities.....</i>	<i>7</i>
<i>Risks from Installed Third Party Software .....</i>	<i>12</i>
<i>Administrative Practices .....</i>	<i>13</i>
<i>Identification and Protection of Sensitive Data on the Host.....</i>	<i>14</i>
<i>Protection of Sensitive Data in Transit or Over the Network or Internet .....</i>	<i>16</i>
<i>Access Controls .....</i>	<i>17</i>
<i>Backup Policies and Disaster Preparedness.....</i>	<i>18</i>
<i>Other Issues.....</i>	<i>18</i>
<b>Critical Issues and Recommendations .....</b>	<b>19</b>
<i>Top 10 Issues Identified.....</i>	<i>19</i>
<i>Other Recommendations .....</i>	<i>20</i>
<b>Appendix A – System Description.....</b>	<b>22</b>
<i>Hardware.....</i>	<i>22</i>
<i>Software .....</i>	<i>23</i>
<b>Appendix B – Detailed Analysis .....</b>	<b>24</b>
<i>OS Vulnerabilities – Patchdiag v1.04 output .....</i>	<i>24</i>
<i>Initialization Scripts.....</i>	<i>34</i>
<i>System Logging.....</i>	<i>34</i>
<b>Appendix C – Automated Scanning Tool Output .....</b>	<b>35</b>
<i>NMAP 3.50.....</i>	<i>35</i>
<i>Nessus 2.0.10 .....</i>	<i>36</i>
<i>CISscan 1.4.0.....</i>	<i>51</i>
<i>UnixAudit.sh .....</i>	<i>55</i>
<i>John 1.6.36.....</i>	<i>64</i>
<b>References .....</b>	<b>65</b>

## Executive Summary

---

### ***Purpose of the Audit***

GIAC Enterprises, hereafter GIAC, has requested that MAW Security Solutions perform a security audit of its UNIX server environment. GIAC is an e-business specializing in the online sale of fortune cookie sayings. Due to the online nature of its business GIAC has UNIX servers both connected to the Internet as well as the internal corporate network. Sensitive customer account information is transacted and stored on GIAC servers, which need to be protected. A breach of this information could significantly impair the financial stability of the company.

This internal audit will identify the current security exposures within the GIAC UNIX environment and help prioritize the remediation and/or mitigation of the security risks associated with the findings.

### ***Audit Scope***

GIAC has requested that the technical portions of this audit *not* be completed against the production online environment supporting GIAC customers. With this restriction in mind it was determined that MAW Security Solutions would audit a representative sample of the UNIX environment.

The server that was selected for this audit is a Sun UNIX server running the Solaris 8 Operating System. This UNIX server was built via an automated installation method (Sun Jumpstart technology). This automated installation provides the base operating system installation for all Sun Solaris servers at GIAC.

Once an automated installation is completed GIAC application administrators will install the appropriate applications for the server in question (Database, Web Server, etc.). An audit of these third party applications was out of scope for this engagement.

### ***Conclusions and Recommendations***

The overall security state of the UNIX servers at GIAC has been rated **poor**. Factors that contributed to this poor security state include:

- Excessive amount of UNIX System Configuration Vulnerabilities,
- Lack of Policies and Procedures,
- Lack of Security Training within the UNIX Administration team,
- Lack of Security Awareness across the enterprise, and
- Moderate Level of Automated Security Monitoring and Notification.

The implementation of the technical recommendations included within the body of this document will greatly improve the security state of the servers at GIAC.

These recommendations can easily be applied to all production servers at GIAC and then be applied to the Sun Jumpstart installation server that is used to build future Sun Solaris servers at GIAC.

In order to effectively implement and maintain a secure environment in the future the UNIX administration team should be properly trained in UNIX security concepts. This training will allow for successful implementation of the recommendations documented in this audit and will also ensure that the proper security related questions will be raised as new servers and application services are implemented at GIAC.

The Information Security Group at GIAC should be tasked to implement a Security Awareness program. This program should be fully documented and made available to all employees at GIAC. The security awareness program may consist of awareness posters, web based training, newsletter articles, and/or workshops. The method of disseminating the awareness information will be different for every organization.

Furthermore, the Information Security Group should also be tasked to provide Internal Auditing of the production operations group at GIAC. It is one thing to create and document security related procedures, but care must be taken to ensure these procedures and policies are adhered to within the organization.

© SANS Institute 2004, Author retains full rights.

## **Description of System and Audit Methodology**

---

### ***Description of the Audited System***

#### Hardware and Software

The system selected for this audit is a Sun Microsystems Sun Fire v440 Server running Solaris 8. The hostname of the system is *giacunixhost.giac-fortune.com*. The Sun Solaris 8 Recommended & Security Patch Cluster was applied on January 13, 2004. This host has dual 1 GHz processors and 8GB of memory. There are 2 36GB hard drives which are used as mirrored OS partitions. All disk drives are managed and mirrored via the Veritas Volume Manager V3.5. The system in question is connected to EMC Clariion CX400 external disk storage via the storage area network (SAN). This connection was made for the purposes of illustrating a typical UNIX host configuration.

This audit concentrates on the UNIX operating system and security configuration and does not attempt to identify vulnerabilities or insecure configurations of the SAN architecture or third party applications that do not come packaged with the Solaris operating system.

Network based backups of all UNIX systems are completed via Veritas NetBackup Data Center 4.5. These backups take place via a dedicated backup service network. The backup procedure and tape storage methods are documented later in this document.

Several scripts have been put in place by the UNIX System Administrators to monitor and notify of changes to the machine. These scripts include: disk space monitoring, network accessibility (ping) monitoring, core file monitoring, SUID file monitoring, and monitoring for password/shadow file changes.

[Appendix A](#) has been provided to detail the steps taken to identify the hardware and software configuration of the UNIX host.

#### System Role in the GIAC Network

The system being audited is a base Solaris 8 operating system configuration with no third-party GIAC applications installed. The role of this system is to provide a secure base from which GIAC application administrators can then install a third party application. Common machines on the GIAC network include web servers and database servers, all of which were installed on top of his standard Jumpstart installation.

Both of these types of hosts (web and database servers) have inherent security risks associated with them. For instance GIAC has several web servers that are installed in a Demilitarized Zone (DMZ) and protected by a firewall. GIAC customers connect to these servers via the Internet to place on-line orders. The

Internet DMZ firewall provides network based packet inspection and traffic filtering for the web servers. Customer confidential information is not stored on the web servers, but is stored in an Oracle Database which sits behind the DMZ firewall and on the corporate network.

The web servers at GIAC have a high risk of being attacked via the Internet, whereas the Database servers cannot be accessed directly via the Internet. The Database servers have a high risk of being compromised via an untrustworthy employee and a low to moderate risk of being compromised via an attack that utilized the web front end to compromise information that is stored in the database.

### ***Audit Methodology***

MAW Security Solutions has developed a multi-phase process for performing UNIX security audits.

#### Phase 1 – Interviews

The first phase of the audit consists of on-site interviews with GIAC personnel. The primary focus of these interviews was with the UNIX system administration team as well as with the Information Security Group Manager. A few employees outside of the technology department were interviewed in order to help determine the security awareness level within the organization. Discussion points during the interviews included:

- Current system administration practices and procedures
- Documentation relating to the Sun Jumpstart standard OS build
- Security awareness within the organization
- Security training level of the UNIX system administration team
- Current Information Security Policy and how it pertains to the UNIX servers
- The level of internal auditing performed by the company

#### Phase 2 – System Configuration

The second phase consists of gathering information relating to the UNIX system configuration. Several UNIX commands will be executed on the audited UNIX system to gather important system configuration information. The output of these commands will be used to validate information learned during the interview process and information that is documented in the Information Security Policy.

#### Phase 3 – Automated Tools

Several automated scanning tools will be used to assess the security configuration of the UNIX hosts being audited. The reports from each of the automated tools are included in [Appendix C](#). These tools that were run include:



- NMAP – NMAP is a network-based port scanning utility which will be used to assess what network services (ports) are available on the UNIX host and will also attempt to gather the operating system of the host.
- Nessus – Nessus is a network based vulnerability scanner that will be deployed to identify the network services (ports) running on the UNIX host as well as identify and possibly exploit any security vulnerabilities it finds in the services running. Nessus is an intrusive scanning utility and could possibly cause services or the server to malfunction during the scanning, hence the use of a non-production system. The Nessus report will identify software vulnerabilities in the UNIX configuration of the server being audited.
- CISscan – CISscan is a host based auditing utility developed by the Center for Internet Security which will be used to benchmark the security level of a given UNIX system based upon its configuration. This tool looks at several configuration aspects of a running UNIX system to create an overall measurement of the system security level. This measurement can be compared against other UNIX systems within the company or the Industry. The CISscan tool is installed and run on the local UNIX system and is not run from a remote location like the NMAP and Nessus tools. Since this tool requires root access to the UNIX system being audited, the tool will be run by the GIAC UNIX Administrators with a security engineer from MAW Security Solutions observing the program execution.
- UnixAudit.sh – A custom script written and maintained by MAW Security Solutions was run to automate the gathering of several configuration files and system states. The output of this script was used during several phases of this audit.
- John the Ripper – John the Ripper is a brute force password cracking utility and will be deployed to assess the strength of the user passwords. John the Ripper will be deployed against the users configured on the audited host only.

#### Phase 4 – Analysis

The final step in the process will be to organize all the information gathered in together to create and prioritize recommendations for improving the information security state at GIAC.

## Detailed Analysis

---

### ***Operating System Vulnerabilities & Patch Management Procedures***

The audited host was running Sun Solaris 8 at a kernel patch level 108528-27. GIAC has standardized on Solaris 8 for their UNIX operating system and will continue to use this release until such a time where either Solaris 8 either does not meet their current needs with regard to feature set, support, or security.

During the interviews the UNIX system administrator stated that this host was patched with the most recent Solaris Recommended and Security Patch cluster in January of 2004. This was confirmed via the patch cluster installation log file located in `/var/sadm/install_data/Solaris_8_Recommended_log`. To further confirm the success of the patch cluster the Sun Patchdiag utility was run to compare the installed system patches against the most current cross reference file (`patchdiag.xref`) that was downloaded from [sunsolve.sun.com](http://sunsolve.sun.com).

The output of the Patchdiag utility is included in [Appendix B](#). A thorough review of the section entitled “UNINSTALLED SECURITY PATCHES” in the Patchdiag report was completed to identify any false positives from the report. It was determined that several of the patches listed as not being installed were actually installed, but under a different patch name due to the original patch being obsoleted by a newer patch under a different name. After removing these false positives from the list, five (5) patches remained uninstalled. Using the “`pkginfo`” command it was determined that the software for four (4) of these patches was not on the system and these patches did not need to be installed. This left one (1) security patch that needs to be installed to bring the system up to date.

Patch #	Package	Applicability
109951	SUNWjwnju	n/a
110416	JSatsvr	n/a
112792	SUNWpcmcu	n/a
114045	SUNWpr	n/a
<b>116455</b>	<b>SUNWadmfw</b>	<b>UNINSTALLED/REQUIRED</b>

The UNIX system administrators have a rigorous patch management procedure in place which allows them to keep the operating system packages up to date and secure. This process consists of installing a quarterly Recommended and Security Patch cluster on all of the Sun Solaris machines in the enterprise. Before installing a patch cluster on a production server the UNIX Administrator’s will first test the patch cluster on their personal Sun workstations. The cluster will run for a week on these workstations to identify any bugs and/or problems that

may arise. Once tested on these workstations the patch cluster will be installed on the application QA machines in the company. The application QA machines are as close to an identical configuration to application production servers and are a very good test of the patch cluster. Once installed, regression testing will be performed on these QA hosts. After a week of successful operation the patch cluster will be installed on all of the production servers within the enterprise. This installation has been automated and happens over a two week period during the off-hours maintenance window. The administrators also have a procedure whereby each time a new patch cluster is installed in production that this same patch cluster must also be applied to the Sun Solaris Jumpstart server to be included in all future automated system builds.

In order to keep current on security patches as they are published the UNIX administrators have subscribed to Sun Alert Bulletins. These bulletins are emailed to the team and identify new security vulnerabilities as they are released. The system administration team in conjunction with the information security department makes a decision if the patch should be installed immediately (via the process above) or wait till the next regularly scheduled patch cluster installation to apply the patch.

## ***Configuration Vulnerabilities***

### Unnecessary Services Configured at System Boot

Several unnecessary services have been configured to start during the UNIX system boot process. This was confirmed via the automated network mapping and vulnerability assessment tools that were run (NMAP and Nessus) as well as from looking in the `/etc/rc2.d` and `/etc/rc3.d` initialization script directories ([Appendix B – Initialization Scripts](#), and [Appendix C – Automated Scanning Tool Output](#)). The UNIX administrators explained that they were not aware of the function of some of these system services and did not want to impact production by disabling these startup scripts.

NMAP was used as the primary tool to identify services that were running since several of the initialization scripts were in place but did not start any running daemons due to the configuration files not being present. When looking at the NMAP output you can immediately see several services that are indicative of a default Solaris OS installation. Several services that are recommended as being disabled include:

- **`/etc/inetd.conf`** – Several services are run from the INET daemon. Although the INETD daemon will not be completely disabled, several service entries in the INETD configuration file (`/etc/inetd.conf`) can be commented out or removed. These include:
  - `echo`, `discard`, `daytime`, `chargen`, `sprayd` – Legacy testing programs that are often used to launch a denial of service attack.

- wall – Write to all users – This is a system broadcast mechanism that could be used to launch a denial of service attack.
- time – Legacy time synchronization – NTP is recommended as a time synchronization protocol.
- nameserver – Trivial Name server – Legacy Name services.
- printer – Printer Services
- talk - Host to host chat program
- uucp – Legacy UNIX to UNIX copy program previously used for email routing
- finger – Legacy service used to provide information about system users. Attackers often use the finger service to gain unauthorized information about the UNIX system and users.
- rusersd – Remote User Daemon – The rusersd daemon can be used by an attacker to gain unauthorized information about system users.
- dmispd – Sun Solstice Management communication channel. Sun Solstice Management tools are not used at GIAC.
- ttldbserverd – Sun Tool Talk Database Server – Not used GIAC.
- sadmind – Sun Solstice System and Network Administration daemon – Not used at GIAC.
- kcms\_server – Sun KCMS Profile Server – Not used at this GIAC.
- rquotad – Provides quota information for NFS clients. NFS is not used at GIAC.
- cmsd – Calendar Daemon – Not used at GIAC.
- font-service – X Windows Font Server – X Windows is not used at GIAC.
- dtspcd – CDE related application – CDE is not used at GIAC.
- **SNMP** – SNMP services are not used at GIAC and should be disabled by removing the startup scripts in `/etc/rc3.d/S76snmpdx` and `/etc/rc3.d/S77dmi`. If SNMP is required in the future the default

community string of “public” should be changed in the SNMP configuration files (/etc/snmp/conf). SNMP has traditionally been used to obtain sensitive system information from a host. This information is used to further an attack against the organization. These attacks are often completed using either the default community string of “public” on an improperly configured server.

- **CDE/X windows** – CDE is not used at GIAC and can be disabled from starting at the UNIX system boot by removing the startup script /etc/rc2.d/S99dtlogin. CDE and X windows services have traditionally been a common avenue of attack by hackers and should be disabled if not used.
- **NFS Client/Server** – NFS is not used anywhere within GIAC and can be disabled by removing the initialization scripts /etc/rc2.d/S73nfs.client and /etc/rc3.d/S15nfs.server. NFS services, if configured in the future, should be properly secured via host based access controls via the /etc/dfs/dfstab configuration file.
- **Sendmail** – Even though this server is not functioning as an email server, Sendmail is currently configured and running in daemon mode. It is recommended that Sendmail be configured to run in “queue” mode only. This will allow for client email services on the UNIX host while removing the listening Sendmail daemons. This can be completed by adding the following directive to the Sendmail configuration file /etc/default/Sendmail.

```
## Set MODE="" to have Sendmail run in non-listening/queue mode
MODE=""
```

Port 587 (submission) was identified as a Sendmail daemon. This was identified in the NMAP and Nessus reports ([Appendix C](#)) and was confirmed with the following commands:

```
# lsof -i -P | grep 587
sendmail  4801  root    8u  IPv4  0x30006b1fa70      0t0  TCP *:587 (LISTEN)

#lsof -i -P | grep sendmail
sendmail  4801  root    4r  IPv4  0x30005791710      0t0  UDP *: (Unbound)
sendmail  4801  root    6u  IPv4  0x30006b17588      0t0  TCP *:25 (LISTEN)
sendmail  4801  root    7u  IPv6  0x30005f08f38      0t0  TCP *:25 (LISTEN)
sendmail  4801  root    8u  IPv4  0x30006b1fa70      0t0  TCP *:587 (LISTEN)
```

The submission protocol has been defined in RFC 2476 and it is okay to see Sendmail listening on this port.

The Nessus vulnerability assessment report ([Appendix C – Nessus](#)) identified several vulnerabilities in the Sendmail application. If Sendmail is configured to not accept email from external hosts (queue mode only),

then all of the *remotely exploitable* vulnerabilities that Nessus identified no longer apply to this host.

The remaining *locally exploitable* Sendmail vulnerabilities are false positives as Nessus identified an incorrect version of Sendmail which was used to perform vulnerability correlation. A review of the Sun patch level indicated that the most recent Sun Sendmail patch (110615-10) has been applied which fixes all known security issues with the Sun Sendmail program to date.

- **Miscellaneous Services:** The CISscan report ([Appendix C - CISscan](#)) in conjunction with an audit of the initialization scripts identified several additional services that can be removed from the default operating system configuration. These services include: llc2, uucp, slpd, PRESERVE, bdconfig, wbem, ncalogd, ncad, mipagent, autoinstall, asppp, cachefs.daemon, cacheos.finish, power, dmi, lp, and spc.

These initialization scripts are located in the directory `/etc/init.d` and have symbolic links in `/etc/rc2.d` or `/etc/rc3.d` which are executed during the system initialization. Removal of a script's symbolic link in the `/etc/rc?.d` directory will effectively stop the running service upon the next system boot while allowing the software to remain on the system until proper regression testing can take place.

Several clear-text services are utilized for remote administrative terminal connections and file transfers to and from the UNIX servers. These services include ftp, telnet, rlogin, rsh, and rexec. All data transferred via these services is clear text. Secure Shell (SSH) should be considered as a secure replacement of these services.

The Nessus Vulnerability Report falsely identified the FTPD service as being vulnerable to a "global heap corruption flaw". This was based on the Solaris ftp banner and an exploit was not attempted. It was confirmed that Sun Patch 111606-01 has been installed, which was indicated as the fix to this vulnerability in the Nessus solution section entitled: BID 2550 (Security Focus BugTraq ID 2550).

```
# showrev -p | grep 111606
Patch: 111606-03 Obsoletes: Requires: Incompatibles: Packages: SUNWftpu
Patch: 111606-04 Obsoletes: Requires: Incompatibles: Packages: SUNWftpu
```

By disabling the services identified above and making the proper changes to the Sendmail configuration all of the application/service level vulnerabilities identified in the Nessus Vulnerability Report will have been remediated.

## Unnecessary Software Packages

In addition to the unnecessary system services starting at boot time there are several unnecessary software packages installed on the server. This can be identified with the command `“/usr/bin/pkginfo”`.

This system appears to be an “entire” installation of Sun Solaris 8.

Unnecessary software packages can pose a threat to the system and network due to un-patched vulnerabilities in the software. Furthermore, these packages could be used by an attacker to launch an attack on another system or be exploited to elevate rights on the local system. For example, the GNU compiler suite was installed on this UNIX host. A compiler could be used by an attacker to build and run additional programs to further advance an attack that is in progress.

## Audit Logging

A review of the `/etc/syslog.conf` file ([Appendix B – System Logging](#)) identified that this host is not recording any of the system logs to a remote host. An off-host copy of the system logs would be required in the event of a system compromise. These off-host logs would be used to research and track any activities of the intruder. This configuration is contrary to the GIAC information security policy which states in *Section IX, Subsection 3 – (Information Protection)* that system audit trails of all computers and network devices within the GIAC network must store audit logs on a network host other than the host that generated the audit log.

A program such as the bundled Sun Syslog or syslog-ng ([http://www.balabit.com/products/syslog\\_ng/](http://www.balabit.com/products/syslog_ng/)) can be used to meet this requirement of off-host logging.

Syslog-ng (“New Generation”) offers several advanced security features over the traditional syslog that make this tool attractive (TCP as the transfer medium as compared to UDP, Secure log storage/hashing, and the ability to use SSH or stunnel to securely send syslog messages to an alternate host).

In addition to storing off-host audit logs, accurate time synchronization of all UNIX hosts must be achieved. Time synchronization will ensure that logs from several hosts within the network can be correlated to provide a timeline of an attack or event within the network. Time synchronization can be achieved via a program called NTP (Network Time Protocol). XNTPD (an implementation of the NTP protocol) is shipped standard with the Sun Solaris operating system and should be utilized on all UNIX hosts. This service can be configured via the `/etc/inet/ntp.conf` configuration file. Care should be taken to understand and implement the proper authentication keys with the NTP configuration. Details can be found in the XNTPD man page `xntpd(1M)`. More information about NTP can be found at <http://www.ntp.org>.

