



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.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Linux/Unix (Security 506)"
at <http://www.giac.org/registration/gcux>

**Security Audit Assessment for
GIAC Enterprises**

November 15 - 17, 2000

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

Table of Contents

<u>EXECUTIVE SUMMARY</u>	2
<u>DETAILED ANALYSIS</u>	3
Operating System	3
Configuration	3
Third Party Software	5
Administrative Practices	5
Security Patches	6
Sensitive Data	6
Data Encryption via Internet Connections	7
Access Restrictions	7
Backup Policies - Disaster Preparedness	7
Other Issues	7
Sensitive Data	6
Data Encryption via Internet Connections	7
Access Restrictions	7
<u>SECURITY VULNERABILITIES PRIORITIZED</u>	9
<u>RECOMMENDED FIXES FOR VULNERABILITES</u>	9
<u>APPENDIX A (Nessus Report)</u>	11
<u>APPENDIX B (Nmap Scans)</u>	24
<u>APPENDIX C (Sample Configuration Files)</u>	28
<u>APPENDIX D (Patchdiag Report)</u>	30
<u>APPENDIX E (Sample files)</u>	38
<u>REFERENCES</u>	39

Executive Summary

The following document details the security audit conducted at GIAC Enterprises from Nov 15, 2000 - Nov 17, 2000 by D&G SecureWorld Consulting. GIAC Enterprises has made a bold new position on the Internet and having a robust security posture is **VITAL** towards its success. During the course of this audit we evaluated several different aspects of GIAC's security infrastructure and have provided detailed reports herein.

All security practices at GIAC enterprises have been evaluated against industry standards and recommendations to alleviate any discovered vulnerabilities have been described.

Overall the security posture at GIAC Enterprises has presented some causes for concern. While most systems are secure from the majority of most external Internet attacks due to a secure firewall configuration. The internal network security has many areas that should be addressed and corrected immediately. Areas that should see immediate correction are: No encryption of any kind, system patch levels, restrict permissions and physical security of facilities. Training and use of security auditing tools should also be addressed.

During the course of this audit one system had a detailed security analysis performed on it with complete support of the IT Department. The system audited was the primary pre-production web server (preweb001) and all findings are described in detail.

© SANS Institute 2000 - 2002

Detailed Analysis

Operating System

The operating system run by all GIAC machines is Sun Solaris 2.7. This is the current recommended release for a production environment. Steps should be taken to evaluate the transition to the latest OS Sun has to offer - Solaris 8 - when it becomes stable. Solaris 8 has many "fixes" to common problems as well as enhancements to existing products but is still too new for an internet production environment and a security stance.

The current security state of preweb001 was evaluated using security tools widely available on the internet. The Nessus Security Scanner(1) and Nmap Scanner(2) were both utilized to conduct an initial security posture scan. Intrusion attempts against other vulnerabilities (sendmail, nfs, dns, etc) were made from a secondary workstation internal to the organization and from machines outside the firewall. All attempts to access the system from outside the firewall were denied and logged. Attempts to access preweb001 from internal machines failed but several areas of concern were documented by Nessus. The full Nessus report is available in Appendix A. It is recommended that all the fixes suggested by Nessus be implemented unless an absolute valid need for these services to be open exists. Care should still be taken to secure these ports as well as possible. Detailed Nmap scans are available in Appendix B also.

Configuration

System configuration of preweb001 needs to be revamped. This system was initially installed while connected to the network. You should install systems and secure them first before connecting them to the network. Systems are also loaded "Full w/OEM" support. This requires too many unnecessary software packages to be installed on the server. This in turn means more pieces of software can be exploited and more pieces of software that must be patched against discovered vulnerabilities. Only software packages specifically needed should be installed from the OS Media. This is the first step towards any new installation. All systems should be installed to meet the need of the system.

Other configuration issues -

Sendmail - Common source of most security risks - Sendmail is required on this system but only delivers outgoing system mail. Sendmail should not be run in daemon mode and this system should be configured as a nullclient. The configuration file for sendmail is then a simple setup.

```
Include(`../m4/cf.m4`)  
OSTYPE(`solaris2`)  
FEATURE(`nullclient`, `mailhub`)
```

A simple cronjob can then deliver any system mail that gets stalled in the system queue.

```
0 * * * * /usr/lib/sendmail -q
```

A good source of sendmail information is available from O'Reilly and Associates "Sendmail 2nd Edition" (3)

FTP - Another common exploit. Care should be taken using this on a production server. Running the FTP server in a chroot'd environment is a good security precaution as this limits access of the users to your system while running FTP. No restrictions are placed on the FTP user list either. Root has full ability to login via FTP (Root logins via telnet/rlogin and rsh have been commented out thou.) It is recommended that a new ftp server be positioned running the OpenSSH(4) version of ftp.

Telnet/RSH/Rlogin - Unsecure protocol (Same as FTP). Any communication over this protocol is unsecure and can be intercepted and viewed in plain text by anyone who can "Sniff" you network traffic. SSH is the adopted standard and provides all existing functionality of these protocols and is a secure transmission. OpenSSH is again the place for this information. Commercial productions with support are also available.

.Rhosts - Use .rhosts files and lack of any encryption tunnels is also another area that needs immediate attention. Compromising the root user on one system gives immediate access to other servers on the network. All .rhosts files should be removed. Even a better solution is to create empty .rhosts files that are owned by root to prevent a malicious user or hacker from tampering with

.rhosts files. This was a common exploit with earlier versions of sendmail.

Unnecessary Services - Removal of all unnecessary services is recommended. NFS/Telnet/Calendar/Etc. Nessus report has this information.

Other configuration issues - Several changes should be implemented to your system files. These will prevent someone using your system as a relay bounce and eliminate certain Denial of Service attacks. Examples of these changes are documented in Appendix C.

Third Party Software

The only third party software packages necessary on this server are Apache Web Server(5), Solstice Networker Backup(6), Perl(7) and OpenSSH. No other third party packages are installed.

Apache Web Server - Known exploits for older versions of this software are widely available. It is one of the most widely used servers on the internet today. You also need to update immediately to the latest version of Apache. 1.3.6 is an out-of-date version. 1.3.14 is currently the latest version available. You should change the signature reported by this web server to prevent assaults against it also.

Solstice Backup - Currently running latest version of this product. All backups are performed over TCP connections and should be tunnnled via OpenSSH for the most secure posture. Sniffing again becomes an issue here.

Perl - Required for CGI Binaries on the Apache Web Server. Make sure latest version is installed. Know exploits for older versions exist.

OpenSSH - Not currently installed. Suggest IMMEDIATE installation of this product and disabling all unsecured protocols.

Administrative Practices

Currently users are required to change passwords and all people who access the system are required to sign and verify they know all policies when they log into the

system. Backups are performed and access is restricted via SUDO(8) to applications that require super-user access. Administrative practices are quite good. Some suggestions are listed below.

Acceptable Use Policy (AUP) - Displayed on the system prior to logging in and that all users are required to re-read and document the AUP quarterly instead of when just getting an account assigned.

Password Policies - Users need to change passwords at least every 90 days. Document these changes. Enforcing a strict set of passwords is also a good idea. No easily guessable passwords should be allowed. Do not allow users to login with NO PASSWORD. This allows anyone who knows the users name to access the system which can lead to root user compromise.

Security Patches

System Patches are generally kept up to date. System administrators download and install the latest security clusters from SunSolve(9). More care should be taken to make sure all vulnerabilities are patched when a new vulnerability is discovered. This is how most systems are compromised. Something that is widely known as a security hole and has patches available for it are not applied. This is the single most cause of security incidents plaguing the internet today. Great sources of this information are SANS(10), SecurityFocus(11) and Packet Storm(12). The current listing of a patchdiag report is available in Appendix D. Recommended that all security and recommended patches are installed immediately. Other patches that are not current should be updated ASAP after evaluating them.

Sensitive Data

All sensitive user data is stored in the oracle database. Communication between the web server and database server needs to be encrypted. Any files that provide sensitive information should also be encrypted. GnuPG(13) provides the best means for encrypting local files. If anyone does happen to gain access to these files they still need to know your password to access these files. No encryption is currently being used. Suggest immediate update to this.

Date Encryption via Internet Connections.

All connections that require users to login to the web server are currently encrypted via SSL Connections. If any connections via Telnet or FTP are being utilized they should be terminated immediately. Anyone on the internet can see all traffic generated in plain text. OpenSSH only connections should be used if this is necessary. Setting up A VPN connection and using OpenSSH is the suggested method for this should the need arise to connect to machines internal to your network from the internet.

Access Restrictions

Currently accesses to systems are based on need. Only system administrators have root access. Database administrators have permissions necessary for them to perform DBA work. No extraneous accounts are currently noticed on the system. FTP Access needs to be restricted via chroot'd environment and logins controlled via /etc/ftpusers restrictions (Make sure root and all system accounts are NOT allow to ftp in by including them in this file). Example ftpusers file is in Appendix E. Suggest implementation of TCP Wrappers (14) to all services. This will help provide even more security when implementing OpenSSH encrypted connections to FTP accounts.

Backup Policies - Disaster Preparedness

Currently information is backed up via Solstice Networker Backup to a DLT 4000 tape drive. Full backups are twice a week and incremental backups all other days. Retention time is 4 weeks. Offsite storage facilities rotate these tapes out on a regular basis. Only area of improvement noted here is to encrypt the backup information via OpenSSH Tunnel.

Contract support has been issued with Sungard for disaster recovery. All essential software and information is available at a remote offsite location to restore the system to full operating capacity in a brand-new facility within 3 days. Only concern here is should a disaster affect the building itself and key personnel are lost.

Other Issues

Physical Security

All computer systems are located in a secure facility with badge card access. Badge access is required to access the building. Addition privilege badge access is required to access the computer room. No PIN number is required for access into the facility. If someone steals an access badge with sufficient access privileges he now has physical access to all systems. Systems are not secured in the computer room. Sensitive servers are placed in lockable storage racks but none of these are currently locked. All systems are accessible once entry to the computer room is gained. Suggest adding PIN Access to the computer room. This requires that simple possession of this access card will not grant access. It is also suggested to place sensitive servers in the locking racks and give physical key access to personal who are required to access these systems.

Training - All System Administrators (SA) need to be kept up to date on training and security related issues as they develop. SANS provides conferences that provide excellent information on security. Web sites and email lists also provide great sources of information regarding security related issues.

Tools - Make sure to download and use all available tools to help secure your system. Encryption tools, Host and Network Based Intrusion Detection Systems (IDS), System Hardening Tools. Anything that is useful in securing your system can be invaluable to help prevent a security compromise. These tools are widely available as both freeware and commercial products. Some recommended security related products are:

Host Based IDS - Tripwire (15), Samhain (16)
Network Based IDS - Snort (17)
System Scanners - Tiger (18), COPS (19)
Vulnerability Scanners - Nessus (1)
Port Scanner - Nmap (2)
Log Monitoring - Swatch (20), Logcheck (21)
Priviledge Restrictions - TCP Wrappers (14), SUDO (8)
Encryption - GnuPG (13), OpenSSH (4)
System - lsof (22)

Please make sure that you fully understand each product and what it does before you implement its use.

Security Vulnerabilities Prioritized

The following is a list of current vulnerabilities discovered and listed in descending order.

1. All access to systems is done via unencrypted channels.
2. Root/System Account Access.
3. .rhosts/.netrc entries.
4. Patches not up-to-date. (Appendix D)
5. All Nessus discovered security problems. (Appendix A)
6. Unnecessary software installed.
7. Software not latest revisions.
8. Unnecessary ports open.
9. System configuration files allow some common exploits.
10. Physical access to machines.
11. Knowledge of if/when your system has been compromised.

Recommended Fixes for Vulnerabilities

The following is a list of recommended fixes to the above problems

1. All access to systems is done via unencrypted channels.
 - Install SSH and GnuPG to provide encryption for both local files and tcp connections.
2. Root/System Account Access.
 - Remove root/system accounts from FTP via /etc/ftpusers
 - Deny any logins via telnet or other programs. Root restricted to console only (/etc/default/login).
 - See Appendix E for examples.
3. .rhosts/.netrc entries.

Removal of all .rhosts/.netrc entries. Replace these with root owned empty files to prevent future exploiting
4. Patches not up-to-date. (Appendix D)

Patches need upgrading to fix all known security bugs
Download these from the SunSolve site.