By default failed login attempts under Solaris are not logged. This can be configured by creating the following log file via the following commands:

```
touch /var/adm/loginlog
chmod 600 /var/adm/loginlog
chown root:sys /var/adm/loginlog
```

Additional logging of authentication attempts should be configured by adding the following entry to the `/etc/syslog.conf` file. The log file `/var/log/authlog` already existed on the server and it has the appropriate permissions of 600 and ownership of `root:sys`. No entries were being written to this file as the `/etc/syslog.conf` file had not yet been updated.

```
# Authentication Logging - Be sure there is a <tab> between the parameters
auth.info      /var/log/authlog
```

Lastly, the syslog daemon on this host should be configured to not accept syslog log entries from remote hosts as this machine is not a centralized syslog server. This can be accomplished in Solaris 8 by adding the “-t” option to the syslog daemon startup sequence in the initialization script `/etc/rc2.d/S74syslog`. See the syslog man page for details: `syslog(1M)`.

The UNIX administrators have taken additional steps to enable INET daemon connection logging to the log file `/var/log/connlog`. This was done over and above the standard Solaris OS installation.

#### Authorized Use Warning Banners

*Section X, Subsection B (System Status/Warning Banners)* of the GIAC information security policy states the following:

1. A warning notice should be displayed prior to network log-in, alerting all users that access to the system is available only to authorized users, the system is being monitored to detect improper use and other illicit activity, and that there should be no expectation of privacy while using this system.

The audited host did not have any warning banners in place in any of the standard locations: `/etc/issue`, `/etc/motd`, `/etc/default/telnetd`, `/etc/default/ftpd`, or the Sun eeprom. This is both a violation of industry best practice as well as is a violation of the GIAC Information Security Policy.

#### ***Risks from Installed Third Party Software***

Since the server that was audited was newly jumpstarted as a base Solaris Operating System, no third party applications had been installed at the time of the audit. Common applications that would be installed on this base OS at GIAC include web servers and Oracle database servers. As these services were out of the scope of this audit and detailed analysis was not completed against GIAC's production Web or Database server configurations.



Special care should be taken when configuring the web server or database server software to ensure that no security holes exist or are created through the installation of these applications. GIAC should work with application vendors to install and properly secure all third party applications.

The following materials are suggested for securing GIAC's Oracle Database Servers:

Finigan, Pete. Oracle Security: Step-by-Step. The SANS Institute, 2003

Theriault, Marlene L. and Aaron Newman. Oracle Security Handbook: Implement a Sound Security Plan in Your Oracle Environment. McGraw-Hill Osborne Media, 2001.

### ***Administrative Practices***

Discussions with the UNIX administrators uncovered a lack of documentation on the daily administrative practices of the team. Loosely documented procedures are in place for items like:

- Adding a new UNIX host to the network
- Adding/removing UNIX users
- Log Review (audit logs, backup logs, etc.)
- Automated Scripts in place to monitor systems
- Configuring and monitoring network backups

The documents that were found were scattered through each system administrator's desktop computer and are not stored on a central file server. Furthermore, no documentation exists to identify the daily routines of the system administrators and to provide accountability for their actions and the systems they manage.

Some of the system administrators do a better job than others in the daily monitoring and log review duties. These inconsistent practices are due in part to the lack of policies, procedures, and security awareness of the system administration staff.

It was clear that the UNIX system administrators were not aware of the GIAC Information Security Policy or the content that was documented with in it. Security Awareness was at a minimum with most employees in the organization and was clearly indicated in the interview as well by reviewing the UNIX system configurations as compared to items in the Information Security Policy. Items in

the Information Security Policy that were not in place on the UNIX systems included:

- Centralized/Off-Host Audit Log Storage
- Password Selection and Aging Criteria
- Authorized Use Banner Configuration

One procedure that was well documented and associated within the system administration group was the Change Control Procedure. A complete set of documentation and policies have been put in place to ensure that all configuration changes go before a change control board before being implemented. The change control board approves a system change based upon several criteria including but not limited to: Impact on other changes/systems Time/Date of Change, System Impact/Downtime, testing/QA criteria, and back-out plan.

### ***Identification and Protection of Sensitive Data on the Host***

Configuration files, application binaries, log files, and application core files are four types of files that contain sensitive data and need to be protected as such. Although GIAC system administrators have put in place a few automated scripts to look for the presence of core files and changes to critical system configuration files, a more thorough and automated process needs to be put in place to expand the current monitoring.

### **System Configuration Files & Application Binaries**

Currently scripts are in place to monitor and notify the system administrators when the following system configuration files are changed:

- /etc/passwd & /etc/shadow
- Root's crontab (/var/spool/cron/crontabs/root)

The CISscan report (Items 7.9) identified the adm, lp, and uucp crontab file permissions as being a security risk. In the current configuration these crontab files are readable by "world". The world readable bit should be removed from these files.

```
-rw-r--r--  1 root    sys      190 Jan 13 10:12 adm
-r--r--r--  1 root    root      750 Jan 13 10:12 lp
-r--r--r--  1 root    sys       404 Jan 13 10:28 uucp
```

Additional protections should be configured to ensure that only a minimal amount of users are allowed to use the CRON daemon. The CRON daemon is often used by an attacker to insert a Trojan program that will run at a certain date and time. This program may go disguised for a period of time before being executed at a predefined time and date.

These additional security protections can be configured by creating the file `/etc/cron.d/cron.allow` and populating this file with the users that are allowed to use the CRON daemon. It is recommended that GIAC limit this ability to a select few accounts on the system.

Scripts have also been written to notify the system administrators of any new SUID files on the system. SUID files allow a non-privileged user to execute a program that will run with root privileges.

A tool such as “tripwire” should be deployed to monitor for changes (content and permissions) to critical system configuration files and binaries. Tripwire creates a database of files, unique file checksum, ownership, permission, and modes. Each time the tripwire utility is run it will report any changes that have been identified. Information about Tripwire can be obtained from <http://www.tripwire.org>.

Additional protections can be implemented at the UNIX filesystem level to ensure that SUID files cannot be created. This is a relatively simple change that is made by adding the “nosuid” option to the mount option section of each filesystem in the `/etc/vfstab` configuration file. This industry best practice was also identified and documented in the CISscan report in [Appendix C – CISscan](#). Special care should be taken to ensure that the “nosuid” option is not implemented on a filesystem such as `/bin` that may require SUID system binaries.

In addition to the “nosuid” option, UNIX filesystems that contain application binaries can be mounted in read-only mode to protect the integrity of system binaries. Common filesystems that are mounted read-only include “`/usr`”, “`/usr/local`”, and “`/opt`”. When an application upgrade or patch installation needs to be completed the UNIX administrators would have to remount the filesystem in read-only mode before starting the installation.

### Log Files

As detailed in the previous section considerable work needs to be completed to increase the protection and storage of log files as well as the routine monitoring of these audit logs. Centralized off-host secure transport and storage of log files can be completed via a utility called “syslog-ng”. Storing these log files on a host other than the server in question will ensure that an attacker cannot alter the system logs and remove or alter the system audit trail.

A documented system log review procedure needs to be created and followed by all of the system administrators. This will ensure that all administrators are reviewing the proper logs and at the agreed upon frequency. Routine log review will ensure that each system administrator understands which log events are normal and will allow the administrator to quickly pick out any anomalies.

## Core Files

GIAC Administrators have made a conscious decision to allow system and application core files to be written to the UNIX file system. They are aware that core files can contain sensitive information that was in memory at the time of the core dump and have decided that the troubleshooting benefits that can be obtained by saving these core files are worth the risk. With this decision in mind the administrators have installed monitoring scripts that notify the team on an hourly basis when a new core file has been created. This allows the administration team to identify if the core file is needed and take appropriate action to protect the core file. Another script was put in place to remove any core files that are over a week old. This ensures that if a file is not deleted by the system administrator within an agreed upon time that the file will be deleted automatically.

## World Writable Files

Several files were identified as being world writable via the command:

```
find / -perm -2 -type f -ls
```

The CISscan utility also reported on these world writable files in its report.

The detailed output is included in [Appendix C](#). World writable files should never exist on a UNIX system and should be properly protected. It appears that the files that were identified as world writable are either temporary files or system/application log files. Care should be taken to properly restrict the permissions of these files.

## ***Protection of Sensitive Data in Transit or Over the Network or Internet***

Several clear text protocols are being used for remote access to the UNIX servers at GIAC. These protocols include ftp, telnet, rlogin, rsh, and rexec. Clear text protocols should never be used to remotely manage the UNIX servers at GIAC. SSH (Secure Shell) can be used as a secure replacement for the clear-text protocols that the system administrators use today. SSH will encrypt all communications with the host while maintaining the same look and feel of a telnet or rlogin client. SSH can be implemented for no charge on the UNIX server and either freeware SSH clients can be deployed on the administrator desktops or commercial products can be obtained for a nominal fee.

The System Administrators were aware of the benefits of SSH, but have not implemented at the site due to resistance from end users. It is highly recommended that the Administrators begin using SSH for their daily activities and work to implement SSH as the replacement for the telnet, rlogin, and ftp services for all GIAC employees that require access to a UNIX server.

## Access Controls

During the interviews with the system administrators it was noted that administrative access is completed by first logging in as a non-privileged user account and using the “su” command to assume root user privileges. Root access is not allowed via a network based login. This was confirmed via the `/etc/default/login` configuration file.

Only the UNIX administration team has access to the root password. This limits the privileged password to five individuals within the organization. Application and Database administrators do not have access to the root password and utilize user and group level permissions to obtain the necessary level of access. On a limited basis the “sudo” command is used to provide a level of access that cannot be obtained via user and group level permissions. SUDO allows these groups of individuals to run specific commands which will be executed with the privileges of the root user.

The GIAC Information Security Policy has defined that all user and administrator passwords must expire within 90 days. These policies have not been implemented on the UNIX servers to date. See [Appendix C – UnixAudit.sh](#) for a copy of the `/etc/default/passwd` file as well as the `/etc/shadow` file which shows that the password expiration fields have not been configured.

MAW Security Solutions ran password cracking utility called John the Ripper ([Appendix C – John](#)) against the users and passwords in the `/etc/shadow` file to attempt to brute force crack passwords. This test was performed in conjunction with the GIAC UNIX system administrators. No passwords were cracked via this utility during the audit. Weak passwords are often an attacker’s first method of entry into a system. A password cracking utility should be run on a regular basis to identify weak user passwords. This utility will help the Information Security team assess the level of secure password selection within the organization and address as necessary.

There are no host based access controls in place to further authenticate and restrict network communications. Even though GIAC has implemented network based firewalls to restrict connections to the Sun Solaris servers in the DMZ, it would be recommended to improve on this model by creating and deploying host based access control lists. A product such as TCPWRAPPERS could be utilized to protect services running from the Sun INET daemon. The TCPWRAPPERS software will allow the system administrator to control which network IP addresses can connect to specific INETD services and will provide increased logging of these connections. Sun Solaris 8 TCPWAPPERS can be downloaded from <http://www.sunfreeware.com>.

In addition to TCPWRAPPERS a host based firewall such as `ipfilter` should be considered to further protect the UNIX systems. This host-based firewall would be configured in conjunction with the network firewall and will provide an

additional layer of defense to protect the UNIX system against un-trusted individuals.

### ***Backup Policies and Disaster Preparedness***

Veritas NetBackup Datacenter is being utilized to perform the UNIX system backups. All UNIX servers have a full system backup completed each weekend. Incremental backups are completed on a nightly basis. The weekly full backups are removed from the tape library on Monday and taken to a fire protective safe in a satellite office building. These backup tapes are re-used after a period of three months. On the first Monday of each month a copy of the completed full backup tapes are made and are stored permanently off-site.

Several procedures have been documented to identify the backup schedule as well as the recovery procedure. Random test restores are completed on a monthly basis and a full system restore is tested and documented every 6 months for critical servers within the GIAC infrastructure.

### ***Other Issues***

One issue that came up several times during the staff interviews was security training and awareness. The UNIX system administration team is comfortable supporting the UNIX servers that they manage, but do not feel that they have had an adequate level of security training to properly build and administer the servers in a secure manner. There is also concern that the administrators would be unable to identify and respond to a security incident if one were to occur. Ongoing security training of the UNIX team is essential to providing and maintaining a secure UNIX environment at GIAC.

Security Awareness throughout the organization is a large issue. Several policies and procedures have been identified by the Information Security Department, but are not well associated throughout the organization. A considerable amount of employees at GIAC were unaware that a corporate wide Information Security Policy even existed. A security awareness program should be created and thoroughly associated amongst all employees at GIAC.

## Critical Issues and Recommendations

---

The following items have been identified as the top 10 issues within the GIAC environment. These issues have been prioritized in the order that they should be remediated with the most extreme issues being as identified first.

### ***Top 10 Issues Identified***

1. Security Awareness – GIAC needs to spend a considerable amount of time building an environment where Security is at the forefront of every employees mind. This is holds true for the receptionist to the CEO. By creating an environment such as this, every employee will understand why certain security policies and procedures have been put in place and will not be so apt to be confrontational as new security policies are published. This type of environment will allow employees to question practices that seem awry and possibly catch or thwart a social engineering attack against the assets of the company.
2. UNIX Security Training – The UNIX administrators have made it clear that they have the skills required to manage a UNIX server, but do not necessarily have the security training required to “securely” manage this same UNIX server. Security changes to a UNIX system can often impact the administrators and/or user community and need to be fully understood before implementing. The proper training of the UNIX Administration team will ensure that the security aspects of a given UNIX service are considered each and every time something new is implemented. This training will allow the administration team to properly evaluate and implement security changes as necessary. Training will also ensure that the UNIX administration team has the tools to identify and react to security incidents should they occur.
3. Unnecessary Services & Software – Several unnecessary services and software packages were identified on the audited Sun Solaris machine. Each service running on the UNIX server can be used as a possible avenue of attack. Minimizing these services to the smallest set required for normal server operation will mitigate this concern. Unnecessary server software can also be used by an attacker to further a system attack. Only the smallest subset of system software required for normal operation should be installed.
4. Clear-text protocols – Several clear text protocols (Telnet, Rlogin, and FTP) are being used to remotely administer the UNIX servers at GIAC. These protocols can easily be migrated to a secure replacement such as SSH. This migration can be done at a minimum cost to GIAC and requires minimal training and configuration changes to implement. The SSH replacement should be completed immediately for the UNIX

administration team and user accounts should follow as a second phase to the implementation plan.

5. System File and Binary Integrity – GIAC system administrators currently have some in-house written scripts to monitor sensitive system files and binaries for unauthorized modification. An automated tool such as tripwire should be evaluated and implemented on all UNIX servers at GIAC. This tool will greatly expand on what GIAC already has in place and can be the key to identifying a system attack shortly after it has happened.
6. Centralized Off-Host Audit Log Storage – As per the GIAC Information Security Policy UNIX audit logs must be configured and stored on an off-host system. This industry standard practice must be completed to comply with GIAC policies.
7. Log Review Procedures – GIAC administrators must create and follow a log review procedure. This procedure should detail how often logs are reviewed, what log events are considered normal for a particular host and how to identify exceptions. The policy should detail how exceptions are handled within the UNIX group and when proper notification and escalation should be made to the information security group.
8. Password Expiration Policies – As per the GIAC Information Security Policy, password expiration rules need to be implemented on the UNIX servers.
9. Authorized-Use Banners – As per the GIAC Information Security Policy Authorized-Use Banners need to be implemented for all services that allow such a facility. Authorized-Use banners will help GIAC in the event that prosecution of a criminal event needs to be completed.
10. Host-Based Access Control Restrictions – Additional host based access control restrictions should be implemented on the UNIX servers at GIAC to further restrict access to services on the UNIX server. Services such as SSH allow for host based access control restrictions in the daemon configuration file, whereas services that run from the INET daemon (inetd) can be properly secured with a tool such as TCPWRAPPERS. A host based firewall package may be considered to further protect the UNIX servers and applications.

### ***Other Recommendations***

In addition to the Top 10 recommendations listed above the following two items are recommended for review by GIAC.



First, it is recommend that the GIAC UNIX Administration team take the technical recommendations from this document and apply to all UNIX servers at the organization. In addition to applying these recommendations to all current production servers these changes should be implemented on the GIAC Sun Solaris Jumpstart Server. This will ensure that all new UNIX servers that are built at GIAC will adhere to the recommendations of this document. Further documentation can be found at [sunsolve.sun.com](http://sunsolve.sun.com) regarding Securing Solaris Installations.

Second, the Information Security team at GIAC should tasks with an internal auditing function. At this time Information Security team has been tasked with creating written security policies and procedures, but no auditing is being completed to make certain the production operations teams properly implement these policies.

© SANS Institute 2004, Author retains full rights.

## Appendix A – System Description

### Hardware

```
#psrinfo -v
Status of processor 0 as of: 02/13/04 15:40:17
  Processor has been on-line since 02/12/04 15:31:09.
  The sparcv9 processor operates at 1062 MHz,
    and has a sparcv9 floating point processor.
Status of processor 1 as of: 02/13/04 15:40:17
  Processor has been on-line since 02/12/04 15:31:08.
  The sparcv9 processor operates at 1062 MHz,
    and has a sparcv9 floating point processor.

# prtconf | grep "Memory size:"
Memory size: 8192 Megabytes

#format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
  0. clt0d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
    /pci@1f,700000/scsi@2/sd@0,0
  1. clt1d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
    /pci@1f,700000/scsi@2/sd@1,0
  2. clt2d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
    /pci@1f,700000/scsi@2/sd@2,0
  3. clt3d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
    /pci@1f,700000/scsi@2/sd@3,0
  4. c3t0d0 <DGC-RAID10-0849 cyl 32766 alt 2 hd 32 sec 12>
    /pci@1c,600000/lpfc@1/sd@0,0
  5. c3t0d1 <DGC-RAID5-0849 cyl 61438 alt 2 hd 256 sec 12>
    /pci@1c,600000/lpfc@1/sd@0,1
  6. c3t0d2 <DGC-RAID5-0849 cyl 53246 alt 2 hd 256 sec 16>
    /pci@1c,600000/lpfc@1/sd@0,2
  7. c3t1d0 <DGC-RAID10-0849 cyl 32766 alt 2 hd 32 sec 12>
    /pci@1c,600000/lpfc@1/sd@1,0
  8. c3t1d1 <DGC-RAID5-0849 cyl 61438 alt 2 hd 256 sec 12>
    /pci@1c,600000/lpfc@1/sd@1,1
  9. c3t1d2 <DGC-RAID5-0849 cyl 53246 alt 2 hd 256 sec 16>
    /pci@1c,600000/lpfc@1/sd@1,2
 10. c4t0d0 <DGC-RAID10-0849 cyl 32766 alt 2 hd 32 sec 12>
    /pci@1d,700000/lpfc@1/sd@0,0
 11. c4t0d1 <DGC-RAID5-0849 cyl 61438 alt 2 hd 256 sec 12>
    /pci@1d,700000/lpfc@1/sd@0,1
 12. c4t0d2 <DGC-RAID5-0849 cyl 53246 alt 2 hd 256 sec 16>
    /pci@1d,700000/lpfc@1/sd@0,2
 13. c4t1d0 <DGC-RAID10-0849 cyl 32766 alt 2 hd 32 sec 12>
    /pci@1d,700000/lpfc@1/sd@1,0
 14. c4t1d1 <DGC-RAID5-0849 cyl 61438 alt 2 hd 256 sec 12>
    /pci@1d,700000/lpfc@1/sd@1,1
 15. c4t1d2 <DGC-RAID5-0849 cyl 53246 alt 2 hd 256 sec 16>
    /pci@1d,700000/lpfc@1/sd@1,2

# vxdisk list
DEVICE      TYPE      DISK      GROUP      STATUS
c1t0d0s2    sliced    rootmirror rootdg      online
c1t1d0s2    sliced    rootdisk  rootdg      online
c1t2d0s2    sliced    -         -          error
c1t3d0s2    sliced    -         -          error
c3t0d0s2    sliced    vgora03_01 vgora03    online nohotuse
c3t0d1s2    sliced    vgora01_01 vgora01    online nohotuse
c3t0d2s2    sliced    vgora02_01 vgora02    online nohotuse
```

## Software

```
# uname -a
SunOS giacunixhost 5.8 Generic_108528-27 sun4u sparc SUNW,Sun-Fire-V440

# more /var/sadm/install_data/Solaris_8_Recommended_log
*** Install Solaris 8 Recommended begins Tue Jan 13 11:24:24 EST 2004 ***
*** PATCHDIR = /home/jdoe/Installdir/8_Recommended ***

Installing 110380-04...

Checking installed patches...
Patch 110380-04 has already been applied.
See patchadd(1M) for instructions.

Patchadd is terminating.
Installing 110934-14...

Checking installed patches...
Verifying sufficient filesystem capacity (dry run method)...
Installing patch packages...

Patch number 110934-14 has been successfully installed.

<cut remaining log information>

#pkginfo -l VRTSvxvm
PKGINST: VRTSvxvm
NAME: VERITAS Volume Manager, Binaries
CATEGORY: system
ARCH: sparc
VERSION: 3.5,REV=06.21.2002.23.14
BASEDIR: /
VENDOR: VERITAS Software
DESC: Virtual Disk Subsystem
PSTAMP: VERITAS-3.5s_p1.7:06-Dec-2002
INSTDATE: Jan 13 2004 15:05
HOTLINE: 800-342-0652
EMAIL: support@veritas.com
STATUS: partially installed
FILES: 603 installed pathnames
       22 shared pathnames
       9 linked files
       78 directories
       337 executables
       160090 blocks used (approx)

# cat /usr/opensv/netbackup/bin/version
NetBackup-Solaris2.6 4.5FP_5
```

## Appendix B – Detailed Analysis

### OS Vulnerabilities – Patchdiag v1.04 output

```
=====
System Name: giacunixhost      SunOS Vers: 5.8      Arch: sparc
Cross Reference File Date: Feb/17/04
```

```
PatchDiag Version: 1.0.4
=====
```

#### Report Note:

Recommended patches are considered the most important and highly recommended patches that avoid the most critical system, user, or security related bugs which have been reported and fixed to date. A patch not listed on the recommended list does not imply that it should not be used if needed. Some patches listed in this report may have certain platform specific or application specific dependencies and thus may not be applicable to your system. It is important to carefully review the README file of each patch to fully determine the applicability of any patch with your system.