5. All Nessus discovered security problems. (Appendix A)
 - All Nessus discovered security problems in Appendix A should be resolved.
 - SNMP
 - Telnet
 - Sendmail
 - etc..
6. Unnecessary software installed.
 - Removal of all unneeded packages and programs.
7. Software not latest revisions.
 - Update existing software to latest revisions
Apache is several revisions behind.
8. Unnecessary ports open.
 - Close unnecessary ports. Again nessus (Appendix A) and nmap (Appendix B) both show large amounts of unnecessary ports/programs in use. Remove these services/ports from /etc/inet/inetd.conf and /etc/inittab
9. System configuration files allow some common exploits.
 - Update system configuration files to restrict common exploits (/etc/system, /etc/rmmount.conf, /etc/init.d/inetinit) (Appendix C)
10. Physical access to machines.
 - Restrict physical access to machines better.
 - PIN Access to computer floor, Locking Racks
11. Knowledge of if/when your system has been compromised.
 - Tripwire, Samhain, Log Server with Swatch/Logcheck
Snort, LSOF, TCP Wrappers

Appendix A
Nessus Security Scan

Nessus Scan Report

SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 5
- Number of security warnings found : 25
- Number of security notes found : 7

TESTED HOSTS

127.0.0.1 (Security holes found)

DETAILS

+ 127.0.0.1 :

- . List of open ports :
 - o echo (7/tcp) (Security warnings found)
 - o discard (9/tcp)
 - o daytime (13/tcp) (Security warnings found)
 - o chargen (19/tcp) (Security warnings found)
 - o ftp (21/tcp) (Security notes found)
 - o telnet (23/tcp) (Security warnings found)
 - o smtp (25/tcp) (Security warnings found)
 - o time (37/tcp)
 - o finger (79/tcp) (Security warnings found)
 - o unknown (80/tcp) (Security notes found)
 - o sunrpc (111/tcp)
 - o exec (512/tcp) (Security warnings found)
 - o login (513/tcp) (Security warnings found)
 - o shell (514/tcp) (Security warnings found)
 - o printer (515/tcp)
 - o uucp (540/tcp)
 - o lockd (4045/tcp)
 - o unknown (6000/tcp)
 - o dtspc (6112/tcp)
 - o fs (7100/tcp)
 - o unknown (7937/tcp)
 - o unknown (7938/tcp)
 - o general/tcp (Security notes found)
 - o general/udp (Security notes found)

- o unknown (161/udp) (Security hole found)
- o unknown (32787/udp) (Security warnings found)
- o unknown (32773/tcp) (Security warnings found)
- o unknown (32782/udp) (Security warnings found)
- o unknown (32786/udp) (Security warnings found)
- o unknown (32783/udp) (Security hole found)
- o unknown (32785/udp) (Security warnings found)
- o unknown (32788/udp) (Security warnings found)
- o unknown (32784/udp) (Security warnings found)
- o lockd (4045/udp) (Security warnings found)
- o unknown (32789/udp) (Security hole found)
- o general/icmp (Security warnings found)
- o echo (7/udp) (Security warnings found)
- o daytime (13/udp) (Security warnings found)
- o chargen (19/udp) (Security warnings found)
- o unknown (25/tcp) (Security hole found)

- . Warning found on port echo (7/tcp)
The 'echo' port is open. This port is not of any use nowadays, and may be a source of problems, since it can be used along with other ports to perform a denial of service. You should really disable this service.

Risk factor : Low.

Solution : comment out 'echo' in /etc/inetd.conf
CVE : CVE-1999-0103

- . Warning found on port daytime (13/tcp)
The daytime service is running.
The date format issued by this service may sometimes help an attacker to guess the operating system type.

In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

- . Warning found on port chargen (19/tcp)
The chargen service is running.
The 'chargen' service should only be enabled when testing the machine.

When contacted, chargen responds with some random (something like all the characters in the alphabet in sequence). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

An easy attack is 'pingpong' which IP spoofs a packet between two machine running chargen. They will commence spewing characters at each other, slowing the machines down and saturating the network.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

- . Information found on port ftp (21/tcp)
Remote FTP server banner :
localhost ftp server (sunos 5.7) ready.

- . Warning found on port telnet (23/tcp)
The Telnet service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

You should disable this service and use OpenSSH instead. (www.openssh.com)

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

Risk factor : Low
CVE : CAN-1999-0619

- . Information found on port telnet (23/tcp)
Remote telnet banner :

- . Warning found on port smtp (25/tcp)
The remote SMTP server
answers to the EXPN and/or VRFY commands.

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.

Your mailer should not allow remote users to use any of these commands, because it gives them too much information.

Solution : if you are using sendmail, add the option

O PrivacyOptions=goaway
in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

- . Warning found on port smtp (25/tcp)
The remote SMTP server is vulnerable to a redirection attack. That is, if a mail is sent to :

user@hostname1@victim

Then the remote SMTP server (victim) will happily send
The mail to :

user@hostname1

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.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
SOME SMTP SERVERS LIKE POSTFIX WILL NOT
COMPLAIN BUT DROP THIS MESSAGE ***

Solution : if you are using sendmail, then at the top of ruleset 98, in /etc/sendmail.cf, insert :
R\$*@\$*\$* \$#error \$@ 5.7.1 \$: '551 Sorry, no redirections.'

Risk factor : Low

- . Warning found on port smtp (25/tcp)
The remote SMTP server allows 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.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a relay any more.
CVE : CAN-1999-0512

- . Information found on port smtp (25/tcp)
Remote SMTP server banner :
localhost ESMTP Sendmail 8.9.3+Sun/8.9.1
Tue, 21 Nov 2000 14:00:40 -0500 (EST)
214-This is Sendmail version 8.9.3+Sun214-Topics:
214- HELO EHLO MAIL RCPT DATA
214- RSET NOOP QUIT HELP VRFY
214- EXPN VERB ETRN DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation contact Sun Microsystems
214-Technical Support.
214-For local information send email to Postmaster at your site.
214 End of HELP info

- . Warning found on port finger (79/tcp)
The remote finger daemon accepts to redirect requests. That is, users can perform requests like :
finger user@host@victim

This allows crackers to use your computer

as a relay to gather information on another network, making the other network think you are making the requests.

Solution: disable your finger daemon (comment out the finger line in /etc/inetd.conf) or install a more secure one.

Risk factor : Low
CVE : CAN-1999-0105

- . Information found on port unknown (80/tcp)
The remote web server type is :
Apache/1.3.6 (Unix)

We recommend that you configure your web server to Return bogus versions, so that it makes the cracker job more difficult

- . Warning found on port exec (512/tcp)
The rexecd service is open.
Because rexecd does not provide any good means of authentication, it can be used by crackers to scan a third party host, giving you troubles or bypassing your firewall.