#### INSTALLED PATCHES

Patch ID	Installed Revision	Latest Revision	Synopsis
108434	13	14	SunOS 5.8: 32-Bit Shared library patch for C++
108435	13	14	SunOS 5.8: 64-Bit Shared library patch for C++
108528	27	29	SunOS 5.8: kernel update patch
108569	08	CURRENT	X11 6.4.1: platform support for new hardware
108609	01	CURRENT	SunOS 5.8: Buttons/Dials Patch
108623	03	CURRENT	SunOS 5.8: Thai Wordbreak Iterator module
108652	76	78	X11 6.4.1: Xsun patch
108714	08	CURRENT	CDE 1.4: libDtWidget patch
108723	01	CURRENT	SunOS 5.8: /kernel/fs/lofs and /kernel/fs/sparcv9/lofs patch
108725	14	15	SunOS 5.8: st driver patch
108727	26	CURRENT	SunOS 5.8: /kernel/fs/nfs and /kernel/fs/sparcv9/nfs patch
108773	17	18	SunOS 5.8: IIIM and X Input & Output Method patch
108806	17	CURRENT	SunOS 5.8: Sun Quad FastEthernet qfe driver
108808	43	CURRENT	SunOS 5.8: Manual Page updates for Solaris 8
108813	12	16	SunOS 5.8: Sun Gigabit Ethernet 3.0
108820	01	02	SunOS 5.8: nss_compat.so.1 patch
108823	01	CURRENT	SunOS 5.8: compress/uncompress/zcat patch
108835	04	CURRENT	CDE 1.4: dtcm patch
108869	22	CURRENT	SunOS 5.8: snmpdx/mibiisa/libssasnmplib patch
108897	01	CURRENT	X11 6.4.1 Xprint patch
108899	04	CURRENT	SunOS 5.8: /usr/bin/ftp patch
108901	06	08	Obsoleted by: 108528-24 SunOS 5.8: /kernel/sys/rpcmod and /kernel/
108909	13	CURRENT	CDE 1.4: Smart Card Administration GUI patch
108919	20	CURRENT	CDE 1.4: dtlogin patch
108921	16	19	CDE 1.4: dtwm patch
108923	01	CURRENT	CDE 1.4: dtwm audio control patch
108940	52	60	Motif 1.2.7 and 2.1.1: Runtime library patch for Solaris 8
108949	07	08	CDE 1.4: libDtHelp/libDtSvc patch
108962	01	CURRENT	SunOS 5.8: XmlReader fails on an HTTP stream
108964	06	CURRENT	SunOS 5.8: /usr/sbin/in.tftpd and /usr/sbin/snoop patch
108968	08	09	SunOS 5.8: vol/vold/rmmount/dev_pcmem.so.1 patch
108970	01	CURRENT	SunOS 5.8: /usr/lib/fs/pcfs/fsck and /usr/lib/fs/pcfs/mkfs patch
108972	04	CURRENT	SunOS 5.8: /sbin/fdisk patch
108974	37	CURRENT	SunOS 5.8: dada, uata, dad, sd, ssd and scsi drivers patch
108975	08	CURRENT	SunOS 5.8: /usr/bin/rmformat and /usr/sbin/format patch
108977	02	CURRENT	SunOS 5.8: libsmmedia patch
108981	13	CURRENT	SunOS 5.8: /kernel/drv/hme and /kernel/drv/sparcv9/hme patch
108982	09	10	WITHDRAWN PATCH SunOS 5.8: fctl/fp/fcp/usoc driver patch
108983	08	CURRENT	SunOS 5.8: /kernel/drv/fcip driver patch
108984	08	CURRENT	SunOS 5.8: /kernel/drv/qlc driver patch

108985	03	CURRENT	SunOS 5.8: /usr/sbin/in.rshd patch
108987	13	CURRENT	SunOS 5.8: Patch for patchadd and patchrm
108989	02	CURRENT	SunOS 5.8: /usr/kernel/sys/acctctl and
/usr/kernel/sys/exacctsys p			
108993	31	CURRENT	SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries
patch			
108995	04	06	SunOS 5.8: /usr/lib/libproc.so.1 patch
108997	03	CURRENT	Obsoleted by: 108993-31 SunOS 5.8: libexacct and libproject
patch			
108999	01	CURRENT	SunOS 5.8: PAM patch
109003	01	CURRENT	SunOS 5.8: /etc/init.d/acctadm and /usr/sbin/acctadm patch
109005	05	CURRENT	Obsoleted by: 108993-31 SunOS 5.8: /sbin/su.static and
/usr/bin/su			
109007	13	15	SunOS 5.8: at/atrm/batch/cron patch
109009	02	CURRENT	SunOS 5.8: /etc/magic and /usr/bin/file patch
109011	01	CURRENT	SunOS 5.8: /usr/bin/id and /usr/xpg4/bin/id patch
109013	02	CURRENT	SunOS 5.8: /usr/bin/lastcomm patch
109015	01	CURRENT	SunOS 5.8: /usr/bin/newtask patch
109017	01	CURRENT	SunOS 5.8: /usr/bin/pgrep and /usr/bin/pkill patch
109019	02	CURRENT	SunOS 5.8: /usr/bin/priocntl patch
109021	01	CURRENT	SunOS 5.8: /usr/bin/projects patch
109023	01	02	SunOS 5.8: /usr/bin/sparcv7/ps and /usr/bin/sparcv9/ps patch
109025	04	05	SunOS 5.8: /usr/bin/sparcv7/truss and /usr/bin/sparcv9/truss
patch			
109027	01	CURRENT	SunOS 5.8: /usr/bin/wracct patch
109029	02	CURRENT	SunOS 5.8: perl patch
109031	01	CURRENT	SunOS 5.8: projadd/projdel/projmod patch
109033	01	CURRENT	SunOS 5.8: /usr/bin/sparcv7/prstat and /usr/bin/sparcv9/prstat
pat			
109035	02	03	SunOS 5.8: useradd/userdel/usermod patch
109037	01	CURRENT	SunOS 5.8: /var/yp/Makefile and /var/yp/nicknames patch
109043	02	CURRENT	SunOS 5.8: sonode adb macro patch
109045	03	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: /usr/sbin/sparcv7/crash and
/us			
109077	13	14	SunOS 5.8: dhcp server and admin patch
109091	06	CURRENT	SunOS 5.8: /usr/lib/fs/ufs/ufsrestore patch
109128	01	CURRENT	SunOS 5.8: Provide conversion between codepages 1256 and
ISO8859-6			
109134	28	CURRENT	SunOS 5.8: WBEM patch
109142	06	07	CDE 1.4: dtterm libDtTerm patch
109145	01	CURRENT	SunOS 5.8: /usr/sbin/in.routed patch
109147	27	CURRENT	SunOS 5.8: linker patch
109149	02	CURRENT	SunOS 5.8: /usr/sbin/mkdevmaps and /usr/sbin/mkdevalloc patch
109152	02	CURRENT	SunOS 5.8: /usr/4lib/libc.so.x.9 and libdbm patch
109159	03	CURRENT	SunOS 5.8: Chinese iconv module updates
109165	13	14	CDE 1.4: dtfile patch
109167	01	CURRENT	CDE 1.4: Desktop Help Updates Patch
109169	12	CURRENT	CDE 1.4: Window Manager Enhancements Patch
109202	05	CURRENT	SunOS 5.8: /kernel/misc/gld and /kernel/misc/sparcv9/gld patch
109223	04	CURRENT	SunOS 5.8: kpasswd, libgss.so.1 and libkadm5clnt.so.1 patch
109234	09	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: Apache Security and NCA
Patch			
109238	02	CURRENT	SunOS 5.8: /usr/bin/sparcv7/ipcs and /usr/bin/sparcv9/ipcs
patch			
109244	02		
109277	03	CURRENT	SunOS 5.8: /usr/bin/iostat patch
109318	34	CURRENT	SunOS 5.8: suninstall Patch
109320	08	09	SunOS 5.8: LP Patch
109324	05	CURRENT	SunOS 5.8: sh/jsh/rsh/pfsh patch
109326	12	13	SunOS 5.8: libresolv.so.2 and in.named patch
109328	03	CURRENT	SunOS 5.8: ypserve, ypxfr and ypxfrd patch
109354	19	CURRENT	CDE 1.4: dtsession patch
109384	06	10	SunOS 5.8: libaio patch
109454	01	02	SunOS 5.8: /kernel/fs/fifofs and /kernel/fs/sparcv9/fifofs
patch			
109458	03	CURRENT	SunOS 5.8: /kernel/strmod/ldterm patch
109460	09	10	SunOS 5.8: social and sf drivers patch
109463	01	CURRENT	OpenWindows 3.6.2: Filemgr Patch
109470	02	CURRENT	CDE 1.4: Actions Patch
109529	06	CURRENT	SunOS 5.8: luxadm, liba5k and libg_fc patch
109568	03	CURRENT	OpenWindows 3.6.2: sys-suspend need to support low power mode

109569	01	CURRENT	OpenWindows 3.6.2: imagetool patch
109576	01	CURRENT	SunOS 5.8: mountall and fsckall patch
109582	02	CURRENT	CDE 1.4: sdtaudio patch
109607	02	CURRENT	SunOS 5.8: /usr/include/iso/stdlib_iso.h patch
109613	06	CURRENT	CDE 1.4: dtmail patch
109639	02	CURRENT	Obsoleted by: 111188-02 SunOS 5.8: th locale has errors in / lacks
109642	01	CURRENT	SunOS 5.8: /usr/include/sys/dkio.h patch
109657	09	CURRENT	SunOS 5.8: isp driver patch
109667	05	CURRENT	SunOS 5.8: /usr/lib/inet/xntpd and /usr/sbin/ntpdate patch
109679	01	CURRENT	SunOS 5.8: /usr/share/lib/smartcard/ibutton.jar patch
109695	03	CURRENT	SunOS 5.8: /etc/smartcard/opencard.properties patch
109704	02	03	SunOS 5.8: Japanese iconv patch
109727	01	CURRENT	SunOS 5.8: /usr/sadm/admin/printmgr/classes/pmclient.jar patch
109729	01	CURRENT	SunOS 5.8: /usr/bin/cat patch
109748	03	CURRENT	CDE 1.4: sdtaudiocontrol patch
109764	04	CURRENT	SunOS 5.8: /kernel/fs/hsfs and /kernel/fs/sparcv9/hsfs patch
109766	02	CURRENT	SunOS 5.8: SUNWjxmft and SUNWjxcft patch for 8/10 dot font.
109778	13	14	SunOS 5.8: Misc loc have errors in CTYPE and lv colln monetary
109783	02	CURRENT	SunOS 5.8: /usr/lib/nfs/nfsd and /usr/lib/nfs/lockd patch
109785	01	CURRENT	SunOS 5.8: /etc/inittab patch
109793	23	CURRENT	SunOS 5.8: su driver patch
109803	01	CURRENT	SunOS 5.8: /usr/bin/du and /usr/xpg4/bin/du patch
109805	17	CURRENT	SunOS 5.8: /usr/lib/security/pam_krb5.so.1 patch
109807	01	CURRENT	SunOS 5.8: /usr/sbin/dumpadm patch
109809	01	CURRENT	SunOS 5.8: timezone data patch for Australasia
109813	01	CURRENT	SunOS 5.8: /usr/include/memory.h patch
109815	20	CURRENT	SunOS 5.8: se, acebus, pcf8574, pcf8591 and scsb patch
109862	03	CURRENT	X11 6.4.1 Font Server patch
109872	01	CURRENT	SunOS 5.8: vis driver patch
109873	22	CURRENT	SunOS 5.8: prtdiag and platform libprtdiag_psr.so.1 patch
109876	02	CURRENT	SunOS 5.8: fd driver patch
109877	01	CURRENT	SunOS 5.8: /usr/include/sys/dma_i8237A.h patch
109879	02	CURRENT	SunOS 5.8: isadma driver patch
109881	02	CURRENT	SunOS 5.8: 1394 adb macros patch
109882	06	CURRENT	SunOS 5.8: eri header files patch
109883	02	CURRENT	SunOS 5.8: /usr/include/sys/ecppsys.h patch
109885	14	CURRENT	SunOS 5.8: glm patch
109887	18	CURRENT	SunOS 5.8: smartcard and usr/sbin/ocfserv patch
109888	26	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: platform drivers patch
109889	06	07	SunOS 5.8: usr platform links and libc_psr patch
109890	01	CURRENT	SunOS 5.8: pmserver.jar patch
109892	04	CURRENT	SunOS 5.8: /kernel/drv/sparcv9/ecpp patch
109893	04	CURRENT	SunOS 5.8: stc driver patch
109894	01	CURRENT	SunOS 5.8: /kernel/drv/sparcv9/bpp driver patch
109896	22	24	SunOS 5.8: USB and Audio Framework patch
109898	05	CURRENT	SunOS 5.8: /kernel/drv/arp patch
109900	02	03	SunOS 5.8: /etc/init.d/network and /sbin/ifparse patch
109902	03	CURRENT	SunOS 5.8: /usr/lib/inet/in.ndpd patch
109920	08	09	SunOS 5.8: pcic and busra driver patch
109922	04	CURRENT	SunOS 5.8: pcelx and pcser driver patch
109924	04	CURRENT	SunOS 5.8: pcata driver patch
109928	05	CURRENT	SunOS 5.8: pcmem and pcmcia patch
109931	05	06	CDE 1.4: sdtimage Patch
109933	01	02	SunOS 5.8: mv, cp, ln patch
109936	01	CURRENT	SunOS 5.8: /usr/bin/diff patch
109960	01	CURRENT	CDE 1.4: sdtperfmeter patch
109990	01	CURRENT	SunOS 5.8: /usr/ccs/bin/dis patch
109994	01	02	SunOS 5.8: /usr/bin/sparcv7/adb and /usr/bin/sparcv9/adb patch
110068	04	CURRENT	CDE 1.4: PDASync patch
110075	01	CURRENT	SunOS 5.8: /kernel/drv/devinfo and /kernel/drv/sparcv9/devinfo pat
110088	02	CURRENT	CDE 1.4: DtPower patch
110127	04	CURRENT	SunOS 5.8: Generic Framebuffer configuration Graphics Patch
110165	04	CURRENT	SunOS 5.8: /usr/bin/sed patch
110208	13	18	Netra Lights Out Management 2.0 patch
110221	07	CURRENT	SunOS 5.8: Dcam1394 patch
110269	01	CURRENT	SunOS 5.8: /usr/lib/libnisdb.so.2 patch
110283	06	CURRENT	SunOS 5.8: mkfs and newfs patch
110285	01	02	SunOS 5.8: consconfig_dacf patch
110286	11	CURRENT	OpenWindows 3.6.2: Tooltalk patch

110320	03	CURRENT	SunOS 5.8: /kernel/misc/sparcv9/s1394 patch
110322	02	CURRENT	SunOS 5.8: /usr/lib/netsvc/yp/ypbind patch
110326	02	CURRENT	CDE 1.4: dtstyle patch
110335	03	CURRENT	CDE 1.4: dtprintinfo patch
110368	02	CURRENT	SunOS 5.8: pcf8574 driver patch for SUNW Sun-Fire-280R
110369	05	CURRENT	SunOS 5.8: sgc9 patch
110370	03	CURRENT	SunOS 5.8: SUNW,Sun-Fire usr platform links patch
110371	03	CURRENT	SunOS 5.8: serengeti support, Update3, sgfru patch
110373	04	05	SunOS 5.8: /platform/SUNW,Sun-Fire/kernel/drv/sparcv9/sgsbcc patch
110374	08	CURRENT	SunOS 5.8: /platform/SUNW,Sun-Fire/kernel/drv/sparcv9/sgenv patch
110375	05	CURRENT	SunOS 5.8: /platform/SUNW,Sun-Fire/kernel/drv/sparcv9/ssm patch
110376	01	CURRENT	SunOS 5.8: littleneck support, usr platform patch, S8 Update 3
110378	06	CURRENT	SunOS 5.8: mipagent patch Mobile IP
110379	01	CURRENT	SunOS 5.8: littleneck support, gpio patch
110380	04	CURRENT	SunOS 5.8: ufssnapshots support, libadm patch
110381	01	CURRENT	SunOS 5.8: ufssnapshots support, clri patch
110382	02	04	SunOS 5.8: ufssnapshots support, fssnap kernel, S8 Update 3
110385	03	04	SunOS 5.8: RCM modules patch
110386	03	CURRENT	SunOS 5.8: RBAC Feature Patch
110387	05	CURRENT	SunOS 5.8: ufssnapshots support, ufsdump patch
110388	01	CURRENT	SunOS 5.8: RBAC Feature for Solaris Update 3
110389	05	CURRENT	SunOS 5.8: cvc CPU signature
110394	01	CURRENT	SunOS 5.8:German Euro locale appears different than any other loca
110407	02	CURRENT	CDE 1.4 Sdttypes patch
110423	03		
110453	04	CURRENT	SunOS 5.8: admintool Patch
110457	05	CURRENT	SunOS 5.8: scmi2c driver patch
110458	02	CURRENT	SunOS 5.8: libcurses patch
110460	32	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: fruid/PICL plug-ins patch
110461	03	CURRENT	SunOS 5.8: ttcompat patch
110511	05	CURRENT	SunOS 5.8: rpc.nisd patch
110603	01	CURRENT	CDE 1.4: sdtname patch
110605	02	CURRENT	Motif 2.1.1: uil patch for Solaris 8
110609	04	CURRENT	SunOS 5.8: cdio.h and command.h USB header patch
110611	01	CURRENT	SunOS 5.8: lp.cat and postio ECP patch
110614	02	CURRENT	SunOS 5.8: ses driver patch
110615	10	CURRENT	SunOS 5.8: sendmail patch
110662	12	CURRENT	SunOS 5.8: ksh patch
110668	04	CURRENT	SunOS 5.8: /usr/sbin/in.telnetd patch
110670	01	CURRENT	SunOS 5.8: usr/sbin/static/rcp patch
110702	01	CURRENT	SunOS 5.8: mknetid patch
110710	01	CURRENT	SunOS 5.8: nsd patch
110716	02	CURRENT	SunOS 5.8: Solaris Product Registry 3.0 patch
110722	03	CURRENT	AP 2.3.1: AP needs to provide interface for Veritas DMP compatibil
110723	06	07	SunOS 5.8: /kernel/drv/sparcv9/eri patch
110724	01	CURRENT	SunOS 5.8: liblayout patch
110750	01	CURRENT	SunOS 5.8: TCX Graphics Patch
110811	01	CURRENT	SunOS 5.8: libnls patch
110813	01	CURRENT	SunOS 5.8: libxfn patch
110815	01	CURRENT	SunOS 5.8: libmp patch
110817	01	CURRENT	SunOS 5.8: apptrace and interceptors patch
110819	04	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: /platform/sun4u/kernel/drv/spar
110820	10	CURRENT	SunOS 5.8: /platform/SUNW,Sun-Fire-15000/kernel/drv/sparcv9/dman p
110821	02	CURRENT	SunOS 5.8: iosram driver patch
110822	01	CURRENT	SunOS 5.8: mboxsc driver patch
110826	07	09	SunOS 5.8: platform/SUNW,Sun-Fire-15000/kernel/drv/sparcv9/schpc p
110827	02	CURRENT	Obsoleted by: 108528-24 SunOS 5.8: scosmb driver patch
110828	02	CURRENT	SunOS 5.8: sbbc driver patch
110829	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/tod/sparcv9/todstarcats patch
110833	01	CURRENT	SunOS 5.8: usr platform links
110838	06	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: /platform/SUNW,Sun-Fire-15000/k
110839	03	04	SunOS 5.8: /usr/lib/rcm/modules/SUNW_ip_rcm.so patch
110840	03	CURRENT	SunOS 5.8: bbc patch