Solution : comment out the 'exec' line in /etc/inetd.conf.

Risk factor : Medium
CVE : CAN-1999-0618

- . Warning found on port login (513/tcp)
The rlogin service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rlogin server. This includes logins and passwords.

You should disable this service and use openssh instead (www.openssh.com)

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

Risk factor : Low
CVE : CAN-1999-0651

- . Warning found on port shell (514/tcp)
The rsh service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

You should disable this service and use ssh instead.

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

Risk factor : Low
CVE : CAN-1999-0651

- . Information found on port general/tcp
Nmap found that this host is running Solaris 2.6 - 2.7,
Solaris 7

- . Information found on port general/tcp
QueSO has found out that the remote host OS is
* Solaris 2.x

CVE : CAN-1999-0454

- . Information found on port general/udp
For your information, here is the traceroute to
127.0.0.1 :
127.0.0.2
127.0.0.1

- . Vulnerability found on port unknown (161/udp) :
SNMP Agent responded as expected with community name:
public
CVE : CAN-1999-0517

- . Vulnerability found on port unknown (161/udp) :
SNMP Agent responded as expected with community name:
private
CVE : CAN-1999-0517

- . Warning found on port unknown (161/udp)
SNMP Agent port open, it is possible to execute
SNMP GET and SET, (with the proper community names)

- . Warning found on port unknown (32787/udp)
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.

Since this service lacks any kind of authentication, a cracker 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.

It can also be used as a denial of service attack, by continually sending garbage to the users screens, preventing them from working properly.

Solution : Deactivate this service.

Risk factor : Medium
CVE : CVE-1999-0181

- . Warning found on port unknown (32773/tcp)
The tooltalk RPC service is running.
An possible implementation fault in the ToolTalk object database server may allow a cracker to execute arbitrary commands as root.

** This warning may be a false
positive since the presence

of the bug was not tested **

Solution : Disable this service.
See also : CERT Advisory CA-98.11

Risk factor : High
CVE : CVE-1999-0003

- . Warning found on port unknown (32782/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 *

We suggest you to disable this service.

Risk factor : High
CVE : CVE-1999-0018

- . Warning found on port unknown (32786/udp)
The sprayd 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 : CAN-1999-0613

- . Vulnerability found on port unknown (32783/udp) :
The sadmin 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

- . Warning found on port unknown (32785/udp)
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 so on.

It usually not a good idea to let this service open.

Risk factor : Low
CVE : CVE-1999-0626

- . Warning found on port unknown (32788/udp)
The rstatd RPC service is running.
It provides an attacker interesting information such as :

- the CPU usage
- the system uptime
- its network usage
- and more

It usually not a good idea to let this service open

Risk factor : Low
CVE : CAN-1999-0624

- . Warning found on port unknown (32784/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.

Risk factor : Low
CVE : CAN-1999-0625

- . Warning found on port lockd (4045/udp)
The nlockmgr RPC service is running.
If you do not use this service, then disable it as it may become a security threat in the future, if a vulnerability

is discovered.

Risk factor : Low
CVE : CAN-2000-0508

- . Vulnerability found on port unknown (32789/udp) :
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.

* NO SECURITY HOLE REGARDING THIS PROGRAM HAS BEEN TESTED, SO THIS MIGHT BE A FALSE POSITIVE *

We suggest you to disable this service.

Risk factor : High
CVE : CVE-1999-0320

- . Warning found on port general/icmp
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentications protocols.

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

Risk factor : Low
CVE : CAN-1999-0524

- . Warning found on port general/icmp
The remote host answered to an ICMP_MASKREQ query and sent us its netmask.

An attacker can use this information to understand how your network is set up and how the routing is done. This may

help him to bypass your filters.

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

Risk factor : Low
CVE : CAN-1999-0524

- . Warning found on port echo (7/udp)
The 'echo' port is open. This port is not of any use nowadays, and may be a source of problems, since it can be used along with other ports to perform a denial of service. You should really disable this service.

Risk factor : Low.

Solution : comment out 'echo' in /etc/inetd.conf
CVE : CVE-1999-0103

- . Warning found on port daytime (13/udp)
The daytime service is running.
The date format issued by this service may sometimes help an attacker to guess the operating system type.

In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

- . Warning found on port chargen (19/udp)
The chargen service is running.
The 'chargen' service should only be enabled when testing the machine.

When contacted, chargen responds with some random

(something like all the characters in the alphabet in sequence). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

An easy attack is 'pingpong' which IP spoofs a packet between two machines running chargen. They will commence spewing characters at each other, slowing the machines down and saturating the network.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

- . Vulnerability found on port unknown (25/tcp) :
It was possible to crash the remote SMTP server by opening a great amount of sockets on it.

This problem allows crackers to make your SMTP server crash, thus preventing you from sending or receiving e-mails, which will affect your work.

Solution :
If your SMTP server is constrained to a maximum number of processes, i.e. it's not running as root and as a ulimit 'max user processes' of 256, you may consider upping the limit with 'ulimit -u'.

If your server has the ability to protect itself from SYN floods, you should turn on that features, i.e. Linux's CONFIG_SYN_COOKIES

The best solution may be cisco's 'TCP intercept' feature.

Risk factor : Serious
CVE : CAN-1999-0846

This file was generated by the Nessus Security Scanner

Appendix B Nmap Scans

Standard TCP Scan

```
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
Host localhost (127.0.0.1) appears to be up ... good.
Initiating TCP connect() scan against localhost (127.0.0.1)
Adding TCP port 7100 (state open).
Adding TCP port 6000 (state open).
Adding TCP port 514 (state open).
Adding TCP port 515 (state open).
Adding TCP port 9 (state open).
Adding TCP port 19 (state open).
Adding TCP port 7 (state open).
Adding TCP port 513 (state open).
Adding TCP port 23 (state open).
Adding TCP port 32775 (state open).
Adding TCP port 111 (state open).
Adding TCP port 32772 (state open).
Adding TCP port 25 (state open).
Adding TCP port 32771 (state open).
Adding TCP port 512 (state open).
Adding TCP port 540 (state open).
Adding TCP port 32773 (state open).
Adding TCP port 13 (state open).
Adding TCP port 80 (state open).
Adding TCP port 21 (state open).
Adding TCP port 6112 (state open).
Adding TCP port 37 (state open).
Adding TCP port 79 (state open).
Adding TCP port 32774 (state open).
The TCP connect scan took 1 second to scan 1523 ports.
Interesting ports on localhost (127.0.0.1):
(The 1499 ports scanned but not shown below are in state:
closed)
```

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
19/tcp	open	chargen
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
79/tcp	open	finger
80/tcp	open	http

```
111/tcp      open        sunrpc
512/tcp      open        exec
513/tcp      open        login
514/tcp      open        shell
515/tcp      open        printer
540/tcp      open        uucp
6000/tcp     open        X11
6112/tcp     open        dtspc
7100/tcp     open        font-service
32771/tcp    open        sometimes-rpc5
32772/tcp    open        sometimes-rpc7
32773/tcp    open        sometimes-rpc9
32774/tcp    open        sometimes-rpc11
32775/tcp    open        sometimes-rpc13
```

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

Stealth Scan with OS Fingerprinting

Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)

Host localhost (127.0.0.1) appears to be up ... good.