110841	01	CURRENT	SunOS 5.8: gptwo patch
110842	11	CURRENT	SunOS 5.8: hpc3130 driver patch for SUNW,Sun-Fire-880
110844	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/lm75 patch
110845	03	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/lm75 patch
110846	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/pcf8574 patch
110847	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/pcf8591 patch
110849	13	15	Obsoleted by: 109873-22 SunOS 5.8: PICL support for SUNW,Sun-Fire-
110851	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/ssc050 patch
110852	03	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/ssc100 patch
110853	01	CURRENT	SunOS 5.8: SUNW,Sun-Fire-880 usr platform links patch
110854	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/smbus_ara patch
110856	01	CURRENT	SunOS 5.8: /etc/inet/services patch
110896	02	CURRENT	SunOS 5.8: cacheefs/mount patch
110898	08	09	SunOS 5.8: csh/pfcsh patch
110901	01	CURRENT	SunOS 5.8: /kernel/drv/sngen and /kernel/drv/sparcv9/sngen patch
110903	07	CURRENT	SunOS 5.8: edit, ex, vedit, vi and view patch
110905	02	CURRENT	SunOS 5.8: /usr/bin/find patch
110907	01	CURRENT	SunOS 5.8: /usr/include/arpa/inet.h patch
110910	01	02	SunOS 5.8: /usr/lib/fs/ufs/fsck patch
110912	03	04	SunOS 5.8: cfgadm patch
110914	01	CURRENT	SunOS 5.8: /usr/bin/tr patch
110916	05	CURRENT	SunOS 5.8: sort patch
110918	06	CURRENT	SunOS 5.8: /kernel/drv/openeep and prtconf patch
110927	01	CURRENT	SunOS 5.8: Need to backport fixes in SUNW_PKGLIST in s8u4
110934	14	CURRENT	SunOS 5.8: pkgtrans, pkgadd, pkgchk, pkgmk and libpkg.a patch
110939	01	CURRENT	SunOS 5.8: /usr/lib/acct/closewtmp patch
110941	03	CURRENT	SunOS 5.8: sar and sadc patch
110943	02	CURRENT	SunOS 5.8: /usr/bin/tcsh patch
110945	08	CURRENT	SunOS 5.8: /usr/sbin/syslogd patch
110951	05	CURRENT	SunOS 5.8: /usr/sbin/tar and /usr/sbin/static/tar patch
110953	06	CURRENT	SunOS 5.8: /usr/kernel/drv/llc2 patch
110955	04	CURRENT	SunOS 5.8: /kernel/strmod/timod patch
110957	02	CURRENT	SunOS 5.8: /usr/bin/mailx patch
110986	02	CURRENT	SunOS 5.8: SMC help fix
111016	01	CURRENT	SunOS 5.8: /usr/bin/sdiff patch
111018	01	CURRENT	SunOS 5.8: /etc/driver_aliases patch for gpio
111023	03	CURRENT	SunOS 5.8: /kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch
111069	01	CURRENT	SunOS 5.8: bsmunconv overwrites root cron tab if cu created
/tmp/r			
111071	01	CURRENT	SunOS 5.8: cu patch
111073	01	CURRENT	SunOS 5.8: re_comp header patch
111075	02	03	X11 6.4.1: keyboards patch
111088	02	CURRENT	Obsoleted by: 108995-06 SunOS 5.8: mdb patch
111095	14	CURRENT	SAN 4.3: fctl/fp/fcp/usoc driver patch
111098	01	CURRENT	SunOS 5.8: ROC timezone should be avoided for political reasons
111111	03	CURRENT	SunOS 5.8: /usr/bin/nawk patch
111141	02	03	SunOS 5.8: /usr/bin/last patch
111197	02	CURRENT	SunOS 5.8: /usr/lib/nfs/mountd patch
111225	02	CURRENT	SunOS 5.8: /usr/bin/tail and /usr/xpg4/bin/tail patch
111231	04	CURRENT	SunOS 5.8: Solaris user registration patch
111232	01	CURRENT	SunOS 5.8: patch in.fingerd
111234	01	CURRENT	SunOS 5.8: patch finger
111265	01	CURRENT	SunOS 5.8: patch who
111269	03	CURRENT	SunOS 5.8: Solaris Management Console patch
111295	01	CURRENT	SunOS 5.8: /usr/bin/sparcv7/pstack & /usr/bin/sparcv9/pstack patch
111297	01	CURRENT	SunOS 5.8: /usr/lib/libsendfile.so.1 patch
111302	02	CURRENT	SunOS 5.8: EDHCP libraries patch
111304	01	CURRENT	SunOS 5.8: /kernel/misc/nfs_dlboot patch
111306	04	05	SunOS 5.8: ufsboot and inetboot patch
111308	03	04	SunOS 5.8: /usr/lib/libmtmalloc.so.1 patch
111310	01	CURRENT	SunOS 5.8: /usr/lib/libdhcpageant.so.1 patch
111313	01	CURRENT	SunOS 5.8: Viper tools are very slow to load
111317	05	CURRENT	SunOS 5.8: /sbin/init and /usr/sbin/init patch
111319	01	CURRENT	SunOS 5.8: /usr/sbin/in.rdisc patch
111321	03	CURRENT	SunOS 5.8: klmmod and klmops patch
111323	01	CURRENT	SunOS 5.8: /usr/xpg4/bin/more patch
111325	02	CURRENT	SunOS 5.8: /usr/lib/saf/ttymon patch
111327	05	CURRENT	SunOS 5.8: libsocket patch
111368	01	CURRENT	SunOS 5.8: /usr/bin/groups patch



111382	01		
111400	01	02	SunOS 5.8: KCMS configure tool has a security vulnerability
111412	12	CURRENT	SAN 4.3: Sun StorEdge Traffic Manager patch
111413	11	CURRENT	SAN 4.3: luxadm, liba5k and libg_fc patch
111439	02	CURRENT	SunOS 5.8: /kernel/fs/tmpfs patch
111471	04	05	SunOS 5.8: Bug fixes for mp in asian locale printing bugs
111481	01	CURRENT	OpenWindows 3.6.2: clock Patch
111504	01	CURRENT	SunOS 5.8: /usr/bin/tip patch
111548	01	CURRENT	SunOS 5.8: catman, man, whatis, apropos and makewhatis patch
111562	02	CURRENT	SunOS 5.8: /usr/lib/librt.so.1 patch
111570	02	03	SunOS 5.8: uucp patch
111588	04	CURRENT	SunOS 5.8: /kernel/drv/ws and /kernel/fs/specfs patch
111596	03	CURRENT	SunOS 5.8: /usr/lib/netsvc/yp/rpc.yppasswdd patch
111606	04	CURRENT	SunOS 5.8: /usr/sbin/in.ftpd patch
111624	04	05	SunOS 5.8: /usr/sbin/inetd patch
111626	03	CURRENT	OpenWindows 3.6.2: Xview Patch
111697	04	CURRENT	SunOS 5.8: /usr/ccs/bin/sccs and /usr/ccs/bin/make patch
111721	03	04	SunOS 5.8: Math Library (libm) patch
111741	02	CURRENT	X11 6.4.1: hwc patch
111760	02		
111775	01	CURRENT	SunOS 5.8: smdiskless patch
111777	01	CURRENT	SunOS 5.8: smossservice patch
111791	01	CURRENT	SunOS 5.8: usr platform links patch for SUNW,Sun-Fire-480R
111792	09	CURRENT	SunOS 5.8: PICL plugins patch for SUNW,Sun-Fire-480R
111793	04	CURRENT	Obsoleted by: 109873-22 SunOS 5.8: libprtdiag_psr.so.1 patch
for S			
111794	02	CURRENT	SunOS 5.8: /usr/lib/libcpc.so.1 patch
111796	04	CURRENT	SunOS 5.8: Remote Shared Memory patch
111800	01	CURRENT	SunOS 5.8: /usr/include/sys/mhd.h patch
111802	01	02	SunOS 5.8: /usr/lib/rcm/modules/SUNW_cluster_rcm.so patch
111804	03	CURRENT	SunOS 5.8: /usr/sbin/rem_drv patch
111808	02	CURRENT	SunOS 5.8: /usr/lib/adb/devinfo patch
111822	01	CURRENT	SunOS 5.8: libpiclfrudata.conf patch for SUNW,Sun-Fire-480R
111826	01	CURRENT	SunOS 5.8: /usr/sbin/sparcv7/whodo & /usr/sbin/sparcv9/whodo
patch			
111831	01	CURRENT	SunOS 5.8: /usr/kernel/drv/dump patch
111844	02	CURRENT	X11 6.4.1 xdm patch
111847	01	08	SAN foundation kit patch
111852	01	CURRENT	SunOS 5.8: SX Graphics Patch
111874	06	CURRENT	SunOS 5.8: usr/bin/mail patch
111881	03	CURRENT	SunOS 5.8: /usr/kernel/strmod/telmod patch
111883	23	CURRENT	SunOS 5.8: Sun GigaSwift Ethernet 1.0 driver patch
111953	04	CURRENT	SunOS 5.8: zh_CN.GB18030 locale support
111958	02	CURRENT	SunOS 5.8: /usr/lib/nfs/statd patch
111989	01	CURRENT	SunOS 5.8: usr/bin/egrep patch
111995	06		
112001	08		
112003	03	CURRENT	SunOS 5.8: Unable to load fontset in 64-bit Solaris 8 iso-1 or
iso			
112034	03		
112036	02	CURRENT	SunOS 5.8: en_US.UTF-8 locale XI18N patch
112039	01	CURRENT	SunOS 5.8: usr/bin/ckitem patch
112050	01	03	SunOS 5.8: ptree patch
112077	07	09	SunOS 5.8: usr/kernel/drv/rsm patch
112082	02		
112097	02	05	SunOS 5.8: /usr/bin/cpio patch
112119	01	04	SunOS 5.8: vlan driver patch
112135	01	CURRENT	SunOS 5.8:: usr/lib/libmapmalloc.so.1 patch
112138	01	CURRENT	SunOS 5.8:: usr/bin/domainname patch
112142	01	CURRENT	SunOS 5.8: Configuration file fix for mp
112158	03	CURRENT	SunOS 5.8: patch SUNWhea header files
112159	02	CURRENT	SunOS 5.8: patch wrsm.so wrsmd.so
112160	01	CURRENT	SunOS 5.8: platform links SUNW,Netra-T12 SUNW,Netra-T4
112161	03	CURRENT	SunOS 5.8: remove libprtdiag_psr.so.1 of SUNW,Netra-T12
SUNW,Netra			
112162	03	CURRENT	SunOS 5.8: patch Netra T12 Lw8 driver
112163	01	CURRENT	SunOS 5.8: patch Netra T4 Lombus
112164	01	CURRENT	SunOS 5.8: patch Netra-T12 sgfru driver
112165	01	CURRENT	SunOS 5.8: patch usr/bin/rpcgen
112167	01	CURRENT	SunOS 5.8: patch usr/platform/SUNW,UltraAX-i2 symlink
112168	02	03	SunOS 5.8: patch dmfe and mii header file

112169	01	CURRENT	SunOS 5.8: patch platform/SUNW,UltraAX-i2/kernel/misc/sparcv9/plat
112170	02	CURRENT	SunOS 5.8: patch platform/sun4u/kernel/tod/sparcv9/todm5819
112171	01	CURRENT	SunOS 5.8: patch usr/sbin/locator
112187	01	CURRENT	SunOS 5.8: Jumpstart patch
112220	04	CURRENT	SunOS 5.8: kernel/misc/nfssrv patch
112237	09	CURRENT	SunOS 5.8: mech_krb5.so.1 patch
112249	04	CURRENT	Obsoleted by: 109873-22 SunOS 5.8: libprtdiag_psr.so.1
SUNW,Netra-			
112254	01	CURRENT	Obsoleted by: 108528-29 SunOS 5.8: /kernel/sched/TS patch
112274	01	02	SunOS 5.8: /usr/bin/acctcom patch
112325	01	CURRENT	SunOS 5.8: /kernel/fs/udfs and /kernel/fs/sparcv9/udfs patch
112328	02	CURRENT	SunOS 5.8: /usr/sbin/rpcbind patch
112345	03	CURRENT	SunOS 5.8: /usr/bin/pax patch
112369	01	CURRENT	SunOS 5.8: environ driver patch
112371	01	CURRENT	SunOS 5.8: /usr/bin/ruptime patch
112394	01	CURRENT	SunOS 5.8: Print euro and other ext. chars
112396	02	CURRENT	SunOS 5.8: /usr/bin/fgrep patch
112425	01	CURRENT	SunOS 5.8: /usr/lib/fs/ufs/mount and /etc/fs/ufs/mount patch
112438	01	02	SunOS 5.8: /kernel/drv/random patch
112459	01	CURRENT	SunOS 5.8: /usr/lib/pt_chmod patch
112472	01	CURRENT	SunOS 5.8: Font2DTest2 abort when Lucida Sans Thai Typewriter
sele			
112501	01	CURRENT	CDE 1.4: dtcreate patch
112597	01	03	SunOS 5.8: /usr/lib/acct/runacct patch
112607	02	CURRENT	SunOS 5.8: /usr/bin/on patch
112609	02	CURRENT	SunOS 5.8: /kernel/drv/le and /kernel/drv/sparcv9/le patch
112611	02	CURRENT	SunOS 5.8: /usr/lib/libz.so.1 patch
112663	01	02	X11 6.4.1: OWconfig patch
112666	01	CURRENT	SunOS 5.8: /usr/lib/acct/acctcon patch
112668	01	CURRENT	SunOS 5.8: /usr/bin/gzip patch
112670	01	CURRENT	SunOS 5.8: /usr/sbin/clinfo patch
112781	01	CURRENT	X11 6.4.1: twm patch
112796	01	CURRENT	SunOS 5.8: /usr/sbin/in.talkd patch
112798	01	CURRENT	SunOS 5.8: /usr/kernel/strmod/rmod patch
112844	02	CURRENT	SunOS 5.8: pfiles and plimit patch
112846	01	CURRENT	SunOS 5.8: /usr/lib/netsvc/rwall/rpc.rwalld patch
112850	01	CURRENT	SunOS 5.8: /kernel/drv/icmp6 and /kernel/drv/sparcv9/icmp6
Patch			
112989	01	CURRENT	SunOS 5.8: /usr/lib/print/conv_lpd patch
112991	01	CURRENT	SunOS 5.8: /usr/sbin/prtvtoc patch
112993	01	CURRENT	SunOS 5.8: /usr/sbin/passmgmt patch
112996	01	CURRENT	SunOS 5.8: /usr/aset/tasks/sysconf patch
113128	02	CURRENT	X11 6.4.1: XKB patch
113203	02	03	Veritas VA 2.5: VRTSob
113210	02	03	Cummulative patch for VRTSfspro 3.5,REV=GA06d for Solaris 8
113242	01	CURRENT	CDE 1.4: libSDtRmedia patch
113261	02	CURRENT	SunOS 5.8: UTF-8 locale ICONV patch
113372	02	CURRENT	X11 6.4.1: xpr patch
113401	01	CURRENT	SunOS 5.8: UTF-8 iconv modules generate/accept invalid ko 3byte
va			
113413	01	CURRENT	SunOS 5.8: /usr/ccs/bin/lex patch
113415	01	CURRENT	SunOS 5.8: msgfmt, msgfmt, gettext patch
113417	01	CURRENT	SunOS 5.8: slp.jar and slpd.jar patch
113419	01	CURRENT	SunOS 5.8: /usr/bin/sparcv7/prun and /usr/bin/sparcv9/prun
patch			
113501	01		
113595	02	04	Veritas VEA 3.5: VRTSobgui
113596	02	03	VRTSvmpro 3.5: supplemental general patch for Solaris 7, 8, and
9			
113648	03	CURRENT	SunOS 5.8: /usr/sbin/mount patch
113650	02	CURRENT	SunOS 5.8: /usr/lib/utmp_update patch
113654	01	CURRENT	SunOS 5.8: /platform/sun4u/kernel/misc/sparcv9/zuluvvm patch
113679	05	06	SunOS 5.8: rmc_comm/rmcadm/rmcclmv/librsc.so.1 patch
113680	03	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/bge patch
113681	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/mc-us3i patch
113682	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/pmugpio patch
113683	02	CURRENT	SunOS 5.8: /platform/sun4u/kernel/tod/sparcv9/todm5819p_rmc
patch			
113684	04	CURRENT	SunOS 5.8: /usr/platform/SUNW,Sun-Fire-V240/sbin/scadm patch
113685	05	CURRENT	SunOS 5.8: logindmux/ptsl/ms/bufmod/llcl1/kb/zs/zsh/ptem patch

```

113687 01 CURRENT SunOS 5.8: /kernel/misc/kbtrans patch
113749 01 CURRENT SunOS 5.8: User Manager CLI Patch
113792 01 CURRENT OpenWindows 3.6.2: mailtool patch
114059 02 03 SunOS 5.8: en_US.UTF-8 locale patch
114155 01 02 SunOS 5.8: /usr/ccs/bin/m4 patch
114157 01 CURRENT SunOS 5.8: /platform/sun4u/kernel/drv/power patch
114158 01 CURRENT SunOS 5.8: /usr/ccs/bin/yacc patch
114160 01 CURRENT SunOS 5.8: avl_tree, avl_node and rnode patch
114162 01 CURRENT SunOS 5.8: /kernel/drv/lofi drivers and /usr/sbin/lofiadm patch
114278 01
114364 01 CURRENT CDE1.4: GNOME/CDE Menu for Solaris 8
114537 03 19 SunOS 5.8: Sun XVR-100 Graphics Accelerator Patch
114610 01 CURRENT SUNOS 5.8: ANSI-1251 encodings file errors
114667 01 CURRENT SunOS 5.8: /usr/ccs/bin/lorder patch
114671 01 CURRENT SunOS 5.8: /usr/kernel/fs/pcfs patch
114673 01 CURRENT SunOS 5.8: /usr/sbin/wall patch
114773 01 CURRENT SunOS 5.8: /usr/bin/dd patch
114802 02 CURRENT SunOS 5.8: Patch for assembler
114984 01 CURRENT SunOS 5.8: /usr/kernel/fs/namefs patch
115274 02 03 SunOS 5.8: /usr/sbin/raidctl patch
115275 01 03 SunOS 5.8: mpt driver patch
115576 01 CURRENT SunOS 5.8: /kernel/exec/elfexec and
/kernel/exec/sparcv9/elfexec p
115797 01 CURRENT CDE 1.4: dtspcd Patch
115827 01 CURRENT SunOS 5.8: /sbin/sulogin and /sbin/netstrategy patch
116602 01 CURRENT SunOS 5.8: /sbin/uadmin and /sbin/hostconfig patch
=====

```

#### UNINSTALLED RECOMMENDED PATCHES

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
108576	N/A	46	22			SunOS 5.8: Expert3D IFB Graphics Patch
108827	N/A	40	376	108528-13	109079-01	(or newer) Obsoleted by: 108993-18 SunOS 5.8: /usr/lib/libthread.so.1 patch
				108989-01		
108875	N/A	13	412	109007-08		Obsoleted by: 109007-11 SunOS 5.8: c2audit patch
108991	N/A	18	833	108528-07	109079-01	(or newer) Obsoleted by: 108827-15 SunOS 5.8: /usr/lib/libc.so.1 patch
				108989-01		
109041	N/A	04	1003	108528-08		Obsoleted by: 108528-09 SunOS 5.8: sockfs patch
109137	N/A	01	1414			Obsoleted by: 110934-03 SunOS 5.8: /usr/sadm/install/bin/pkginstall
109154	N/A	20	113			SunOS 5.8: PGX32 Graphics
109181	N/A	04	933			Obsoleted by: 108528-13 SunOS 5.8: /kernel/fs/cacheefs patch
109221	N/A	06	1118	108993-01		Obsoleted by: 109318-12 SunOS 5.8: Patch for sysidnet
109279	N/A	18	848			Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/ip patch
109322	N/A	09	833	108991-07		Obsoleted by: 108827-15 SunOS 5.8: libnsl patch
				108827-15		
109587	N/A	03	979			Obsoleted by: 109318-18 SunOS 5.8: libspmistore patch
109742	N/A	04	1013	109279-09		Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/icmp patch
109904	N/A	05	848	109279-16		Obsoleted by: 108528-13 SunOS 5.8: /etc/default/mpathd and /sbin/i
				108528-13		
109906	N/A	06	911	109904-02		Obsoleted by: 108528-13 SunOS 5.8: dhcpgent, dhcinfo, ifconfig a
				109279-07		
				111310-01		
				109742-02		
				108528-13		
				108528-13		
				108528-13		
109951	N/A	01	1280			SunOS 5.8: jserver buffer overflow
110383	N/A	02	932			Obsoleted by: 108528-13 SunOS 5.8: libnvpair patch

110390 N/A 02 1015 patch	Obsoleted by: 108993-05 SunOS 5.8: ldapclient
110700 N/A 01 1136 patch	Obsoleted by: 108993-18 SunOS 5.8: automount
110949 N/A 01 945 /usr/sadm/install/bin/pkgremove	Obsoleted by: 110934-04 SunOS 5.8:
111085 N/A 02 797 patch	Obsoleted by: 108993-18 SunOS 5.8: /usr/bin/login
111090 N/A 03 926 /usr/lib/libldap.so.1 patch	Obsoleted by: 108993-05 SunOS 5.8:
111177 N/A 06 847 /usr/lib/lwp/libthread.so.1 pat	Obsoleted by: 108827-15 SunOS 5.8:
111293 N/A 04 876 /usr/lib/libdevinfo.so.1 patch	Obsoleted by: 108528-21 SunOS 5.8:
111299 N/A 04 530 110386-01	Obsoleted by: 108993-18 SunOS 5.8: PPP patch
111363 N/A 01 1008 /usr/sbin/installf patch	Obsoleted by: 110934-04 SunOS 5.8:
111659 N/A 07 589 pam_unix.so.1 patch	Obsoleted by: 108993-18 SunOS 5.8: passwd and
111879 N/A 01 905	SunOS 5.8: Solaris Product Registry patch SUNWwsr
112218 N/A 01 827 patch	Obsoleted by: 108993-18 SunOS 5.8:: pam_ldap.so.1
112279 N/A 02 628 Solaris 8 to Solaris 9	SunOS 5.8: pkgm failed during upgrade from
112334 N/A 02 715 /usr/include/sys/archsystem.h pa	Obsoleted by: 108528-14 SunOS 5.8:
114152 N/A 01 435 Compatibility(BCP) patch	SunOS 5.8: Japanese SunOS 4.x Binary
114251 N/A 01 279 upper release with	SunOS 5.8: pkgm failed if upgrade from S8U7 to
116610 N/A 01 23 writes to the console	SunOS 5.8: audit_warn uses /usr/ucb/mail and