Initiating SYN half-open stealth scan against localhost (127.0.0.1)

```
Adding TCP port 32775 (state open).
Adding TCP port 32791 (state open).
Adding TCP port 32772 (state open).
Adding TCP port 6000 (state open).
Adding TCP port 7937 (state open).
Adding TCP port 32773 (state open).
Adding TCP port 22370 (state open).
Adding TCP port 32771 (state open).
Adding TCP port 32789 (state open).
Adding TCP port 32774 (state open).
Adding TCP port 79 (state open).
Adding TCP port 21 (state open).
Adding TCP port 540 (state open).
Adding TCP port 513 (state open).
Adding TCP port 32790 (state open).
Adding TCP port 25 (state open).
Adding TCP port 19 (state open).
Adding TCP port 515 (state open).
Adding TCP port 80 (state open).
Adding TCP port 13 (state open).
Adding TCP port 7 (state open).
Adding TCP port 111 (state open).
```

Adding TCP port 37 (state open).
 Adding TCP port 512 (state open).
 Adding TCP port 9 (state open).
 Adding TCP port 7938 (state open).
 Adding TCP port 6112 (state open).
 Adding TCP port 514 (state open).
 Adding TCP port 7100 (state open).
 Adding TCP port 23 (state open).
 The SYN scan took 50 seconds to scan 65535 ports.
 For OSScan assuming that port 7 is open and port 1 is
 closed and neither are firewalled
 Interesting ports on localhost (127.0.0.1):
 (The 65505 ports scanned but not shown below are in state:
 closed)

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
19/tcp	open	chargen
21/tcp	open	ftp
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
79/tcp	open	finger
80/tcp	open	http
111/tcp	open	sunrpc
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
515/tcp	open	printer
540/tcp	open	uucp
6000/tcp	open	X11
6112/tcp	open	dtspc
7100/tcp	open	font-service
7937/tcp	open	unknown
7938/tcp	open	unknown
22370/tcp	open	unknown
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32773/tcp	open	sometimes-rpc9
32774/tcp	open	sometimes-rpc11
32775/tcp	open	sometimes-rpc13
32789/tcp	open	unknown
32790/tcp	open	unknown
32791/tcp	open	unknown

TCP Sequence Prediction: Class=random positive increments
Difficulty=11463(Worthy challenge)

Sequence numbers: 8276F278 827752BA 82783DE6 827A3529
827B8988 827C80FF

Remote OS guesses: Solaris 2.6 - 2.7, Solaris 7

Nmap run completed -- 1 IP address (1 host up) scanned in
54 seconds

UDP Scan with OS Fingerprinting

Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/)

Warning: No TCP ports found open on this machine, OS
detection will be MUCH less reliable

Interesting ports on localhost (127.0.0.1):

(The 1427 ports scanned but not shown below are in state:
closed)

Port	State	Service
7/udp	open	echo
9/udp	open	discard
13/udp	open	daytime
19/udp	open	chargen
37/udp	open	time
42/udp	open	nameserver
67/udp	open	bootps
111/udp	open	sunrpc
123/udp	open	ntp
161/udp	open	snmp
177/udp	open	xmcp
512/udp	open	biff
514/udp	open	syslog
517/udp	open	talk
4045/udp	open	lockd
32771/udp	open	sometimes-rpc6
32776/udp	open	sometimes-rpc16
32778/udp	open	sometimes-rpc20
32779/udp	open	sometimes-rpc22
32786/udp	open	sometimes-rpc26
32787/udp	open	sometimes-rpc28

Too many fingerprints match this host for me to give an
accurate OS guess

Nmap run completed -- 1 IP address (1 host up) scanned in
2084 seconds

Appendix C

Sample Configuration Files

Add these lines to /etc/system

* Added 11/16/2000 Sans Recommended Settings

```
set priority_paging=1
```

* Disable bufferoverflow attacks on the stack

* Attempt to prevent and log stack-smashing attacks

```
set noexec_user_stack = 1
```

```
set noexec_user_stack_log = 1
```

* Enable more pty connections

```
set pt_cnt = 256
```

* Set ulimit hard 2048, soft 1024

```
set rlim_fd_max = 2048
```

```
set rlim_fd_cur = 1024
```

* Max process per one user

```
set maxuprc = 150
```

* Require NFS Clients to use privileged ports

* Solaris 2.6+

```
set nfssrv:nfs_portmon = 1
```

* Solaris 2.5

```
* set nfs:nfs_portmon = 1
```

/etc/init.d/inetinit

Add these lines

```
# Security Settings SANS Recommended
```

```
nnd -set /dev/tcp tcp_conn_req_max_q0 1024
```

```
nnd -set /dev/ip ip_ignore_redirect 1
```

```
nnd -set /dev/ip ip_send_redirects 0
```

```
nnd -set /dev/ip ip_ire_flush_interval 60000
```

```
nnd -set /dev/arp arp_cleanup_interval 60000
```

```
nnd -set /dev/ip ip_forward_src_routed 0
```

```
nnd -set /dev/ip ip_forward_directed_broadcasts 0
```

```
nnd -set /dev/ip ip_forwarding 0
```

```
nnd -set /dev/ip ip_strict_dst_multihoming 1
```

```
# End Security Settings
```

/etc/rmmount.conf

Add these lines

```
# Disable setuid root for users mounting removable media  
via vold  
mount hsfs -o nosuid  
mount ufs -o nosuid
```

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

Appendix D
Patchdiag Report

=====
System Name: localhost SunOS Vers: 5.7 Arch: sparc
Cross Reference File Date: Nov/21/00