=====

#### UNINSTALLED SECURITY PATCHES

NOTE: This list includes the Security patches that are also Recommended

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
108827	N/A	40	376	108528-13	109079-01	(or newer) Obsoleted by: 108993-18 SunOS 5.8:
/usr/lib/libthread.so.1 patch						
108875	N/A	13	412	109007-08		Obsoleted by: 109007-11 SunOS 5.8: c2audit patch
108979	N/A	10	1190	108528-03		Obsoleted by: 108528-04 SunOS 5.8: platform
nexus, I2C, Netra ct a						
108991	N/A	18	833	108528-07	109079-01	(or newer) Obsoleted by: 108827-15 SunOS 5.8:
/usr/lib/libc.so.1 patch						
109041	N/A	04	1003	108528-08		Obsoleted by: 108528-09 SunOS 5.8: sockfs patch
109154	N/A	16	439			WITHDRAWN PATCH SunOS 5.8: PGX32 Graphics
109154	N/A	20	113			SunOS 5.8: PGX32 Graphics
109279	N/A	18	848			Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/ip
patch						
109322	N/A	09	833	108991-07	108827-15	Obsoleted by: 108827-15 SunOS 5.8: libnsl patch
109951	N/A	01	1280			SunOS 5.8: jserver buffer overflow
109965	N/A	03	1118			Obsoleted by: 109887-02 SunOS 5.8:
pam_smartcard.so.1 patch						
110416	N/A	03	930			SunOS 5.8: ATOK12 patch
111085	N/A	02	797			Obsoleted by: 108993-18 SunOS 5.8: /usr/bin/login
patch						
111090	N/A	03	926			Obsoleted by: 108993-05 SunOS 5.8:
/usr/lib/libldap.so.1 patch						
111299	N/A	04	530	110386-01		Obsoleted by: 108993-18 SunOS 5.8: PPP patch
111332	N/A	06	408			SunOS 5.8: /usr/lib/dcs patch
111647	N/A	01	926			BCP libmle buffer overflow
111659	N/A	07	589			Obsoleted by: 108993-18 SunOS 5.8: passwd and
pam_unix.so.1 patch						

```

112218 N/A 01 827                               Obsoleted by: 108993-18 SunOS 5.8:: pam_ldap.so.1
patch
112390 N/A 08 104 109223-02                       SunOS 5.8: Supplemental Encryption Kerberos V5:
mech_krb5.so.1 pat
112605 N/A 04 530 108993-11                       Obsoleted by: 108993-18 SunOS 5.8:
/kernel/fs/autofs and /usr/lib/
                               111023-02
112792 N/A 01 589 108968-06                       SunOS 5.8: /usr/lib/pcmciad patch
113652 N/A 03 422 108528-17 108528-18 (or newer) SunOS 5.8: Supplemental Kernel Update
Patch for 108528-17
114045 N/A 07 68                                   SunOS 5.8: NSPR 4.1.4 / NSS 3.3.4.1
114146 N/A 01 436 108528-16 108528-17 (or newer) SunOS 5.8: Supplemental Kernel Update
Patch for 108528-16
116455 N/A 01 12                               SunOS 5.8: Solaris sadmind default security level
=====

```

#### UNINSTALLED Y2K PATCHES

NOTE: This list includes the Y2K patches that are also Recommended

Patch ID	Ins ID	Lat Rev	Age Rev	Require ID	Incomp ID	Synopsis
----------	--------	---------	---------	------------	-----------	----------

-----  
All Y2K patches installed!  
=====

© SANS Institute 2004, Author retains full rights.

## Initialization Scripts

```
# ls /etc/rc2.d
K06mipagent      S401llc2      S74autofs      S89bdconfig
K07dmi           S47asppp      S74syslog      S90wbem
K07snmpdx        S47pppd       S74xntpd       S92volmgt
K16apache        S50isisd      S75cron        S93cacheos.finish
K21dhcp          S69inet       S75savecore    S94ncalogd
K28nfs.server    S70uucp       S76nscd        S94vxnm-vxnetd
README           S71ldap.client S80PRESERVE    S95ncad
S01MOUNTFSYS     S71rpc        S80agent       S95vxvm-recover
S05RMTMPFILES    S71sysid.sys  S80lp          S96vradmind
S10lu            S72autoinstall S80spc         S96vxrsyncd
S20syssetup      S72inetsvc    S85power       S99audit
S21perf          S72slpd       S88bvcontrold  S99dtlogin
S25lom           S73cachefs.daemon S88sendmail    S99eccmad
S30sysid.net     S73nfs.client S88utmpd       S99hbanyware

# ls /etc/rc3.d
README           S50apache      S77dmi
S15nfs.server    S50san_driverchk S80mipagent
S34dhcp          S76snmpdx      S88bvcontrold
```

## System Logging

```
# cat /etc/syslog.conf
#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 *
)

# Added to increase inetd logging
# also added the "-t" to the inetd startup
daemon.debug /var/log/connlog
```

## Appendix C – Automated Scanning Tool Output

---

### NMAP 3.50

```
# /usr/local/bin/nmap -sT -sU -sR -O giacunixhost.giac-fortune.com
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-17 08:48 EST
Interesting ports on giacunixhost (10.1.201.218):
(The 3086 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
7/udp     open  echo
9/tcp     open  discard
9/udp     open  discard
13/tcp    open  daytime
13/udp    open  daytime
19/tcp    open  chargen
19/udp    open  chargen
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
37/tcp    open  time
37/udp    open  time
42/udp    open  nameserver
79/tcp    open  finger
111/tcp   open  rpcbind (rpcbind V2-4)      2-4 (rpc #100000)
111/udp   open  rpcbind (rpcbind V2-4)      2-4 (rpc #100000)
161/udp   open  snmp
177/udp   open  xdmcp
512/tcp   open  exec
512/udp   open  biff
513/tcp   open  login
514/tcp   open  shell
514/udp   open  syslog
515/tcp   open  printer
517/udp   open  talk
540/tcp   open  uucp
587/tcp   open  submission
898/tcp   open  sun-manageconsole
4045/tcp  open  nlockmgr (nlockmgr V1-4)    1-4 (rpc #100021)
4045/udp  open  nlockmgr (nlockmgr V1-4)    1-4 (rpc #100021)
6112/tcp  open  dtspc
7100/tcp  open  font-service
32771/tcp open  status (status V1)          1 (rpc #100024)
32771/udp open  sometimes-rpc6
32772/tcp open  rusersd (rusersd V2-3)      2-3 (rpc #100002)
32772/udp open  status (status V1)          1 (rpc #100024)
32773/tcp open  ttldbserverd (ttldbserverd V1) 1 (rpc #100083)
32773/udp open  sadmind (sadmind V10)        10 (rpc #100232)
32774/tcp open  kcms_server (kcms_server V1) 1 (rpc #100221)
32774/udp open  rquotad (rquotad V1)         1 (rpc #100011)
32775/udp open  rusersd (rusersd V2-3)      2-3 (rpc #100002)
32776/tcp open  sometimes-rpc15
32776/udp open  sprayd (sprayd V1)           1 (rpc #100012)
32777/tcp open  snmpXdmid (snmpXdmid V1)     1 (rpc #100249)
32777/udp open  walld (walld V1)             1 (rpc #100008)
32778/tcp open  dmispd (dmispd V1)           1 (rpc #300598)
32778/udp open  rstatd (rstatd V2-4)         2-4 (rpc #100001)
32779/udp open  cmsd (cmsd V2-5)             2-5 (rpc #100068)
32786/udp open  sometimes-rpc26
32787/udp open  sometimes-rpc28
Device type: general purpose
Running: Sun Solaris 8
OS details: Sun Solaris 8
Uptime 4.732 days (since Thu Feb 12 15:29:52 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 912.087 seconds
```

## Nessus 2.0.10

### Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

#### Scan Details

Hosts which were alive and responding during test 1  
Number of security holes found 21  
Number of security warnings found 19

#### Host List

Host(s)	Possible Issue
Giacunixhost.giac-fortune.com	Security hole(s) found

[\[ return to top \]](#)

#### Analysis of Host

Address of Host	Port/Service	Issue regarding Port
giacunixhost	<a href="#">echo (7/tcp)</a>	Security notes found
giacunixhost	<a href="#">discard (9/tcp)</a>	No Information
giacunixhost	<a href="#">daytime (13/tcp)</a>	No Information
giacunixhost	<a href="#">chargen (19/tcp)</a>	Security notes found
giacunixhost	<a href="#">ftp (21/tcp)</a>	Security hole found
giacunixhost	<a href="#">telnet (23/tcp)</a>	Security notes found
giacunixhost	<a href="#">smtp (25/tcp)</a>	Security hole found
giacunixhost	<a href="#">time (37/tcp)</a>	Security notes found
giacunixhost	<a href="#">finger (79/tcp)</a>	Security warning(s) found
giacunixhost	<a href="#">sunrpc (111/tcp)</a>	Security notes found
giacunixhost	<a href="#">exec (512/tcp)</a>	No Information
giacunixhost	<a href="#">login (513/tcp)</a>	No Information
giacunixhost	<a href="#">shell (514/tcp)</a>	No Information
giacunixhost	<a href="#">printer (515/tcp)</a>	Security notes found
giacunixhost	<a href="#">uucp (540/tcp)</a>	Security notes found
giacunixhost	<a href="#">submission (587/tcp)</a>	Security hole found
giacunixhost	<a href="#">unknown (898/tcp)</a>	No Information
giacunixhost	<a href="#">unknown (1236/tcp)</a>	Security notes found
giacunixhost	<a href="#">unknown (2148/tcp)</a>	No Information
giacunixhost	<a href="#">lockd (4045/tcp)</a>	Security notes found
giacunixhost	<a href="#">unknown (5798/tcp)</a>	No Information
giacunixhost	<a href="#">unknown (5987/tcp)</a>	No Information
giacunixhost	<a href="#">dtspc (6112/tcp)</a>	Security hole found
giacunixhost	<a href="#">unknown (6389/tcp)</a>	No Information



giacunixhost	<a href="#">font-service (7100/tcp)</a>	Security hole found
giacunixhost	unknown (10555/tcp)	No Information
giacunixhost	<a href="#">sometimes-rpc5 (32771/tcp)</a>	Security notes found
giacunixhost	<a href="#">sometimes-rpc7 (32772/tcp)</a>	Security notes found
giacunixhost	<a href="#">sometimes-rpc9 (32773/tcp)</a>	Security hole found
giacunixhost	<a href="#">sometimes-rpc11 (32774/tcp)</a>	Security notes found
giacunixhost	sometimes-rpc15 (32776/tcp)	No Information
giacunixhost	<a href="#">sometimes-rpc17 (32777/tcp)</a>	Security hole found
giacunixhost	<a href="#">sometimes-rpc19 (32778/tcp)</a>	Security notes found
giacunixhost	unknown (36441/tcp)	No Information
giacunixhost	<a href="#">unknown (36451/tcp)</a>	Security notes found
giacunixhost	<a href="#">unknown (36475/tcp)</a>	Security notes found
giacunixhost	<a href="#">unknown (36477/tcp)</a>	Security notes found
giacunixhost	<a href="#">unknown (36478/tcp)</a>	Security notes found
giacunixhost	echo (7/udp)	No Information
giacunixhost	discard (9/udp)	No Information
giacunixhost	daytime (13/udp)	No Information
giacunixhost	chargen (19/udp)	No Information
giacunixhost	time (37/udp)	No Information
giacunixhost	nameserver (42/udp)	No Information
giacunixhost	<a href="#">sunrpc (111/udp)</a>	Security notes found
giacunixhost	<a href="#">snmp (161/udp)</a>	Security hole found
giacunixhost	xdmcp (177/udp)	No Information
giacunixhost	biff (512/udp)	No Information
giacunixhost	syslog (514/udp)	No Information
giacunixhost	talk (517/udp)	No Information
giacunixhost	unknown (2148/udp)	No Information
giacunixhost	<a href="#">lockd (4045/udp)</a>	Security warning(s) found
giacunixhost	sometimes-rpc6 (32771/udp)	No Information
giacunixhost	<a href="#">sometimes-rpc8 (32772/udp)</a>	Security warning(s) found
giacunixhost	<a href="#">sometimes-rpc10 (32773/udp)</a>	Security hole found
giacunixhost	<a href="#">sometimes-rpc12 (32774/udp)</a>	Security warning(s) found
giacunixhost	<a href="#">sometimes-rpc14 (32775/udp)</a>	Security warning(s) found
giacunixhost	<a href="#">sometimes-rpc16 (32776/udp)</a>	Security warning(s) found
giacunixhost	<a href="#">sometimes-rpc18 (32777/udp)</a>	Security hole found

giacunixhost	<a href="#">sometimes-rpc20 (32778/udp)</a>	Security warning(s) found
giacunixhost	<a href="#">sometimes-rpc22 (32779/udp)</a>	Security hole found
giacunixhost	<a href="#">unknown (32781/udp)</a>	Security notes found
giacunixhost	<a href="#">unknown (32782/udp)</a>	Security hole found
giacunixhost	unknown (32783/udp)	No Information
giacunixhost	sometimes-rpc26 (32786/udp)	No Information
giacunixhost	sometimes-rpc28 (32787/udp)	No Information
giacunixhost	unknown (32788/udp)	No Information
giacunixhost	unknown (32800/udp)	No Information
giacunixhost	<a href="#">general/udp</a>	Security hole found
giacunixhost	<a href="#">general/tcp</a>	Security warning(s) found
giacunixhost	<a href="#">general/icmp</a>	Security warning(s) found
giacunixhost	<a href="#">sometimes-rpc21 (32779/tcp)</a>	Security hole found

Security Issues and Fixes: giacunixhost		
Type	Port	Issue and Fix
Informational	echo (7/tcp)	An echo server is running on this port Nessus ID : <a href="#">10330</a>
Informational	chargen (19/tcp)	Chargen is running on this port Nessus ID : <a href="#">10330</a>
Vulnerability	ftp (21/tcp)	<p>You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw. An attacker may use this problem to execute arbitrary commands on this host.</p> <p>*** Nessus relied solely on the banner of the server to issue this warning, *** so this alert might be a false positive *** NOTE: must have a valid username/password to fully check this vulnerability</p> <p>Solution : Upgrade your ftp server software to the latest version. Risk factor : High</p> <p>CVE : <a href="#">CAN-2001-0249</a>, <a href="#">CVE-2001-0550</a>            BID : <a href="#">2550</a>, <a href="#">3581</a>            Nessus ID : <a href="#">10821</a></p>
Informational	ftp (21/tcp)	An FTP server is running on this port. Here is its banner : 220 giacunixhost FTP server (SunOS 5.8) ready. Nessus ID : <a href="#">10330</a>
Informational	ftp (21/tcp)	Remote FTP server banner : 220 giacunixhost FTP server (SunOS 5.8) ready. Nessus ID : <a href="#">10092</a>
Informational	telnet (23/tcp)	A telnet server seems to be running on this port Nessus ID : <a href="#">10330</a>
Informational	telnet (23/tcp)	<p>Remote telnet banner :</p> <p>SunOS 5.8</p> <p>Nessus ID : <a href="#">10281</a></p>

Informational	telnet (23/tcp)	Remote telnet banner :  SunOS 5.8  Nessus ID : <a href="#">10281</a>
Vulnerability	smtp (25/tcp)	<p>The remote sendmail server, according to its version number, may be vulnerable to a buffer overflow its DNS handling code.</p> <p>The owner of a malicious name server could use this flaw to execute arbitrary code on this host.</p> <p>Solution : Upgrade to Sendmail 8.12.5 Risk factor : High CVE : <a href="#">CVE-2002-0906</a> BID : <a href="#">5122</a> Nessus ID : <a href="#">11232</a></p>
Vulnerability	smtp (25/tcp)	<p>The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.</p> <p>Sendmail versions from 5.79 to 8.12.7 are vulnerable. Solution : Upgrade to Sendmail ver 8.12.8 or greater or if you cannot upgrade, apply patches for 8.10-12 here:  <a href="http://www.sendmail.org/patchcr.html">http://www.sendmail.org/patchcr.html</a></p> <p>NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerabilty.</p> <p>*** Nessus reports this vulnerability using only *** the banner of the remote SMTP server. Therefore, *** this might be a false positive.</p> <p>see <a href="http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950">http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950</a> <a href="http://www.cert.org/advisories/CA-2003-07.html">http://www.cert.org/advisories/CA-2003-07.html</a> <a href="http://www.kb.cert.org/vuls/id/398025">http://www.kb.cert.org/vuls/id/398025</a></p> <p>Risk factor : High CVE : <a href="#">CAN-2002-1337</a>, <a href="#">CVE-2001-1349</a> BID : <a href="#">6991</a> Other references : IAVA:2003-A-0002 Nessus ID : <a href="#">11316</a></p>
Vulnerability	smtp (25/tcp)	<p>The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.</p> <p>Sendmail versions from 5.79 to 8.12.8 are vulnerable. Solution : Upgrade to Sendmail ver 8.12.9 or greater or if you cannot upgrade, apply patches for 8.10-12 here:  <a href="http://www.sendmail.org/patchps.html">http://www.sendmail.org/patchps.html</a></p> <p>NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerabilty.</p> <p>*** Nessus reports this vulnerability using only *** the banner of the remote SMTP server. Therefore, *** this might be a false positive.</p>

Vulnerability	smtp (25/tcp)	<p>Risk factor : High            CVE : <a href="#">CAN-2003-0161</a>            BID : <a href="#">7230</a>            Other references : RHSA:RHSA-2003:120-01            Nessus ID : <a href="#">11499</a></p>
		<p>The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.</p> <p>Sendmail versions from 5.79 to 8.12.9 are vulnerable.            Solution : Upgrade to Sendmail ver 8.12.10.            See also : <a href="http://lists.netsys.com/pipermail/full-disclosure/2003-September/010287.html">http://lists.netsys.com/pipermail/full-disclosure/2003-September/010287.html</a></p> <p>NOTE: manual patches do not change the version numbers.            Vendors who have released patched versions of sendmail may still falsely show vulnerability.</p> <p>*** Nessus reports this vulnerability using only            *** the banner of the remote SMTP server. Therefore,            *** this might be a false positive.</p> <p>Risk factor : High            CVE : <a href="#">CAN-2003-0681</a>, <a href="#">CAN-2003-0694</a>            BID : <a href="#">8641</a>            Other references : RHSA:RHSA-2003:283-01, SuSE:SUSE-SA:2003:040            Nessus ID : <a href="#">11838</a></p>
Warning	smtp (25/tcp)	<p>The remote SMTP server answers to the EXPN and/or VRFY commands.</p> <p>The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.</p> <p>Your mailer should not allow remote users to use any of these commands, because it gives them too much information.</p> <p>Solution : if you are using Sendmail, add the option :</p> <p>O PrivacyOptions=goaway</p> <p>in /etc/sendmail.cf.</p> <p>Risk factor : Low            CVE : <a href="#">CAN-1999-0531</a>            Nessus ID : <a href="#">10249</a></p>
Warning	smtp (25/tcp)	<p>The remote SMTP server is vulnerable to a redirection attack. That is, if a mail is sent to :</p> <p>user@hostname1@victim</p> <p>Then the remote SMTP server (victim) will happily send the mail to :            user@hostname1</p> <p>Using this flaw, an attacker may route a message through your firewall, in order to exploit other SMTP servers that can not be reached from the outside.</p> <p>Solution : In sendmail.cf, at the top of ruleset 98, in /etc/sendmail.cf, insert the following statement :</p>

		<p>R\$*@\$*@\$* \$#error \$@ 5.7.1 \$: '551 Sorry, no redirections.'</p> <p>Risk factor : Low Nessus ID : <a href="#">10250</a></p>
Warning	smtp (25/tcp)	<p>The remote SMTP server seems to allow the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.</p> <p>Risk factor : Low/Medium</p> <p>Solution : configure your SMTP server so that it can't be used as a relay any more. CVE : <a href="#">CAN-1999-0512</a>, <a href="#">CAN-2002-1278</a>, <a href="#">CAN-2003-0285</a>            BID : <a href="#">8196</a>            Nessus ID : <a href="#">10262</a></p>
Warning	smtp (25/tcp)	<p>According to the version number of the remote mail server, a local user may be able to obtain the complete mail configuration and other interesting information about the mail queue even if he is not allowed to access those information directly, by running <code>sendmail -q -d0-nnnn.xxx</code> where <code>nnnn</code> &amp; <code>xxx</code> are debugging levels.</p> <p>If users are not allowed to process the queue (which is the default) then you are not vulnerable.</p> <p>Solution : upgrade to the latest version of Sendmail or do not allow users to process the queue (RestrictQRun option)            Risk factor : Very low / none            Note : This vulnerability is <code>_local_</code> only            CVE : <a href="#">CAN-2001-0715</a>            BID : <a href="#">3898</a>            Nessus ID : <a href="#">11088</a></p>
Informational	smtp (25/tcp)	<p>An SMTP server is running on this port            Here is its banner :            220 giacunixhost ESMTP Sendmail 8.11.7p1+Sun/8.11.7; Tue, 17 Feb 2004 08:51:27 -0500 (EST)            Nessus ID : <a href="#">10330</a></p>
Informational	smtp (25/tcp)	<p>Remote SMTP server banner :            220 giacunixhost ESMTP Sendmail 8.11.7p1+Sun/8.11.7; Tue, 17 Feb 2004 08:52:22 -0500 (EST)</p>
		<p>This is probably: Sendmail version 8.11.7p1+Sun</p> <p>Nessus ID : <a href="#">10263</a></p>
Informational	smtp (25/tcp)	<p>This server could be fingerprinted as being Sendmail 8.10.1            Nessus ID : <a href="#">11421</a></p>
Informational	time (37/tcp)	<p>A time server seems to be running on this port            Nessus ID : <a href="#">10330</a></p>
Warning	finger (79/tcp)	<p>The remote finger service accepts to redirect requests. That is, users can perform requests like :</p> <p><code>finger user@host@victim</code></p> <p>This allows an attacker to use this computer as a relay to gather information on a third party network.</p> <p>Solution: Disable the remote finger daemon (comment out the 'finger' line in <code>/etc/inetd.conf</code> and restart the <code>inetd</code> process) or upgrade it to a more secure one.</p> <p>Risk factor : Low</p>

		<p>CVE : <a href="#">CAN-1999-0105</a>, <a href="#">CVE-1999-0106</a>  Nessus ID : <a href="#">10073</a></p>
Informational	finger (79/tcp)	<p>A finger server seems to be running on this port  Nessus ID : <a href="#">10330</a></p>
Informational	sunrpc (111/tcp)	<p>The RPC portmapper is running on this port.</p> <p>An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port.</p> <p>Risk factor : Low  CVE : <a href="#">CAN-1999-0632</a>, <a href="#">CVE-1999-0189</a>  BID : <a href="#">205</a>  Nessus ID : <a href="#">10223</a></p>
Informational	sunrpc (111/tcp)	<p>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</p> <p>Nessus ID : <a href="#">11111</a></p>
Informational	printer (515/tcp)	<p>A LPD server seems to be running on this port  Nessus ID : <a href="#">10330</a></p>
Informational	uucp (540/tcp)	<p>An UUCP server seems to be running on this port  Nessus ID : <a href="#">10330</a></p>
Vulnerability	submission (587/tcp)	<p>The remote sendmail server, according to its version number, may be vulnerable to a buffer overflow its DNS handling code.</p> <p>The owner of a malicious name server could use this flaw to execute arbitrary code on this host.</p> <p>Solution : Upgrade to Sendmail 8.12.5  Risk factor : High  CVE : <a href="#">CVE-2002-0906</a>  BID : <a href="#">5122</a>  Nessus ID : <a href="#">11232</a></p>
Vulnerability	submission (587/tcp)	<p>The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.</p> <p>Sendmail versions from 5.79 to 8.12.7 are vulnerable.  Solution : Upgrade to Sendmail ver 8.12.8 or greater or if you cannot upgrade, apply patches for 8.10-12 here:</p> <p><a href="http://www.sendmail.org/patchcr.html">http://www.sendmail.org/patchcr.html</a></p> <p>NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerability.</p> <p>*** Nessus reports this vulnerability using only  *** the banner of the remote SMTP server. Therefore,  *** this might be a false positive.</p> <p>see <a href="http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950">http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950</a>  <a href="http://www.cert.org/advisories/CA-2003-07.html">http://www.cert.org/advisories/CA-2003-07.html</a>  <a href="http://www.kb.cert.org/vuls/id/398025">http://www.kb.cert.org/vuls/id/398025</a></p> <p>Risk factor : High  CVE : <a href="#">CAN-2002-1337</a>, <a href="#">CVE-2001-1349</a>  BID : <a href="#">6991</a>  Other references : IAVA:2003-A-0002</p>

<p><b>Vulnerability</b> submission (587/tcp)</p>	<p>Nessus ID : <a href="#">11316</a></p> <p>The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.</p> <p>Sendmail versions from 5.79 to 8.12.8 are vulnerable. Solution : Upgrade to Sendmail ver 8.12.9 or greater or if you cannot upgrade, apply patches for 8.10-12 here:</p> <p><a href="http://www.sendmail.org/patchps.html">http://www.sendmail.org/patchps.html</a></p> <p>NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerability.</p> <p>*** Nessus reports this vulnerability using only *** the banner of the remote SMTP server. Therefore, *** this might be a false positive.</p> <p>Risk factor : High CVE : <a href="#">CAN-2003-0161</a> BID : <a href="#">7230</a> Other references : RHSA:RHSA-2003:120-01 Nessus ID : <a href="#">11499</a></p>
<p><b>Vulnerability</b> submission (587/tcp)</p>	<p>The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges.</p> <p>Sendmail versions from 5.79 to 8.12.9 are vulnerable. Solution : Upgrade to Sendmail ver 8.12.10. See also : <a href="http://lists.netsys.com/pipermail/full-disclosure/2003-September/010287.html">http://lists.netsys.com/pipermail/full-disclosure/2003-September/010287.html</a></p> <p>NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerability.</p> <p>*** Nessus reports this vulnerability using only *** the banner of the remote SMTP server. Therefore, *** this might be a false positive.</p> <p>Risk factor : High CVE : <a href="#">CAN-2003-0681</a>, <a href="#">CAN-2003-0694</a> BID : <a href="#">8641</a> Other references : RHSA:RHSA-2003:283-01, SuSE:SUSE-SA:2003:040 Nessus ID : <a href="#">11838</a></p>
<p><b>Warning</b> submission (587/tcp)</p>	<p>The remote SMTP server is vulnerable to a redirection attack. That is, if a mail is sent to :</p> <p>user@hostname1@victim</p> <p>Then the remote SMTP server (victim) will happily send the mail to : user@hostname1</p> <p>Using this flaw, an attacker may route a message through your firewall, in order to exploit other SMTP servers that can not be reached from the outside.</p> <p>Solution : In sendmail.cf, at the top of ruleset 98, in /etc/sendmail.cf, insert the following statement : R\$*@\$*@\$* \$#error \$@ 5.7.1 \$: '551 Sorry, no redirections.'</p>

Warning	submission (587/tcp)	<p>Risk factor : Low Nessus ID : <a href="#">10250</a></p> <p>The remote SMTP server seems to allow the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.</p> <p>Risk factor : Low/Medium</p> <p>Solution : configure your SMTP server so that it can't be used as a relay any more. CVE : <a href="#">CAN-1999-0512</a>, <a href="#">CAN-2002-1278</a>, <a href="#">CAN-2003-0285</a>            BID : <a href="#">8196</a>            Nessus ID : <a href="#">10262</a></p>
		<p>According to the version number of the remote mail server, a local user may be able to obtain the complete mail configuration and other interesting information about the mail queue even if he is not allowed to access those information directly, by running <code>sendmail -q -d0-nnnn.xxx</code> where nnnn &amp; xxx are debugging levels.</p> <p>If users are not allowed to process the queue (which is the default) then you are not vulnerable.</p> <p>Solution : upgrade to the latest version of Sendmail or do not allow users to process the queue (RestrictQRun option)            Risk factor : Very low / none            Note : This vulnerability is _local_ only            CVE : <a href="#">CAN-2001-0715</a>            BID : <a href="#">3898</a>            Nessus ID : <a href="#">11088</a></p>
Informational	submission (587/tcp)	<p>An SMTP server is running on this port            Here is its banner :            220 giacunixhost ESMTP Sendmail 8.11.7p1+Sun/8.11.7; Tue, 17 Feb 2004 08:50:49 -0500 (EST)            Nessus ID : <a href="#">10330</a></p>
Informational	submission (587/tcp)	<p>Remote SMTP server banner :            220 giacunixhost ESMTP Sendmail 8.11.7p1+Sun/8.11.7; Tue, 17 Feb 2004 08:52:21 -0500 (EST)</p> <p>This is probably: Sendmail version 8.11.7p1+Sun</p> <p>Nessus ID : <a href="#">10263</a></p>
Informational	submission (587/tcp)	<p>This server could be fingerprinted as being Sendmail 8.10.1            Nessus ID : <a href="#">11421</a></p>
Informational	unknown (1236/tcp)	<p>The service closed the connection after 0 seconds without sending any data            It might be protected by some TCP wrapper</p> <p>Nessus ID : <a href="#">10330</a></p>
Informational	lockd (4045/tcp)	<p>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</p> <p>Nessus ID : <a href="#">11111</a></p>
Vulnerability	dtspc (6112/tcp)	<p>The 'dtspcd' service is running. This service deals with the CDE interface for the X11 system.</p> <p>Some versions of this daemon are vulnerable to a buffer overflow attack which may allow an attacker to gain root privileges on this host.</p>



		<p>*** This warning might be a false positive, *** as no real overflow was performed</p> <p>Solution : See <a href="http://www.cert.org/advisories/CA-2001-31.html">http://www.cert.org/advisories/CA-2001-31.html</a> to determine if you are vulnerable or deactivate this service (comment out the line 'dtspc' in /etc/inetd.conf and restart the inetd process)</p> <p>Risk factor : High CVE : <a href="#">CVE-2001-0803</a> BID : <a href="#">3517</a> Other references : IAVA:2002-A-0001 Nessus ID : <a href="#">10833</a></p>
Vulnerability	font-service (7100/tcp)	<p>The remote X Font Service (xfs) might be vulnerable to a buffer overflow.</p> <p>An attacker may use this flaw to gain root on this host remotely.</p> <p>*** Note that Nessus did not actually check for the flaw *** as details about this vulnerability are still unknown</p> <p>Solution : See CERT Advisory CA-2002-34 Risk factor : High CVE : <a href="#">CAN-2002-1317</a> Nessus ID : <a href="#">11188</a></p>
Informational	sometimes-rpc5 (32771/tcp)	<p>RPC program #100024 version 1 'status' is running on this port RPC program #100133 version 1 is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Informational	sometimes-rpc7 (32772/tcp)	<p>RPC program #100002 version 2 'rusersd' (rusers) is running on this port RPC program #100002 version 3 'rusersd' (rusers) is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Vulnerability	sometimes-rpc9 (32773/tcp)	<p>The tooltalk RPC service is running.</p> <p>There is a format string bug in many versions of this service, which allow an attacker to gain root remotely.</p> <p>In addition to this, several versions of this service allow remote attackers to overwrite arbitrary memory locations with a zero and possibly gain privileges via a file descriptor argument in an AUTH_UNIX procedure call which is used as a table index by the _TT_ISCLOSE procedure.</p> <p>*** This warning may be a false positive since the presence *** of the bug was not verified locally.</p> <p>Solution : Disable this service or patch it See also : CERT Advisories CA-2001-27 and CA-2002-20</p> <p>Risk factor : High CVE : <a href="#">CAN-2002-0677</a>, <a href="#">CVE-2001-0717</a>, <a href="#">CVE-2002-0679</a> BID : <a href="#">3382</a> Nessus ID : <a href="#">10787</a></p>
Vulnerability	sometimes-rpc9 (32773/tcp)	<p>The remote host is running the sadmind RPC service. It is possible to misuse this service to execute arbitrary commands on this host as root.</p>

		<p>Solution : Disable this service as Sun does not intend to provide a patch</p> <p>Risk Factor : High</p> <p>CVE : <a href="#">CAN-2003-0722</a></p> <p>BID : <a href="#">8615</a></p> <p>Other references : IAVA:2003-A-0013</p> <p>Nessus ID : <a href="#">11841</a></p>
Informational	sometimes-rpc9 (32773/tcp)	<p>RPC program #100083 version 1 is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Informational	sometimes-rpc11 (32774/tcp)	<p>RPC program #100221 version 1 is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Vulnerability	sometimes-rpc17 (32777/tcp)	<p>The remote RPC service 100249 (snmpXdmid) may be vulnerable to a heap overflow which allows any user to obtain a root shell on this host.</p> <p>*** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled.</p> <p>Solution : disable this service (/etc/init.d/init.dmi stop) if you don't use it, or contact Sun for a patch</p> <p>Risk factor : High</p> <p>CVE : <a href="#">CVE-2001-0236</a></p> <p>BID : <a href="#">2417</a></p> <p>Nessus ID : <a href="#">10659</a></p>
Informational	sometimes-rpc17 (32777/tcp)	<p>RPC program #100249 version 1 is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Informational	sometimes-rpc19 (32778/tcp)	<p>RPC program #300598 version 1 is running on this port</p> <p>RPC program #805306368 version 1 is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Informational	unknown (36451/tcp)	<p>RPC program #100068 version 2 is running on this port</p> <p>RPC program #100068 version 3 is running on this port</p> <p>RPC program #100068 version 4 is running on this port</p> <p>RPC program #100068 version 5 is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Informational	unknown (36451/tcp)	<p>This port was detected as being open by a port scanner but is now closed.</p> <p>This service might have been crashed by a port scanner or by a plugin</p> <p>Nessus ID : <a href="#">10919</a></p>
Informational	unknown (36475/tcp)	<p>This port was detected as being open by a port scanner but is now closed.</p> <p>This service might have been crashed by a port scanner or by a plugin</p> <p>Nessus ID : <a href="#">10919</a></p>
Informational	unknown (36477/tcp)	<p>This port was detected as being open by a port scanner but is now closed.</p> <p>This service might have been crashed by a port scanner or by a plugin</p> <p>Nessus ID : <a href="#">10919</a></p>
Informational	unknown (36478/tcp)	<p>This port was detected as being open by a port scanner but is now closed.</p> <p>This service might have been crashed by a port scanner or by a plugin</p> <p>Nessus ID : <a href="#">10919</a></p>
Informational	sunrpc (111/udp)	<p>RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port</p> <p>RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port</p> <p>RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port</p> <p>Nessus ID : <a href="#">11111</a></p>
Vulnerability	snmp	

	(161/udp)	SNMP Agent responded as expected with community name: public CVE : <a href="#">CAN-1999-0517</a> , <a href="#">CAN-1999-0186</a> , <a href="#">CAN-1999-0254</a> , <a href="#">CAN-1999-0516</a> BID : <a href="#">177</a> , <a href="#">7081</a> , <a href="#">7212</a> , <a href="#">7317</a> Other references : IAVA:2001-B-0001 Nessus ID : <a href="#">10264</a>
Informational	snmp (161/udp)	snmpwalk could get the open port list with the community name 'public' Nessus ID : <a href="#">10841</a>
Informational	snmp (161/udp)	Using SNMP, we could determine that the remote operating system is : Sun SNMP Agent, Sun-Fire-V440 Nessus ID : <a href="#">10800</a>
Warning	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 : <a href="#">CVE-2000-0508</a> BID : <a href="#">1372</a> Nessus ID : <a href="#">10220</a>
Informational	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 : <a href="#">11111</a>
Warning	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 : <a href="#">CVE-1999-0018</a> , <a href="#">CVE-1999-0019</a> , <a href="#">CVE-1999-0493</a> BID : <a href="#">127</a> , <a href="#">450</a> Nessus ID : <a href="#">10235</a>
Informational	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 : <a href="#">11111</a>
Vulnerability	sometimes- rpc10 (32773/udp)	The sadmind RPC service is running. There is a bug in Solaris versions of this service that allow an intruder to execute arbitrary commands on your system.  Solution : disable this service Risk factor : High CVE : <a href="#">CVE-1999-0977</a> BID : <a href="#">866</a> , <a href="#">8615</a> Nessus ID : <a href="#">10229</a>
Informational	sometimes- rpc10 (32773/udp)	RPC program #100232 version 10 'sadmind' is running on this port Nessus ID : <a href="#">11111</a>
Warning	sometimes- rpc12 (32774/udp)	The rquotad 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.

		<p>Risk factor : Low            CVE : <a href="#">CAN-1999-0625</a>            Nessus ID : <a href="#">10226</a></p>
Informational	sometimes-rpc12 (32774/udp)	<p>RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port            Nessus ID : <a href="#">11111</a></p>
Warning	sometimes-rpc14 (32775/udp)	<p>The rusersd RPC service is running. It provides an attacker interesting information such as how often the system is being used, the names of the users, and more.</p> <p>It usually not a good idea to leave this service open.            Risk factor : Low            CVE : <a href="#">CVE-1999-0626</a>            Nessus ID : <a href="#">10228</a></p>
Informational	sometimes-rpc14 (32775/udp)	<p>RPC program #100002 version 2 'rusersd' (rusers) is running on this port            RPC program #100002 version 3 'rusersd' (rusers) is running on this port            Nessus ID : <a href="#">11111</a></p>
Warning	sometimes-rpc16 (32776/udp)	<p>The sprayd RPC service is running.            You should disable this service, as it may be used to saturate your network.            Furthermore, it might become a security threat in the future, if a RPC vulnerability is discovered.</p>
Informational	sometimes-rpc16 (32776/udp)	<p>Risk factor : Low            CVE : <a href="#">CAN-1999-0613</a>            Nessus ID : <a href="#">10234</a></p>
Vulnerability	sometimes-rpc18 (32777/udp)	<p>RPC program #100012 version 1 'sprayd' (spray) is running on this port            Nessus ID : <a href="#">11111</a></p> <p>The rpc.walld RPC service is running. Some versions of this server allow an attacker to gain root access remotely, by consuming the resources of the remote host then sending a specially formed packet with format strings to this host.</p> <p>Solaris 2.5.1, 2.6, 7 and 8 are vulnerable to this issue.            Other operating systems might be affected as well.</p> <p>*** Nessus did not check for this vulnerability, so this might be a            *** false positive</p> <p>Solution : Deactivate this service.            Risk factor : High            CVE : <a href="#">CVE-2002-0573</a>            BID : <a href="#">4639</a>            Nessus ID : <a href="#">10950</a></p>
Warning	sometimes-rpc18 (32777/udp)	<p>The walld RPC service is running. It is usually used by the administrator to tell something to the users of a network by making a message appear on their screen.</p> <p>Since this service lacks any kind of authentication, an attacker may use it to trick users into doing something (change their password, leave the console, or worse), by sending a message which would appear to be written by the administrator.</p> <p>It can also be used as a denial of service attack, by continually sending garbage to the users screens, preventing them from working properly.</p> <p>Solution : Disable this service.            Risk factor : Medium</p>

		<p>CVE : <a href="#">CVE-1999-0181</a>  Nessus ID : <a href="#">10240</a></p>
Informational	sometimes-rpc18 (32777/udp)	<p>RPC program #100008 version 1 'wallid' (rwall shutdown) is running on this port  Nessus ID : <a href="#">11111</a></p>
Warning	sometimes-rpc20 (32778/udp)	<p>The rstatd RPC service is running. It provides an attacker interesting information such as :</p> <ul style="list-style-type: none"> <li>- the CPU usage</li> <li>- the system uptime</li> <li>- its network usage</li> <li>- and more</li> </ul> <p>Letting this service run is not recommended.  Risk factor : Low  CVE : <a href="#">CAN-1999-0624</a>  Nessus ID : <a href="#">10227</a></p>
Informational	sometimes-rpc20 (32778/udp)	<p>RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port  RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port  RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port  Nessus ID : <a href="#">11111</a></p>
Vulnerability	sometimes-rpc22 (32779/udp)	<p>The cmsd 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.</p> <p>*** No security hole regarding this program has been tested, so  *** this might be a false positive</p> <p>Solution : We suggest that you disable this service.  Risk factor : High  CVE : <a href="#">CVE-1999-0320</a>, <a href="#">CVE-1999-0696</a>, <a href="#">CVE-2002-0391</a>  BID : <a href="#">428</a>, <a href="#">5356</a>  Nessus ID : <a href="#">10213</a></p>
Informational	sometimes-rpc22 (32779/udp)	<p>RPC program #100068 version 2 is running on this port  RPC program #100068 version 3 is running on this port  RPC program #100068 version 4 is running on this port  RPC program #100068 version 5 is running on this port  Nessus ID : <a href="#">11111</a></p>
Informational	unknown (32781/udp)	<p>RPC program #100249 version 1 is running on this port  Nessus ID : <a href="#">11111</a></p>
Vulnerability	unknown (32782/udp)	<p>The dmisd RPC service is running.</p> <p>This service uses the function xdr_array() of the RPC library.  It turns out that some older versions of the RPC library are vulnerable to an integer overflow in this function, which could allow an attacker to gain root privileges on this host.</p> <p>*** No security hole regarding this program has been tested, so  *** this might be a false positive.</p> <p>Solution : We suggest that you disable this service.  See also : <a href="http://www.cert.org/advisories/CA-2002-25.html">http://www.cert.org/advisories/CA-2002-25.html</a>  Risk factor : High  CVE : <a href="#">CVE-2002-0391</a>  BID : <a href="#">5356</a>  Nessus ID : <a href="#">11405</a></p>

Informational	unknown (32782/udp)	RPC program #300598 version 1 is running on this port RPC program #805306368 version 1 is running on this port  Nessus ID : <a href="#">11111</a>
Vulnerability	general/udp	<p>It is possible to by-pass the rules of the remote firewall by sending UDP packets with a source port equal to 53.</p> <p>An attacker may use this flaw to inject UDP packets to the remote hosts, in spite of the presence of a firewall.</p> <p>Solution : Review your firewall rules policy Risk Factor : High BID : <a href="#">7436</a> Nessus ID : <a href="#">11580</a></p>
Informational	general/udp	<p>For your information, here is the traceroute to 10.1.201.218 : 10.1.201.39 10.1.201.218</p> <p>Nessus ID : <a href="#">10287</a></p>
Warning	general/tcp	<p>The remote host does not discard TCP SYN packets which have the FIN flag set.</p> <p>Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.</p> <p>See also : <a href="http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html">http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html</a> <a href="http://www.kb.cert.org/vuls/id/464113">http://www.kb.cert.org/vuls/id/464113</a></p> <p>Solution : Contact your vendor for a patch Risk factor : Medium BID : <a href="#">7487</a> Nessus ID : <a href="#">11618</a></p>
Warning	general/tcp	<p>The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself.</p> <p>Solution : drop source routed packets on this host or on other ingress routers or firewalls.</p> <p>Risk factor : Low Nessus ID : <a href="#">11834</a></p>
Informational	general/tcp	<p>The remote host is running Sun Solaris 8 Nessus ID : <a href="#">11936</a></p>
Warning	general/icmp	<p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>Risk factor : Low CVE : <a href="#">CAN-1999-0524</a> Nessus ID : <a href="#">10114</a></p>
Warning	general/icmp	<p>The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.248.0).</p>

<p><b>Vulnerability</b> sometimes-rpc21 (32779/tcp)</p>	<p>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.</p> <p>Solution : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17.</p> <p>Risk factor : Low            CVE : <a href="#">CAN-1999-0524</a>            Nessus ID : <a href="#">10113</a></p> <p>The remote Sun rpc.cmsd has integer overflow problem in xdr_array. An attacker may use this flaw to execute arbitrary code on this host with the privileges rpc.cmsd is running as (typically, root), by sending a specially crafted request to this service.</p> <p>Solution : We suggest that you disable this service and apply a new patch.            Risk factor : High            CVE : <a href="#">CVE-2002-0391</a>            BID : <a href="#">5356</a>            Nessus ID : <a href="#">11418</a></p>
---	---

This file was generated by [Nessus](#), the open-sourced security scanner.