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
106144	09	21	SunOS 5.7: Elite3D AFB Graphics Patch
106145	08	17	SunOS 5.7: Creator 7 FFB Graphics Patch
106146	09	16	SunOS 5.7: M64 Graphics Patch
106147	04	06	SunOS 5.7: VIS/XIL Graphics Patch
106148	05	12	SunOS 5.7: XFB Graphics Patch
106300	07	09	SunOS 5.7: Shared library patch for 64bit C++
106327	06	08	SunOS 5.7: Shared library patch for C++
106541	12	CURRENT	SunOS 5.7: Kernel update patch
106725	02	CURRENT	OpenWindows 3.6.1: mailtool vacation security patch
106793	05	CURRENT	SunOS 5.7: ufsdump and ufsrestore patch
106812	04	CURRENT	OBSOLETEED by 107432
106857	10	CURRENT	SunOS 5.7: IS08859-15 bug fixes and EOL Openwindows support.
106879	01	CURRENT	SunOS 5.7: sys-suspend patch

106887	02	CURRENT	SunOS 5.7: SunVideo 1.4 Patch
106917	01	CURRENT	SunOS 5.7: when view mails change charset, dtmail dump core.
106924	02	06	SunOS 5.7: isp driver patch
106925	02	04	SunOS 5.7: glm driver patch
106934	03	CURRENT	CDE 1.3: libDtSvc Patch
106936	01	CURRENT	SunOS 5.7: /etc/cron.d/logchecker patch
106938	04	CURRENT	SunOS 5.7: libresolv patch
106940	01	CURRENT	SunOS 5.7: /usr/sbin/makedbm patch
106942	07	CURRENT	SunOS 5.7: libnsl, rpc.nisd and nis_cachemgr patch
106944	03	CURRENT	SunOS 5.7: /kernel/fs/fifofs and /kernel/fs/sparcv9/fifofs patch
106946	01	02	SunOS 5.7: /usr/sbin/sar patch
106948	01	CURRENT	SunOS 5.7: /kernel/drv/qe and /kernel/drv/sparcv9/qe patch
106949	01	CURRENT	SunOS 5.7: BCP (binary compatibility) patch
106950	11	13	SunOS 5.7: Linker patch
106952	01	CURRENT	SunOS 5.7: /usr/bin/uux patch
106959	01	CURRENT	SunOS 5.7: Last portion of audio file gets chopped or repeats
106960	01	CURRENT	SunOS 5.7: Manual Pages for patchadd.lm and patchrm.lm
106963	01	CURRENT	SunOS 5.7: /kernel/drv/esp and /kernel/drv/sparcv9/esp patch
106978	10	CURRENT	SunOS 5.7: sysid patch
106980	07	13	SunOS 5.7: libthread patch
106982	01	CURRENT	SunOS 5.7: /kernel/drv/fas and /kernel/drv/sparcv9/fas patch
106985	01	CURRENT	SunOS 5.7: /usr/sbin/uadmin and /sbin/uadmin patch
106987	02	CURRENT	SunOS 5.7: /usr/sbin/tar patch
106999	01	CURRENT	SunOS 5.7: /usr/lib/adb/sparcv9/adbsub.o patch
107001	01	CURRENT	OBSOLETE by 107887
107003	03	CURRENT	SunOS 5.7: Updated Lucida Hebrew Fonts for Solaris 7
107011	01	CURRENT	CDE 1.3: sdtwebclient patch
107014	01	02	XIL 1.4: Deskset Loadable Pipeline Libraries Patch
107018	02	CURRENT	SunOS 5.7: /usr/sbin/in.named patch
107022	04	06	CDE 1.3: Calendar Manager patch
107031	01	CURRENT	OBSOLETE by 106541

107038	01	CURRENT	SunOS 5.7:
apropos/catman/man/whatis patch			
107044	01	CURRENT	SunOS 5.7: Russian and Polish
print failure on some printers			
107049	01	CURRENT	SunOS 5.7: dtlogin language menu
displays wrong info			
107058	01	CURRENT	SunOS 5.7: Patch for assembler
107059	01	CURRENT	SunOS 5.7: /usr/bin/sort and
/usr/xpg4/bin/sort patch			
107063	01	CURRENT	SunOS 5.7: Thai engine crashes in
64bit mode			
107072	01	CURRENT	CDE 1.3: Spell Checker patch
107074	01	CURRENT	SunOS 5.7: SUNWultratest doesn't
support sun4us platform			
107076	01	CURRENT	SunOS 5.7: /usr/kernel/drv/vol
and /usr/kernel/drv/sparcv9/vol pat			
107078	18	CURRENT	OBSOLETE by 108376
107081	08	24	Motif 1.2.7 and 2.1.1: Runtime
library patch for Solaris 7			
107094	04	10	CDE 1.3: dtterm libDtTerm.so.2
Patch			
107115	05	CURRENT	SunOS 5.7: LP patch
107117	03	05	OBSOLETE by 106541
107121	01	02	OBSOLETE by 107458
107127	02	CURRENT	SunOS 5.7:
/usr/lib/autofs/automountd patch			
107147	05	08	SunOS 5.7: pci driver patch
107148	04	08	SunOS 5.7: /kernel/fs/cachefs
patch			
107171	06	CURRENT	SunOS 5.7: Fixes for patchadd and
patchrm			
107178	01	CURRENT	CDE 1.3: libDtHelp.so.1 patch
107180	12	24	CDE 1.3: dtlogin patch
107185	01	CURRENT	SunOS 5.7: Miscellaneous Russian
KOI8-R problems			
107187	01	02	SunOS 5.7: Miscellaneous Eastern
European locale problems			
107200	08	12	CDE 1.3: dtmail patch
107219	02	CURRENT	OBSOLETE by 107885
107226	07	12	CDE 1.3: dtwm patch
107233	01	CURRENT	OpenWindows 3.6.1: xterm patch
107248	01	02	CDE 1.3: sdtaudio patch
107250	02	CURRENT	OpenWindows 3.6.1: libsv8.so.1
Patch			
107259	01	CURRENT	SunOS 5.7: /usr/sbin/vold patch
107285	02	CURRENT	SunOS 5.7: passwd & pam library
patch			