## CISscan 1.4.0

```
# cd /opt/CIS; ./cis-scan
```

```
*****
***** CIS Security Benchmark Checker v1.4.0 *****
*
* Lead Developer : Jay Beale *
* Benchmark Coordinator and Gadfly : Hal Pomeranz *
*
* Copright 2001 - 2003 The Center for Internet Security www.cisecurity.org *
*
* Please send feedback to sol-scan@cisecurity.org. *
*****
```

Investigating system...this will take a few minutes...

\*\*\*\*\*

Now a final check for non-standard world-writable files, Set-UID and Set-GID programs -- this can take a whole lot of time if you have a large filesystem. Your score if there are no extra world-writable files or SUID/SGID programs found will be 3.29 / 10.00 . If there are extra SUID/SGID programs or world-writable files, your score could be as low as 3.01 / 10.00 .

You can hit CTRL-C at any time to stop at this remaining step.

The preliminary log can be found at: ./cis-most-recent-log

\*\*\*\*\*

Rating = 3.01 / 10.00

\*\*\*\*\*  
 To learn more about the results, do the following:

```
All results/diagnostics:
  more ./cis-ruler-log.20040219-12:48:31.29715
Positive Results Only:
  egrep "^Positive" ./cis-ruler-log.20040219-12:48:31.29715
Negative Results Only:
```

```
egrep "^Negative" ./cis-ruler-log.20040219-12:48:31.29715
```

For each item that you score or fail to score on, please reference the corresponding item in the CIS Benchmark Document.

For additional instructions/support, please reference the CIS web page:

<http://www.cisecurity.org>

```
# egrep "^Positive" ./cis-ruler-log.20040219-12:48:31.29715
Positive: 2.5 tftp is deactivated.
Positive: 3.2 Found a good daemon umask of 022 in /etc/default/init.
Positive: 5.4 cron usage is being logged.
Positive: 5.5 System accounting appears to be enabled.
Positive: 5.7 All logfile permissions and owners match benchmark recommendations.
Positive: 6.2 logging option is set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 /etc/dfs/dfstab doesn't have any non-fully qualified pathname share
commands.
Positive: 6.5 password and group files have right permissions and owners.
Positive: 6.6 all temporary directories have sticky bits set.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either don't exist or are
links to /dev/null.
Positive: 7.3 All users necessary are present in /etc/ftpusers
Positive: 7.11 Root is only allowed to login on console
Positive: 7.12 /etc/default/login allows 3 login attempts.
Positive: 8.2 All users have passwords
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.7 No user's home directory is world or group writable.
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc file.
```

```
egrep "^Negative" ./cis-ruler-log.20040219-12:48:31.29715
Negative: 1.1 System appears not to have been patched within the last month.
Negative: 1.2 tcp6-protocol service ftp in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service telnet in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service name in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service shell in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service shell in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service login in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service exec in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service exec in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service comsat in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service talk in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service uucp in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service finger in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service time in inetd.conf is not wrapped.
Negative: 1.2 udp6-protocol service time in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service echo in inetd.conf is not wrapped.
Negative: 1.2 udp6-protocol service echo in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service discard in inetd.conf is not wrapped.
Negative: 1.2 udp6-protocol service discard in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service daytime in inetd.conf is not wrapped.
Negative: 1.2 udp6-protocol service daytime in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service chargen in inetd.conf is not wrapped.
Negative: 1.2 udp6-protocol service chargen in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service fs in inetd.conf is not wrapped.
Negative: 1.2 tcp6-protocol service printer in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service dtspc in inetd.conf is not wrapped.
Negative: 1.3 System isn't running sshd.
Negative: 2.1 inetd listens on port time -- this port's line should be commented out or
deleted in inetd.conf.
Negative: 2.1 inetd listens on port echo -- this port's line should be commented out or
deleted in inetd.conf.
Negative: 2.1 inetd listens on port discard -- this port's line should be commented out
or deleted in inetd.conf.
Negative: 2.1 inetd listens on port daytime -- this port's line should be commented out
or deleted in inetd.conf.
```



Negative: 2.1 inetd listens on port chargen -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port fs -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port dtspc -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port exec -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port comsat -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port talk -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port finger -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port uucp -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port name -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100068/2-5 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100146/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100147/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100150/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100221/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100232/10 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port 100235/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port rstatd/2-4 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port rusersd/2-3 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port sprayd/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.1 inetd listens on port walld/1 -- this port's line should be commented out or deleted in inetd.conf.  
Negative: 2.2 telnet not deactivated.  
Negative: 2.3 ftp not deactivated.  
Negative: 2.4 rsh (shell) should be deactivated.  
Negative: 2.4 rlogin (rlogin) should be deactivated.  
Negative: 2.6 BSD-compatible printer server should be deactivated.  
Negative: 2.7 rquotad is not deactivated.  
Negative: 2.8 CDE-related daemon rpc.ttdbserverd not deactivated in inetd.conf.  
Negative: 2.8 CDE-related daemon fs.auto (port fs) not deactivated in inetd.conf.  
Negative: 2.8 CDE-related daemon kcms\_server not deactivated in inetd.conf.  
Negative: 2.10 kerberos net daemon ktkt\_warnd not deactivated in inetd.conf.  
Negative: 2.10 kerberos net daemon gssd not deactivated in inetd.conf.  
Negative: 3.1 Serial login prompt not disabled.  
Negative: 3.3 inetd is still active.  
Negative: 3.4 System is running syslogd without the -t switch, accepting remote logging.  
Negative: 3.5 Mail daemon is on and collecting mail from the network.  
Negative: 3.6 in.rarpd program has not been disabled in /etc/rc3.d/S15nfs.server.  
Negative: 3.6 rpc.bootparamd program has not been disabled in /etc/rc3.d/S15nfs.server.  
Negative: 3.6 in.rarpd program has not been disabled in /etc/rc3.d/S15nfs.server.  
Negative: 3.6 rpc.bootparamd program has not been disabled in /etc/rc3.d/S15nfs.server.  
Negative: 3.7 llc2 not deactivated.  
Negative: 3.7 uucp not deactivated.  
Negative: 3.7 slpd not deactivated.  
Negative: 3.7 PRESERVE not deactivated.  
Negative: 3.7 bdconfig not deactivated.  
Negative: 3.7 wbem not deactivated.  
Negative: 3.7 ncalogd not deactivated.  
Negative: 3.7 ncad not deactivated.  
Negative: 3.7 mipagent not deactivated.  
Negative: 3.7 autoinstall not deactivated.  
Negative: 3.7 asppp not deactivated.  
Negative: 3.7 cacheefs.daemon not deactivated.

Negative: 3.7 cacheos.finish not deactivated.  
Negative: 3.7 power not deactivated.  
Negative: 3.7 dmi not deactivated.  
Negative: 3.9 NFS Server script nfs.server not deactivated.  
Negative: 3.10 NFS script nfs.client not deactivated.  
Negative: 3.10 NFS script autofs not deactivated.  
Negative: 3.11 rpc rc-script (rpcbind) not deactivated.  
Negative: 3.14 LDAP cache manager not deactivated.  
Negative: 3.15 lp not deactivated.  
Negative: 3.15 spc not deactivated.  
Negative: 3.16 volume manager not deactivated.  
Negative: 3.17 Graphical login-related script dtlogin not deactivated.  
Negative: 3.18 Apache web server rc-script not deactivated.  
Negative: 3.19 SNMP daemon should be deactivated.  
Negative: 4.1 Coredumps aren't deactivated.  
Negative: 4.2 Stack is not set non-executable  
Negative: 4.2 Non-executable stack violation logging is not active.  
Negative: 4.3 NFS clients aren't restricted to privileged ports.  
Negative: 4.4 ip6 source routing (ip6\_forward\_src\_routed) should be deactivated  
Negative: 4.4 tcp\_ip\_abort\_cinterval should be at most 60,000 to avoid TCP flood problems.  
Negative: 4.4 ip\_respond\_to\_timestamp isn't 0.  
Negative: 4.4 ip\_respond\_to\_timestamp\_broadcast should be 0.  
Negative: 4.4 ip6 ignore\_redirect isn't set to 1.  
Negative: 4.4 ARP timer (arp\_cleanup\_interval) should be at most 60,000.  
Negative: 4.4 ARP timer (ip\_ire\_arp\_interval) should be at most 60,000  
Negative: 4.5 ip6\_strict\_dst\_multihoming isn't activated.  
Negative: 5.1 syslog does not permanently capture auth messages.  
Negative: 5.3 /var/adm/loginlog doesn't exist to track failed logins.  
Negative: 5.6 kernel-level auditing isn't enabled.  
Negative: 6.1 Never found separate /usr partition, so it couldn't be mounted read-only.  
Negative: 6.1 /opt is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u0 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u01 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u11 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u02 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u12 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u03 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /var is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /home is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u04 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u05 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u06 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u07 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u08 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.1 /u09 is not mounted non-SUID-capable (nosuid) or read-only (ro).  
Negative: 6.9 Fix-modes has not been run here.  
Negative: 7.1 /etc/pam.conf appears to support rhost auth.  
Negative: 7.4 /etc/shells does not exist.  
Negative: 7.5 /etc/dt/config/Xaccess doesn't exist, thus permits remote X-terminal login.  
Negative: 7.7 /etc/dt/config/ doesn't exist, so GUI screenlocker can't be configured.  
Negative: 7.8 Couldn't open cron.allow  
Negative: 7.8 Couldn't open at.allow  
Negative: 7.9 The permissions on /var/spool/cron/crontabs/adm are not sufficiently restrictive.  
Negative: 7.9 The permissions on /var/spool/cron/crontabs/lp are not sufficiently restrictive.  
Negative: 7.9 The permissions on /var/spool/cron/crontabs/uucp are not sufficiently restrictive.  
Negative: 7.10 EEPROM banner isn't on.  
Negative: 7.10 No authorized-use banner in /etc/motd.  
Negative: 7.10 /etc/issue doesn't have a authorized-use banner.  
Negative: 7.10 Couldn't open /etc/default/telnetd to test for BANNER line.  
Negative: 7.10 Couldn't open /etc/default/ftpd to test for BANNER line.  
Negative: 7.10 /etc/dt/config/ doesn't exist, so GUI welcome message couldn't have been changed.  
Negative: 7.13 EEPROM isn't password-protected.  
Negative: 8.1 uucp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.  
Negative: 8.1 listen has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 nobody4 has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 adm has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 daemon has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 bin has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 lp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 nobody has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 noaccess has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.3 User ddoe should have a minimum password life of at least 7 days.

Negative: 8.3 User ddoe should have a maximum password life of between 1 and 91 days.

Negative: 8.3 User ddoe should have a password expiration warning of at least 7 days.

Negative: 8.3 User msmith should have a minimum password life of at least 7 days.

Negative: 8.3 User msmith should have a maximum password life of between 1 and 91 days.

Negative: 8.3 User msmith should have a password expiration warning of at least 7 days.

Negative: 8.3 /etc/default/passwd doesn't have a value for MAXWEEKS.

Negative: 8.3 /etc/default/passwd doesn't have a value for MINWEEKS.

Negative: 8.3 /etc/default/passwd doesn't have a value for WARNWEEKS.

Negative: 8.6 Directory /opt/Navisphere/bin is in root's PATH and is group-writable.

Negative: 8.10 File /etc/default/ftpd cannot be opened, so the umask setting can't be set.

Negative: 8.11 /etc/profile should have mesg n to block talk/write commands and strengthen permissions on user tty.

Negative: 8.11 /etc/.login should have mesg n to block talk/write commands and strengthen permissions on user tty.

Negative: 6.7 Non-standard world-writable file: /etc/vx/array.info

Negative: 6.7 Non-standard world-writable file: /var/vx/isis/tasklog/logfile0.log

Negative: 6.7 Non-standard world-writable file: /var/adm/log/agent.pid

Negative: 6.7 Non-standard world-writable file: /var/vx/isis/state

Negative: 6.7 Non-standard world-writable file: /var/vx/isis/alertlog/alert.log

Negative: 6.8 Non-standard SUID program /usr/lib/fbconfig/SUNWpfb\_config

Negative: 6.8 Non-standard SGID program /usr/platform/SUNW,Sun-Fire-V240/sbin/scadm

## UnixAudit.sh

```
=== Hostname: giacunixhost.giac-fortune.com =====
=== OS Details: SunOS giacunixhost 5.8 Generic_108528-27 sun4u sparc SUNW,Sun-Fire-V440
=====
=== Date Audited: Tue Feb 17 11:08:48 EST 2004 =====

=== /etc/passwd ===
FILE PERMISSION: -r--r--r-- 1 root sys 643 Feb 3 10:05 /etc/passwd
root:x:0:1:Super-User:/root:/usr/bin/ksh
daemon:x:1:1:/:
bin:x:2:2:/:usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
ddoe:x:100:1:Don Doe, 555-1414:/home/ddoe:/usr/bin/ksh
msmith:x:101:1:Mike Smith, 555-1212, Portland Office:/home/msmith:/bin/sh
=====
```

```

=== /etc/shadow ===
FILE PERMISSION: -r----- 1 root sys 316 Feb 10 12:52 /etc/shadow
root:X2.XnN5pwtFzQ:6445:.....:
daemon:NP:6445:.....:
bin:NP:6445:.....:
sys:NP:6445:.....:
adm:NP:6445:.....:
lp:NP:6445:.....:
uucp:NP:6445:.....:
nuucp:NP:6445:.....:
listen:*LK*:.....:
nobody:NP:6445:.....:
noaccess:NP:6445:.....:
nobody4:NP:6445:.....:
ddoe:vIlpNp85LcpmU:12430:.....:
msmith:CnhfswEFmgbyA:12432:.....:
=====

=== /etc/group ===
FILE PERMISSION: -rw-r--r-- 1 root sys 288 Feb 3 10:44 /etc/group
root::0:root
other::1:
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
uucp::5:root,uucp
mail::6:root
tty::7:root,tty,adm
lp::8:root,lp,adm
nuucp::9:root,nuucp
staff::10:
daemon::12:root,daemon
sysadmin::14:
nobody::60001:
noaccess::60002:
nogroup::65534:
dba::101:
=====

=== /etc/inetd.conf ===
FILE PERMISSION: lrwxrwxrwx 1 root root 17 Jan 13 10:11 /etc/inetd.conf ->
./inet/inetd.conf
#
# Copyright 1989-2002 Sun Microsystems, Inc. All rights reserved.
# Use is subject to license terms.
#
#ident "@(#)inetd.conf 1.45 02/11/05 SMI" /* SVr4.0 1.5 */
#
# 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.
#
# Ftp and telnet are standard Internet services.
#
ftp      stream tcp6    nowait root    /usr/sbin/in.ftpd      in.ftpd
telnet   stream tcp6    nowait root    /usr/sbin/in.telnetd   in.telnetd
#
# Tnamed serves the obsolete IEN-116 name server protocol.
#
name     dgram  udp      wait    root    /usr/sbin/in.tnamed    in.tnamed
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
shell    stream tcp      nowait root    /usr/sbin/in.rshd      in.rshd
shell    stream tcp6     nowait root    /usr/sbin/in.rshd      in.rshd
login    stream tcp6     nowait root    /usr/sbin/in.rlogind   in.rlogind
exec     stream tcp      nowait root    /usr/sbin/in.rexecd    in.rexecd
exec     stream tcp6     nowait root    /usr/sbin/in.rexecd    in.rexecd
comsat   dgram  udp       wait    root    /usr/sbin/in.comsat    in.comsat
talk     dgram  udp       wait    root    /usr/sbin/in.talkd     in.talkd
#
# Must run as root (to read /etc/shadow); "-n" turns off logging in utmp/wtmp.
#
uucp     stream tcp      nowait root    /usr/sbin/in.uucpd     in.uucpd
#
# Tftp service is provided primarily for booting. Most sites run this
# only on machines acting as "boot servers."
#
#tftp    dgram  udp6      wait    root    /usr/sbin/in.tftpd     in.tftpd -s /tftpboot
#
# 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.
#
finger   stream tcp6     nowait nobody /usr/sbin/in.fingerd   in.fingerd
#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,udp      wait      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
#
# Rquotad supports UFS disk quotas for NFS clients
#
rquotad/1      tli      rpc/datagram_v wait root /usr/lib/nfs/rquotad      rquotad
#
# The rusers service gives out user information. Sites concerned
# with security may choose to disable it.
#
rusersd/2-3    tli      rpc/datagram_v,circuit_v      wait root
/usr/lib/netsvc/rusers/rpc.rusersd      rpc.rusersd
#
# The spray server is used primarily for testing.
#
sprayd/1       tli      rpc/datagram_v wait root /usr/lib/netsvc/spray/rpc.sprayd
rpc.sprayd
#
# The rwall server allows others to post messages to users on this machine.
#
walld/1        tli      rpc/datagram_v wait root /usr/lib/netsvc/rwall/rpc.rwalld
rpc.rwalld
#
# Rstatd is used by programs such as perfmeter.
#
rstatd/2-4     tli      rpc/datagram_v wait root /usr/lib/netsvc/rstat/rpc.rstatd rpc.rstatd
#
# The rexd server provides only minimal authentication and is often not run
#
# rexd/1        tli      rpc/tcp wait root /usr/sbin/rpc.rexd      rpc.rexd
#
# 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
#
# UFS-aware service daemon
#
# ufsd/1 tli      rpc/*  wait      root      /usr/lib/fs/ufs/ufsd  ufsd -p
#
# Sun KCMS Profile Server
#
100221/1       tli      rpc/tcp wait root /usr/openwin/bin/kcms_server      kcms_server
#
# Sun Font Server
#
fs             stream tcp      wait nobody /usr/openwin/lib/fs.auto fs
#
# CacheFS Daemon
#
100235/1 tli rpc/ticotsord wait root /usr/lib/fs/cachefs/cachefsd cachefsd
#
# Kerberos V5 Warning Message Daemon
#
100134/1       tli      rpc/ticotsord wait      root      /usr/lib/krb5/ktkt_warnd ktkt_warnd
#
# Print Protocol Adaptor - BSD listener
#
printer        stream tcp6     nowait root      /usr/lib/print/in.lpd in.lpd
#
# GSS Daemon

```

```

#
100234/1      tli      rpc/ticotsord  wait   root    /usr/lib/gss/gssd gssd
#
# AMI Daemon
#
100146/1      tli      rpc/ticotsord  wait   root    /usr/lib/security/amiserv  amiserv
100147/1      tli      rpc/ticotsord  wait   root    /usr/lib/security/amiserv  amiserv
#
# OCF (Smart card) Daemon
#
100150/1      tli      rpc/ticotsord  wait   root    /usr/sbin/ocfserve  ocfserve
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
=====

=== /etc/default/passwd ===
FILE PERMISSION: -r--r--r-- 1 root sys 74 Jan 13 10:12
/etc/default/passwd
#ident "@(#)passwd.dfl 1.3 92/07/14 SMI"
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6
=====

=== /etc/default/login ===
FILE PERMISSION: -r--r--r-- 1 root sys 2043 Jan 15 9:35 /etc/default/login
# ident "@(#)login.dfl 1.13 03/01/10 SMI"
#
# Copyright 1989-2002 Sun Microsystems, Inc. All rights reserved.
# Use is subject to license terms.
#

# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT

# ULIMIT sets the file size limit for the login. Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0

# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console

# PASSREQ determines if login requires a password.
#
PASSREQ=YES

# ALTSHELL determines if the SHELL environment variable should be set
#
ALTSHELL=YES

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
SUPATH=/usr/sbin:/usr/bin

# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
#
TIMEOUT=60

# UMASK sets the initial shell file creation mode mask. See umask(1).
#
UMASK=022

```

```

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all root logins at level LOG_NOTICE and multiple failed login
# attempts at LOG_CRIT.
#
SYSLOG=YES

# SLEEPTIME controls the number of seconds that the command should
# wait before printing the "login incorrect" message when a
# bad password is provided. The range is limited from
# 0 to 5 seconds.
#
#SLEEPTIME=4

# DISABLETIME If present, and greater than zero, the number of seconds
# login will wait after RETRIES failed attempts or the PAM framework returns
# PAM_ABORT. Default is 20. Minimum is 0. No maximum is imposed.
#
#DISABLETIME=20

# RETRIES determines the number of failed logins that will be
# allowed before login exits.
#
RETRIES=3
#
# The SYSLOG_FAILED_LOGINS variable is used to determine how many failed
# login attempts will be allowed by the system before a failed login
# message is logged, using the syslog(3) LOG_NOTICE facility. For example,
# if the variable is set to 0, login will log -all- failed login attempts.
#
SYSLOG_FAILED_LOGINS=0
=====

=== /etc/syslog.conf ===
FILE PERMISSION: -rw-r--r-- 1 root sys 1001 Jan 13 10:12 /etc/syslog.conf
#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 *
)

# Added to increase inetd logging

```



```

# also added the "-t" to the inetd startup
daemon.debug                               /var/log/connlog
=====

=== /etc/dfs/dfstab ===
FILE PERMISSION: -rw-r--r--    1 root      sys          393 Jan 13 10:12 /etc/dfs/dfstab

#      Place share(1M) commands here for automatic execution
#      on entering init state 3.
#
#      Issue the command '/etc/init.d/nfs.server start' to run the NFS
#      daemon processes and the share commands, after adding the very
#      first entry to this file.
#
#      share [-F fstype] [ -o options] [-d "<text>"] <pathname> [resource]
#      .e.g,
#      share -F nfs  -o rw=engineering -d "home dirs" /export/home2
#
=====

=== /etc/default/su ===
FILE PERMISSION: -r--r--r--    1 root      sys          703 Jan 13 10:12 /etc/default/su
#ident "@(#)su.dfl    1.6      93/08/14 SMI" /* SVr4.0 1.2 */

# SULONG determines the location of the file used to log all su attempts
#
SULONG=/var/adm/sulog

# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
#CONSOLE=/dev/console

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all su attempts. LOG_NOTICE messages are generated for su's to
# root, LOG_INFO messages are generated for su's to other users, and LOG_CRIT
# messages are generated for failed su attempts.
#
SYSLOG=YES
=====

=== /etc/default/inetinit ===
FILE PERMISSION: -r--r--r--    1 root      sys          367 Jan 13 10:12
/etc/default/inetinit
# @(#)inetinit.dfl 1.2 97/05/08
#
# TCP_STRONG_ISS sets the TCP initial sequence number generation parameters.
# Set TCP_STRONG_ISS to be:
#      0 = Old-fashioned sequential initial sequence number generation.
#      1 = Improved sequential generation, with random variance in increment.
#      2 = RFC 1948 sequence number generation, unique-per-connection-ID.
#
TCP_STRONG_ISS=2
=====

=== showmount -d ===
showmount: giacunixhost: RPC: Program not registered
=====

=== showmount -e ===
showmount: giacunixhost: RPC: Program not registered
=====

=== ifconfig -a ===

```

```

lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
ce0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.1.201.218 netmask fffff800 broadcast 10.1.207.255
    ether 0:3:ba:43:79:c7
=====

=== passwd -sa ===
root      PS
daemon    LK
bin        LK
sys        LK
adm        LK
lp         LK
uucp       LK
nuucp      LK
listen     LK
nobody     LK
noaccess   LK
nobody4    LK
ddoe       PS
msmith     PS
=====

=== find / -nouser -ls ===
=====

=== find / -name .rhosts -exec echo == {} == ; -exec cat {} ; ===
=====

=== find / -name .netrc -exec echo == {} == ; -exec cat {} ; ===
=====

=== find / -perm -0007 -type d -ls ===
174593    1 drwxrwxrwt    3 root    mail    512 Feb 13 16:29 /var/mail
202753    1 drwxrwxrwt    2 root    bin     512 Jan 13 10:11 /var/preserve
10041549   8 drwxrwxrwt    2 root    root    117 Feb 12 15:32 /var/run/rpc_door
270337    1 drwxrwxrwt    2 root    bin     512 Jan 13 10:11 /var/spool/pkg
84497     1 drwxrwxrwt    2 uucp    uucp    512 Jan 13 10:28 /var/spool/uucppublic
275969    1 drwxrwxrwt    3 root    sys     512 Feb 17 11:08 /var/tmp
636422    1 drwxrwxrwt    2 root    root    512 Jan 13 10:17
/var/dt/dtpower/schemes
11280     1 drwxrwxrwt    2 root    root    512 Jan 13 10:45 /var/dt/tmp
10849727   8 drwxrwxrwt    6 root    sys     960 Feb 17 11:00 /tmp
=====

=== find / -perm -2 -type f -ls ===
11267     0 -rw-rw-rw-    1 root    root    0 Jan 13 10:09
/var/sadm/install/.pkg.lock
630790    1 -rw-rw-rw-    1 root    root    8 Sep 23 1999
/var/dt/dtpower/_current_scheme
647715   160 -rw-rw-rw-    1 root    root    147504 Feb 12 15:32
/var/vx/isis/alertlog/alert.log
84492     1 -rw-rw-rw-    1 root    root    88 Jan 13 14:56
/var/vx/isis/tasklog/logfile0.log
642079    1 -rwxrwxrwx    1 root    root    16 Feb 12 15:32 /var/vx/isis/state
506895    2 ------rw-    1 root    root    1771 Jan 16 08:37
/opt/ecc/exec/MSR510.rcfile
247928    1 -rw-rw-rw-    1 bin     bin     137 Jun 2 1999
/usr/dt/appconfig/jmf/jmf.properties
878708    0 -rw--w--w-    1 bin     bin     0 Jan 5 2000 /usr/oasys/tmp/TERRLOG
523973    1 -rw-rw-rw-    1 root    other   60 Feb 12 16:39 /etc/vx/array.info
8212573   0 -rw-rw-rw-    1 root    root    0 Feb 12 15:32 /tmp/.X11-pipe/X0
=====

=== lsof -i ===
COMMAND    PID    USER    FD    TYPE    DEVICE SIZE/OFF NODE NAME
vxsvc      248    root     5u     IPv4    0x300053b5828 0t0 TCP *:2148 (LISTEN)
vxsvc      248    root    11u     IPv4    0x3000562b0c8 0t0 UDP *:2148 (Idle)
vxsvc      248    root    12u     IPv4    0x30006b15310 0t0 TCP giacunixhost:2148-
>giachosta.giac-fortune.com:45707 (CLOSE_WAIT)

```

vxsvc	248	root	13u	IPv4	0x30006afcf88	0t0	TCP	giacunixhost:2148-
>giachosta.giac-fortune.com:45716 (CLOSE WAIT)								
vxsvc	248	root	14u	IPv4	0x30006b15bd0	0t0	TCP	giacunixhost:2148-
>giachosta.giac-fortune.com:45727 (CLOSE WAIT)								
vxsvc	248	root	15u	IPv4	0x30006b1eb70	0t0	TCP	giacunixhost:2148-
>giachosta.giac-fortune.com:45997 (CLOSE WAIT)								
rpcbind	275	root	3u	IPv4	0x30005215458	0t0	UDP	*:sunrpc (Idle)
rpcbind	275	root	4u	IPv4	0x300052c6920	0t0	UDP	*: (Unbound)
rpcbind	275	root	5u	IPv4	0x300052c66a0	0t0	UDP	*:32771 (Idle)
rpcbind	275	root	6u	IPv4	0x300052c62e0	0t0	TCP	*:sunrpc (LISTEN)
rpcbind	275	root	7u	IPv4	0x300052c6060	0t0	TCP	*: (IDLE)
inetd	313	root	11u	IPv6	0x300053b46a8	0t0	TCP	*:ftp (LISTEN)
inetd	313	root	12u	IPv6	0x300053b4428	0t0	TCP	*:telnet (LISTEN)
inetd	313	root	13u	IPv4	0x300053b41a8	0t0	UDP	*:name (Idle)
inetd	313	root	14u	IPv4	0x30005453e70	0t0	TCP	*:shell (LISTEN)
inetd	313	root	15u	IPv6	0x30005453bf0	0t0	TCP	*:shell (LISTEN)
inetd	313	root	16u	IPv6	0x30005453970	0t0	TCP	*:login (LISTEN)
inetd	313	root	17u	IPv4	0x300054536f0	0t0	TCP	*:exec (LISTEN)
inetd	313	root	18u	IPv6	0x30005453470	0t0	TCP	*:exec (LISTEN)
inetd	313	root	19u	IPv4	0x300054531f0	0t0	UDP	*:biff (Idle)
inetd	313	root	20u	IPv4	0x30005452f70	0t0	UDP	*:talk (Idle)
inetd	313	root	21u	IPv4	0x30005452cf0	0t0	TCP	*:uucp (LISTEN)
inetd	313	root	22u	IPv6	0x30005452a70	0t0	TCP	*:finger (LISTEN)
inetd	313	root	23u	IPv6	0x300054527f0	0t0	TCP	*:time (LISTEN)
inetd	313	root	24u	IPv6	0x30005452570	0t0	UDP	*:time (Idle)
inetd	313	root	25u	IPv6	0x300054522f0	0t0	TCP	*:echo (LISTEN)
inetd	313	root	26u	IPv6	0x30005452070	0t0	UDP	*:echo (Idle)
inetd	313	root	27u	IPv6	0x300054ffdf38	0t0	TCP	*:discard (LISTEN)
inetd	313	root	28u	IPv6	0x300054ffab8	0t10099	UDP	*:discard (Idle)
inetd	313	root	29u	IPv6	0x300054fff838	0t0	TCP	*:daytime (LISTEN)
inetd	313	root	30u	IPv6	0x300054fff5b8	0t0	UDP	*:daytime (Idle)
inetd	313	root	31u	IPv6	0x300054fff338	0t0	TCP	*:chargen (LISTEN)
inetd	313	root	32u	IPv6	0x300054fff0b8	0t0	UDP	*:chargen (Idle)
inetd	313	root	33u	IPv4	0x300054fecf8	0t0	UDP	*:32773 (Idle)
inetd	313	root	34u	IPv4	0x300054fee38	0t0	UDP	*:32774 (Idle)
inetd	313	root	36u	IPv4	0x300054fe938	0t0	UDP	*:32775 (Idle)
inetd	313	root	38u	IPv4	0x300053b4928	0t0	TCP	*:32772 (LISTEN)
inetd	313	root	41u	IPv4	0x300054fe578	0t0	UDP	*:32776 (Idle)
inetd	313	root	43u	IPv4	0x300054fe1b8	0t0	UDP	*:32777 (Idle)
inetd	313	root	45u	IPv4	0x300054e7e80	0t0	UDP	*:32778 (Idle)
inetd	313	root	47u	IPv4	0x300054e7c00	0t0	TCP	*:32773 (LISTEN)
inetd	313	root	48u	IPv4	0x300054e7980	0t0	TCP	*:32774 (LISTEN)
inetd	313	root	49u	IPv4	0x300054e7700	0t0	TCP	*:fs (LISTEN)
inetd	313	root	52u	IPv6	0x300054e7340	0t0	TCP	*:printer (LISTEN)
inetd	313	root	57u	IPv4	0x300054e6f80	0t0	TCP	*:dtspc (LISTEN)
inetd	313	root	58u	IPv4	0x300054e6bc0	0t0	UDP	*:32779 (Idle)
lockd	314	root	4u	IPv4	0x300054fe2f8	0t0	UDP	*:lockd (Idle)
lockd	314	root	5u	IPv4	0x300054e6940	0t0	TCP	*:lockd (LISTEN)
statd	315	daemon	3u	IPv4	0x300053b5468	0t0	UDP	*: (Unbound)
statd	315	daemon	4u	IPv4	0x300053b51e8	0t0	UDP	*:32772 (Idle)
statd	315	daemon	5u	IPv4	0x300053b4ce8	0t0	TCP	*:32771 (LISTEN)
syslogd	328	root	3u	IPv4	0x300054e6300	0t0	UDP	*:syslog (Idle)
naviagent	366	root	3u	IPv4	0x300054e6080	0t0	TCP	*:6389 (LISTEN)
bvcontrol	396	root	3u	IPv4	0x300052c6420	0t0	TCP	*:bvcontrol (LISTEN)
dtlogin	504	root	6u	IPv4	0x30005790f90	0t0	UDP	*:177 (Idle)
dtlogin	504	root	7u	IPv4	0x30005790d10	0t0	TCP	*:32776 (LISTEN)
snmpdx	550	root	4u	IPv4	0x30005790a90	0t0	UDP	*:161 (Idle)
snmpdx	550	root	5u	IPv4	0x30003f70f98	0t0	UDP	*:32787 (Idle)
snmpdx	550	root	6u	IPv4	0x30003ea8590	0t0	UDP	*:32788 (Idle)
dmispd	557	root	3u	IPv4	0x30005791350	0t0	UDP	*:32782 (Idle)
dmispd	557	root	4u	IPv4	0x30005790590	0t0	TCP	*:32778 (LISTEN)
mstragent	580	root	8u	IPv4	0x30005921c18	0t0	TCP	*:5798 (LISTEN)
mstragent	580	root	10u	IPv4	0x30006b1c178	0t0	TCP	*:57703 (BOUND)
mstragent	580	root	12u	IPv4	0x300059201d8	0t0	TCP	localhost:5798-
>localhost:32784 (ESTABLISHED)								
mibiisa	592	root	0u	IPv4	0x30003f70a98	0t0	UDP	*:32786 (Idle)
msragent	593	root	8u	IPv4	0x30005920bd8	0t0	TCP	localhost:32784-
>localhost:5798 (ESTABLISHED)								
msragent	593	root	9u	IPv4	0x300059206d8	0t0	TCP	*:10555 (LISTEN)
sendmail	4801	root	4r	IPv4	0x30005791710	0t0	UDP	*: (Unbound)
sendmail	4801	root	6u	IPv4	0x30006b17588	0t0	TCP	*:smtp (LISTEN)

```

sendmail 4801 root 7u IPv6 0x30005f08f38 0t0 TCP *:smtp (LISTEN)
sendmail 4801 root 8u IPv4 0x30006b1fa70 0t0 TCP *:submission (LISTEN)
xfs 12324 nobody 0u IPv4 0x300054e7700 0t0 TCP *:fs (LISTEN)
xfs 12324 nobody 1u IPv4 0x300054e7700 0t0 TCP *:fs (LISTEN)
rpc.ttdbs 12325 root 0u IPv4 0x300054e7c00 0t0 TCP *:32773 (LISTEN)
rpc.ttdbs 12325 root 1u IPv4 0x300054e7c00 0t0 TCP *:32773 (LISTEN)
rpc.ttdbs 12325 root 2u IPv4 0x300054e7c00 0t0 TCP *:32773 (LISTEN)
java 12345 root 11u IPv4 0x30005f09938 0t0 TCP *:5987 (LISTEN)
java 12345 root 13u IPv4 0x3000562aa88 0t0 TCP *:36441 (LISTEN)
java 12345 root 15u IPv4 0x30005f09e38 0t0 TCP *:898 (LISTEN)
in.tnamed 16418 root 0u IPv4 0x300053b41a8 0t0 UDP *:name (Idle)
in.tnamed 16418 root 1u IPv4 0x300053b41a8 0t0 UDP *:name (Idle)
in.tnamed 16418 root 2u IPv4 0x300053b41a8 0t0 UDP *:name (Idle)
rpc.cmsd 16992 daemon 0u IPv4 0x300054e6bc0 0t0 UDP *:32779 (Idle)
rpc.cmsd 16992 daemon 1u IPv4 0x300054e6bc0 0t0 UDP *:32779 (Idle)
rpc.cmsd 16992 daemon 5u IPv4 0x30006b13598 0t0 TCP *:36583 (LISTEN)
in.telnet 16996 root 0u IPv4 0x30006b1e530 0t101 TCP giacunixhost:telnet-
>10.1.206.66:1318 (ESTABLISHED)
in.telnet 16996 root 1u IPv4 0x30006b1e530 0t101 TCP giacunixhost:telnet-
>10.1.206.66:1318 (ESTABLISHED)
in.telnet 16996 root 2u IPv4 0x30006b1e530 0t101 TCP giacunixhost:telnet-
>10.1.206.66:1318 (ESTABLISHED)
sadmind 17040 root 0u IPv4 0x300054fecf8 0t0 UDP *:32773 (Idle)
sadmind 17040 root 1u IPv4 0x300054fecf8 0t0 UDP *:32773 (Idle)
sadmind 17040 root 2u IPv4 0x300054fecf8 0t0 UDP *:32773 (Idle)
in.telnet 17042 root 0u IPv4 0x30005f09078 0t101 TCP giacunixhost:telnet-
>10.1.206.66:1334 (ESTABLISHED)
in.telnet 17042 root 1u IPv4 0x30005f09078 0t101 TCP giacunixhost:telnet-
>10.1.206.66:1334 (ESTABLISHED)
in.telnet 17042 root 2u IPv4 0x30005f09078 0t101 TCP giacunixhost:telnet-
>10.1.206.66:1334 (ESTABLISHED)
=====

```

## John 1.6.36

```

# ./john --wordlist=/usr/dict/all --rules sample-passwd.txt
Loaded 3 password hashes with 3 different salts (Traditional DES [64/64 BS])
guesses: 0 time: 0:00:00:03 0% c/s: 288446 trying: correles - corserez
guesses: 0 time: 0:00:00:04 0% c/s: 290569 trying: perpétue - perse'cu
guesses: 0 time: 0:00:00:05 0% c/s: 291155 trying: tunge - typesitu
guesses: 0 time: 0:00:00:06 0% c/s: 291897 trying: Pamella - Pantheon
guesses: 0 time: 0:00:01:35 12% c/s: 251207 trying: sgninotr - leotsrei
guesses: 0 time: 0:00:02:48 19% c/s: 255523 trying: rlinf2 - rlv2
guesses: 0 time: 0:00:05:19 45% c/s: 248381 trying: tztunsuA - tgufeB
guesses: 0 time: 0:00:08:19 70% c/s: 248655 trying: Volkje6 - Wegebt6
guesses: 0 time: 0:00:10:09 83% c/s: 248718 trying: 5macwd - 5maddux
guesses: 0 time: 0:00:10:56 89% c/s: 248907 trying: Fbapathe - Fbjoinns
guesses: 0 time: 0:00:11:35 100% c/s: 248181 trying: Zinkwegg - Wysifigg
#
#./john --show sample-passwd.txt
0 passwords cracked, 3 left

```

## References

---

Acheson, Green and Hal Pomeranz. Track 6 – Securing UNIX - 6.3 Topics in UNIX Security. The Sans Institute, 2003.

“Awareness Materials/Activities.” January 2004.  
URL: <http://csrc.nist.gov/ATE/materials.html> (26 Feb 2004).

“Central Loghost Mini-HOWTO.” URL: <http://www.campin.net/newlogcheck.html> (18 Feb 2004)

“CIS benchmark and scoring tool for Solaris.” October 2003.  
URL: [http://www.cisecurity.org/bench\\_solaris.html](http://www.cisecurity.org/bench_solaris.html) (19 Feb 2004)

Gellens, R. and J. Klensin. “Request for Comments: 2476 Message Submission.” December 1998. URL: <http://www.ietf.org/rfc/rfc2476.txt> (19 Feb 2004)

“John the Ripper password cracker.” URL: <http://www.openwall.com/john/> (19 Feb 2004)

“Nessus.” URL: <http://www.nessus.org> (16 Feb 2004).

“NMAP Introduction.” URL: <http://www.insecure.org/nmap/index.html> (20 Feb 2004).

Pomeranz, Hal. Track 6 – Securing UNIX - 6.2 Unix Security Tools. The Sans Institute, 2003.

Pomeranz, Hal. Track 6 – Securing UNIX - 6.5 Unix Practicum. The Sans Institute, 2003.

“Sun Security Coordination Team.” URL:  
<http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec>> (20 Feb 2004).

“Syslog-ng FAQ.” URL: <http://www.campin.net/syslog-ng/faq.html> (28 Feb 2004).