107292	02	07	SunOS 5.7: ifp driver patch
107293	01	CURRENT	SunOS 5.7: libgss.so.1 and gsscred patch
107306	01	03	CDE 1.3: dtfile patch
107316	01	CURRENT	SunOS 5.7: localeconv() returns wrong results for French
107318	04	CURRENT	OBSOLETE by 108068
107330	01	CURRENT	SunOS 5.7: /usr/sbin/ntpdate patch
107332	02	CURRENT	SunOS 5.7: libadm patch
107337	01	CURRENT	OpenWindows 3.6.1: KCMS configure tool has a security vulnerabilit
107351	01	03	XGL 3.3.1: XGL Patch (stripped version)
107359	02	CURRENT	SunOS 5.7: Patch for SPARCompiler Binary Compatibility Libraries
107401	01	CURRENT	SunOS 5.7: /usr/bin/iostat patch
107403	01	CURRENT	SunOS 5.7: rlmod & telmod patch
107430	01	CURRENT	SunOS 5.7: Installer utility used by NCR breaks under Solaris 7
107432	03	CURRENT	SunOS 5.7: CTL printing patch
107437	03	CURRENT	SunOS 5.7: support IBM Cp837 and Cp874 iconv modules(th_TH)
107438	02	CURRENT	SunOS 5.7: iso8859-15 locale copy and paste fix
107441	01	02	SunOS 5.7: /usr/bin/mailx patch
107443	09	12	SunOS 5.7: packaging utilities patch
107445	01	03	OBSOLETE by 107709
107448	01	CURRENT	SunOS 5.7: /usr/lib/fs/cachefs/cachefsd patch
107450	01	CURRENT	SunOS 5.7: /platform/SUNW,Ultra- Enterprise-10000/lib/cvcd patch
107451	04	05	SunOS 5.7: /usr/sbin/cron patch
107453	01	CURRENT	SunOS 5.7: Ultra-80 platform patch
107454	05	CURRENT	SunOS 5.7: /usr/bin/ftp patch
107456	01	CURRENT	SunOS 5.7: /etc/nsswitch.dns patch
107458	04	10	SunOS 5.7: dad, sd, ssd, uata drivers patch
107459	01	CURRENT	SunOS 5.7: qec driver patch
107460	03	08	SunOS 5.7: st driver patch
107462	01	CURRENT	SunOS 5.7: /kernel/sched/TS patch
107465	02	CURRENT	SunOS 5.7: /kernel/fs/hsfs and /kernel/fs/sparcv9/hsfs patch

107469	03	08	SunOS 5.7: sf & social drivers patch
107472	02	CURRENT	SunOS 5.7: ses driver patch
107473	02	06	SunOS 5.7: luxadm patch
107474	01	CURRENT	SunOS 5.7: ifp adb macro patch
107475	01	CURRENT	SunOS 5.7: /usr/sbin/in.telnetd patch
107477	02	CURRENT	SunOS 5.7: /usr/lib/nfs/mountd patch
107499	02	CURRENT	SunOS 5.7: koi8-R -ow hanged before dtlogin screen
107544	03	CURRENT	SunOS 5.7: /usr/lib/fs/ufs/fsck patch
107546	02	CURRENT	OpenWindows 3.6.1: Ultra 80 Support Patch
107551	01	CURRENT	SunOS 5.7: /usr/bin/date and /usr/xpg4/bin/date patch
107553	01	CURRENT	SunOS 5.7: /usr/kernel/drv/ipdcm & /usr/kernel/drv/sparcv9/ipdcm p
107555	01	CURRENT	SunOS 5.7: /usr/lib/libldap.so.3 & /usr/lib/sparcv9/libldap.so.3 p
107557	02	CURRENT	SunOS 5.7: /usr/sbin/sag patch
107584	01	CURRENT	SunOS 5.7: /usr/lib/vold/dev_cdrom.so.1 patch
107587	01	CURRENT	SunOS 5.7: /usr/lib/acct/lastlogin patch
107589	03	05	SunOS 5.7: se, zs, kbd and kbio.h patch
107624	01	CURRENT	SunOS 5.7: /usr/lib/fs/ufs/df patch
107636	05	CURRENT	SunOS 5.7: X Input & Output Method patch
107648	09	CURRENT	OBSOLETE by 108376
107650	08	CURRENT	OpenWindows 3.6.1 X11R6.4 Xprint Extension Patch
107652	05	06	OpenWindows 3.6.1: X11R6.4 XKB Extension Patch
107654	05	07	OpenWindows 3.6.1 X11R6.4 LBX & XRX Extensions Patch
107656	05	06	OpenWindows 3.6.1: libXt Patch
107658	04	05	OpenWindows 3.6.1: X11R6.4 API man pages Patch
107680	01	CURRENT	SunOS 5.7: /kernel/sys/msgsys and /kernel/sys/sparcv9/msgsys patch
107684	01	CURRENT	SunOS 5.7: Sendmail patch
107688	01	CURRENT	OBSOLETE by 107887
107702	01	05	CDE 1.3: dtsession patch

107709	06	07	SunOS 5.7:
libssasmp/libssagent/snmpdx/mibiisa patch			
107711	01	CURRENT	OBSOLETE by 107306
107716	04	10	SunOS 5.7: PGX32 Graphics Patch
107738	01	CURRENT	SunOS 5.7: Estonian locale uses
incorrect codeset (QU)			
107744	01	02	SunOS 5.7: /usr/bin/du and
/usr/xpg4/bin/du patch			
107746	03	CURRENT	SunOS 5.7: Croatian locale hr_HR
corrections			
107792	02	CURRENT	SunOS 5.7: /usr/bin/pax patch
107794	01	CURRENT	SunOS 5.7: ASET patch
107796	01	03	SunOS 5.7: /kernel/fs/lofs patch
107799	01	02	SunOS 5.7:
compress/uncompress/zcat patch			
107807	01	CURRENT	OpenWindows 3.6.1: xrdb patch
107813	01	CURRENT	SunOS 5.7: Japanese UTF-8 iconv
patch			
107834	02	03	SunOS 5.7: dkio.h & commands.h
patch			
107836	01	CURRENT	SunOS 5.7: /usr/sbin/format patch
107838	01	CURRENT	SunOS 5.7: libtnfctl patch
107841	01	02	SunOS 5.7: rpcsec patch
107843	02	CURRENT	SunOS 5.7: /sbin/init and
/usr/sbin/init patch			
107853	01	CURRENT	OpenWindows 3.6.1: xdm patch
107865	01	CURRENT	SunOS 5.7: /kernel/sys/shmsys
patch			
107881	10	CURRENT	OBSOLETE by 108374
107883	04	06	CDE 1.3: sdtimage Patch
107885	06	CURRENT	CDE 1.3: dtprintinfo Patch
107887	09	10	CDE 1.3: Actions Patch
107893	08	09	OpenWindows 3.6.1: Tooltalk patch
107899	01	CURRENT	OBSOLETE by 106541
107917	02		
107919	01	CURRENT	SunOS 5.7: /usr/include/sys/mhd.h
patch			
107962	01	CURRENT	SunOS 5.7: iconv from UTF-8 to
euc requires a buffer with 1 extra			
107972	01	CURRENT	SunOS 5.7: /usr/sbin/static/rcp
patch			
108029	02	CURRENT	SunOS 5.7: S899 u3 prodreg fixes
for Java 1.1 and Java 1.2 VM			
108068	03	CURRENT	SunOS 5.7: Manual Page updates
for Solaris 7			
108089	02	CURRENT	SunOS 5.7: /usr/bin/tail patch
108147	01	CURRENT	SunOS 5.7: SX Graphics Patch

```

108148    01    CURRENT SunOS 5.7: prtconf patch
108151    01         02    CDE 1.3: sdtname patch
108158    01    CURRENT SunOS 5.7: /usr/lib/fs/nfs/share
patch
108162    01         02    SunOS 5.7: jsh, rsh, sh patch
108168    01    CURRENT OpenWindows 3.6.1: X Window
include files patch
108170    01    CURRENT SunOS 5.7: showrev patch
108175    01    CURRENT SunOS 5.7: DSR Upgrade patch for
localization packages
108197    01    CURRENT CDE 1.3: dtpad patch
108203    01         04    SunOS 5.7: adb macro & headers
for fibre channel transport layer
108219    01    CURRENT CDE 1.3: dtaction Patch
108221    01    CURRENT CDE 1.3: dtspcd Patch
108224    01    CURRENT SunOS 5.7: envctrl driver patch
108244    01    CURRENT SunOS 5.7: libaio patch
108263    01         06    SunOS 5.7: hme driver patch
108285    01    CURRENT SunOS 5.7: /etc/init.d/MOUNTFSYS
patch
108301    02    CURRENT SunOS 5.7: /usr/sbin/in.tftpd
patch
108327    01    CURRENT SunOS 5.7: /usr/bin/cu patch
108331    01    CURRENT SunOS 5.7: /usr/bin/uustat patch
108343    01         04    CDE 1.3: sdtperfmeter patch
108374    03         04    CDE 1.3: libDtWidget Patch
108376    12         16    OpenWindows 3.6.1: Xsun Patch
108482    02    CURRENT SunOS 5.7: /usr/sbin/snoop patch
108484    01    CURRENT SunOS 5.7: aset patch
108662    01    CURRENT SunOS 5.7: Patch for sadmind
108721    01    CURRENT SunOS 5.7: admintool patch
108798    01    CURRENT SunOS 5.7: /usr/bin/tip patch
108838    02    CURRENT SunOS 5.7:
allocate/mkdevmaps/mkdevalloc patch
109104    04    CURRENT SunOS 5.7: /kernel/fs/sockfs
patch
109253    01    CURRENT SunOS 5.7: /usr/bin/mail patch
109404    01    CURRENT SunOS 5.7: /usr/vmsys/bin/chkperm
patch
109744    01    CURRENT SunOS 5.7: /usr/lib/nfs/nfsd
patch
=====

```

UNINSTALLED RECOMMENDED PATCHES

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

```
-----
-----
109949 N/A 01 97 SunOS 5.7: jserver
buffer overflow
=====
```

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
-----	---	---	---	-----	-----	-----
-----	---	---	---	-----	-----	-----
109949	N/A	01	97			SunOS 5.7: jserver buffer overflow

```
=====
```

UNINSTALLED Y2K PATCHES

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

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
-----	---	---	---	-----	-----	-----
-----	---	---	---	-----	-----	-----
108815	N/A	02	134			OpenWindows 3.6.1: Calendar Manager patch

```
=====
```

© SANS Institute 2000 - 2002, Author retains full rights

Appendix E

Sample /etc/ftpusers, /etc/default/login files

/etc/ftpusers

```
root
daemon
bin
sys
nobody
noaccess
nobody4
uucp
adm
lp
smtp
list
```

/etc/default/login

Make sure the following lines exist

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

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

References

- (1) Nessus Security Scanner - <http://www.nessus.org>
- (2) Nmap Scanner, <http://www.insecure.org/nmap>
- (3) Bryan Costales with Eric Allman, "Sendmail 2nd Edition", O'Reilly and Associates, Inc., 1997
- (4) Openssh - <http://www.openssh.com>
- (5) Apache Web Server - The Apache Software Foundation
<http://www.apache.org>
- (6) Solstice Networker Backup - <http://sunsolve.sun.com>
- (7) Perl - <http://www.perl.com>
- (8) SUDO - <http://www.courtesan.com/sudo/>
- (9) Sunsolve Homepage - <http://sunsolve.sun.com>
- (10) SANS - <http://www.sans.org>
- (11) Security Focus - <http://www.securityfocus.com>
- (12) Packet Storm - <http://packetstorm.securify.com/>
- (13) GNUPG - The Gnu Privacy Guard - <http://www.gnupg.org>
- (14) TCP Wrappers - <ftp://ftp.porcupine.org/pub/security/>
- (15) Tripwire - Tripwire Inc. - <http://www.tripwire.com>
- (16) Samhain - <http://www.la-samhna.de/samhain/index.html>
- (17) Snort - <http://www.snort.org>
- (18) Tiger - <http://net.tamu.edu/ftp/security/TAMU/>
- (19) COPS - Computer Oracle and Password System
<http://www.fish.com/cops/>
- (20) Swatch - <http://www.stanford.edu/~atkins/swatch/>
- (21) Logcheck - <http://www.psionic.com/abacus/logcheck/>
- (22) lsof - <ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/>

Other reference materials:

Alex Noordergraaf and Keith Watson, "Solaris Operating Environment Network Settings for Security", Sun Blueprints Online - Dec 1999

Martin Roesch, "Snort and Unix Exploits", SANS NS 2000 Conference, Oct 2000

Sendmail Homepage - <http://www.sendmail.org>

Aeleen Frisch, "Essential System Administration 2nd Edition", O'Reilly & Associates, Inc., Dec 1995

Paul Albitz and Cricket Liu, "DNS and Bind 2nd Edition", O'Reilly & Associates, Inc., Jan 1997

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced