Global Information Assurance Certification Paper

Auditor's Report
GIAC University
Solaris MTA Security Audit

Susan Hanna
December 4, 2003
GCUX Practical Assignment
Version 1.9 (April 2002)

Abstract

In response to a request for a security audit of the University of GIAC's MTA server, an
evaluation of the resent state of the Solaris 8 server was made using the security analysis tools CIS scan and nessus as well as through administrator interviews and examiniation of the running system.

Based on the results of the evaluation, a number of improvements are recommended as well as acknowlegment made of the efforts to date to secure the system. The most noteworthy changes recommended include implementation of encryted instead of clear-text access and file transfer, removal or disabling of ununsed and services, minimization of the operating system, and the implementation of a better monitoring logging through additional tools, possibly including a host-based firewall.

The University clearly regards security as important, but due to budgetary constraints, has found it difficult to channel the necessary dollars and staff time to developing optimally secure systems for their environement The University will benefit from the methodology applied to analysis of this system and be able to apply the basic principles set forth here to other servers in their domain.

Trademarks

Sun, Sun Microsystems, UNIX, Solaris and the Sun logo are trademarks or registered trademarks of Sun Microsystems, Inc.

SSH is a registered tradmark of SSH Communications Security in the United States and certain other jurisdictions.

All other company, brand and product names may be registered trademarks or trademarks or servicemarks of their respective companies and are hereby recognized as such.

Table of Contents

1. EXECUTIVE SUMMARY

Purpose and Goals:

GIAC University has undertaken an information systems security evaluation intended to determine the security weaknesses and strengths of the existing systems and current administration practices. This evaluation will be used as a guide for developing a high level security policy for all of the University's UNIX systems.

Audit Scope:

This particular engagement focuses on analysis of the GIAC University MTA, which has recently been replaced in service with a new system. The University plans to rebuild the MTA system based on the recommendations of this evaluation, and will eventually rebuild the current production system to the same specifications allowing for fail-over redundancy and load balancing. The lessons learned from this analysis will also play a key role in the formation of UNIX security policies applicable to all other Solaris servers at the University.

Summary Analysis:

Strengths of the existing installation include a scripted framework for local customized OS builds including the application of locally determined security settings and frequent and up-to-date patch application.

Weaknesses of this system include the use of clear-text protocols for access and data transfer by system administrators, the use of excess privilege for certain tasks by junior staff, and installation of unneeded packages and running of unneeded services by default.

Significant improvements can be made in the security of this system including use of OS minimization, replacement of clear-text services with encrypted services, access control, removal of unnecessary network services, and installation of a host-based firewall.

Recommendations:

GIAC University can leverage it's existing customized approach to OS installation and hardening and significantly improve the security of it's servers by installing a reasonably minimized base set of packages applicable to all server installs at the University. Remaining unneeded services can be started, stopped or removed based on each server's requirements. Replacement of clear-text services and rpc access with encrypted services including ssh and sftp will support the security and confidentiality of server administration and data transfer. A host-based firewall will make additional monitoring and access control available to secure the system and provide reporting capabilities. This approach can augment the existing superior patch management with enhanced monitoring and form the basis for a reasonably secure server installation and management strategy achievable with the current level of staff and resources.

2. DESCRIPTION OF SYSTEM AND AUDIT METHODOLOGY

2.1 SYSTEM OVERVIEW

The audit system is a Sun Microsystems entry-level server with an external array running a recent version of the Solaris Operating System and functioning as the University's MTA mail gateway server, currently directly exposed to the Internet.

.

2.2 AUDIT METHODOLOGY

The audit process has several steps in the data gathering phase followed by an analysis phase.

The first step is to interview the administrators of the system to learn about the current administrative practices including installation and management strategies. Determining the level of access to the actual machine shapes the scope and nature of the audit. In this case, since the system has been recently removed from production pending a rebuild, the University has agreed to provide full root access to the system with the assistance of the system administrators.

Next, a review of the hardware, OS installation, installed applications and processes and network environment is made at a preliminary level. Given this information, the audit is refined to target identified and suspected weaknesses in the system as well as to document strengths in the system. Tools are chosen to assist in the analysis of the system's security. For this audit, nessus, including nmap, and CIS scan tools are being utilized. Finally a determination of patchlevel and unpatched vulnerabilities will be checked with Sun's patchdiag tool and reference to Sun Alerts.

After data gathering is complete, the data is analyzed to determine the most significant vulnerabilities and to make recommendations to improve the security of the system.

2.3 INTERVIEW WITH SYSTEM ADMINISTRATORS

The System Administrators were helpful and cooperative and appeared to view the audit process as an opportunity to improve the host-based security of the Solaris systems under their administration.

The administrators have developed a customized build process consisting of a stand-alone installation from the appropriate Solaris CDs, usually the latest (if supported by applications vendors) release, followed by running several build scripts. The build scripts are logically divided into patching the system to current patch levels while disconnected from the network, the application of a series of security fixes and finally installation of utility applications such as shells and system utilities.

The administrators typically install the “Full” distribution option for the Solaris install because they have been unable to justify the time and attention needed to minimize the OS. The

administrators state that this does insure that various libraries and utilities are available, although the extra packages, especially if not used but present on the system, may pose an additional security risk.

The administrators provided the following details on the security fixes applied in the standard Solaris 8 install via one of their custom build scripts:

--Edit /etc/system
--to attempt to prevent and log stack-smashing attacks:
set noexec_user_stack=1
set noexec_user_stack_log=1

--Chmod various setuid files to remove the setuid bit and to set appropriate permissions on key files such as /var/crash

--Edit /etc/default/su and uncomment the following to log su.
CONSOLE=/dev/console

--Edit /etc/default/inetinit to avoid session hijack attacks.
TCP_STRONG_ISS=2

--Edit conf files to log ftp connections/sessions:
change "daemon.notice" to "daemon.debug" for /var/adm/messages
edit /etc/inetd.conf change in.ftpd to in.ftpd -dl

--Disable some services in inetd.conf:
name, finger,sadmind,rquotad, rusersd,rwalld, cachefsd, in.lpd, kcms, talk,
ttdbserverd, fs,dtspcd

--Create /etc/default/ftpd
add UMASK:077 to prevent the creation of world-readable files

--Edit /etc/init.d/inetinit to prevent smurf attacks:
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_respond_to_echo_broadcast 0

--Edit etc/ftpd/ftpusers to prevent ftp to system users
(root is already listed, also add:)
www
smtp
solstice
ftp

--Create loginlog to monitor repeated failed login attempts:

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

--Kill running services:

```
name, sun-dr
```

--Shut down dmi and snmpXdmi

```
mv /etc/rc3.d/S77dmi /etc/rc3.d/K77dmi
mv /etc/rc3.d/S76snmpdx /etc/rc3.d/K76snmpdx
/etc/init.d/init.dmi stop
/etc/init.d/init.snmpdx stop
chmod 000 /usr/lib/dmi/snmpXdmid /usr/lib/dmi/dmispd
```

--Create /etc/inet/ntp.conf to sync time:

```
server time1.giac.edu
server time2.giac.edu
server time3.giac.edu
server time4.giac.edu
driftfile /etc/inet/ntp.drift
restrict default noquery
restrict 127.0.0.1
logconfig =syncstatus +sysevents
```

In addition , the system administrators edit /etc/vfstab to add logging and appropriate options to filesystem , including nosuid where reasonable:

```
/dev/dsk/c2t5d1s0 /dev/rdsk/c2t5d1s0 /pacct    ufs    1      yes    noatime,
logging,nosuid
```

As part of ongoing system administration, the administrators report daily monitoring of new patches from Sun and frequent patching to keep the system up to the current patch levels. Particular importance is attached to any security patch; although such patches are usually deferred until weekly regularly scheduled systems time unless the severity requires emergency attention. Management generally okays brief downtimes during the early morning for true security emergency patching or upgrades.

Applications are monitored for security vulnerabilities and patched or upgraded as necessary, the urgency of such action depending on the severity of the perceived threat. Sun Alerts, Bugtraq, Security Focus, SANS and CERT are monitored for announcements of vulnerabilities in

both appications and the OS.

The administrators use a combination of ssh, telnet and ftp to connect to the server and for file transfer. At least one automated process relies on ftp, while some administration is done using rsh and rhosts. Another automated task relies on wget to automatically update virus identify files. Further, a junior staff member takes care of most postmaster tasks and has root access to two servers, including the audit system, in this capacity.

2.4 HARDWARE

The system is a Sun Microsystems server. The prtdiag -v command provides the details:

System Configuration: Sun Microsystems sun4u Sun Fire 280R (2 X UltraSPARC-III)
System clock frequency: 150 MHz
Memory size: 4096 Megabytes
. . .
System PROM revisions:

OBP 4.10.11 2003/09/25 11:53

The firmware is at the latest level per the current reversion of patch 111292-15 as noted from the Sun patch README:

Patch-ID# 111292-15
Keywords: update sun blade 1000 sun fire 280r netra[tm] t20 sun blade 2000
Synopsis: Sun Blade 1000, Sun Fire 280R, Netra[tm] T20, Sun Blade 2000
Date: Nov/03/2003

Unbundled Release: OBP_4.10.11,POST_4.10.9,OBDIAG_4.10.11

This server has two internal disks and an external D1000 array. The format command gives additional information, showing the internal disks are 36G each and that the D1000 is configured as two logical volumes.

AVAILABLE DISK SELECTIONS:
0. c1t0d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
/pci@8,600000/SUNW,qlc@4/fp@0,0/ssd@w21000004cf09647e,0
1. c1t1d0 <SUN36G cyl 24620 alt 2 hd 27 sec 107>
/pci@8,600000/SUNW,qlc@4/fp@0,0/ssd@w21000004cf0965a1,0
2. c2t5d0 <Symbios-StorEDGEA1000-0003 cyl 8615 alt 2 hd 64 sec 64>
/pseudo/rdnexus@2/rdriver@5,0
3. c2t5d1 <Symbios-StorEDGEA1000-0003 cyl 60318 alt 2 hd 64 sec 64>
/pseudo/rdnexus@2/rdriver@5,1

The available internal storage has been partitioned and mounted with a single partition for root, including /var, /export/home, /opt/, /usr and /bin and a second partition for swap space on one of the internal disks, then mirrored to the seocond internal disk. The storage array has a seperate file system created for the MTA software, including it's queue and log directories. Accounting log storage is hosted on the second logical volume in the storage array. The df -h command gives information on partitions and usage:

```
Filesystem             Size  Used Avail Use% Mounted on
/dev/md/dsk/d0         7.7G  2.8G  4.9G  36% /
swap                   7.0G   24k  7.0G   1% /var/run
swap                   7.0G  1.4M  7.0G   1% /tmp
/dev/dsk/c2t5d1s0      118G   29G   88G  25% /pacct
/dev/dsk/c2t5d0s0       16G  4.3G   12G  26% /opt/pmdf
admin:/usr/local/src    8.4G  3.0G  5.2G  37% /usr/local/src
admin:/usr/local/patches  8.4G  7.5G  950M  89% /usr/local/patches
```

In addition to the local mounts, two NFS-mounted file systems are in use, a patch archive and a software source archive. Both are mounted from another Solaris server.

2.5 OPERATING SYSTEM

The system is running Solaris 8 7/01 as indicated by the commands showrev and a review of /etc/release:

```
mtaserver>showrev
Hostname: mtaserver
Hostid: ########
Release: 5.8
Kernel architecture: sun4u
Application architecture: sparc
Hardware provider: Sun_Microsystems
Domain:
Kernel version: SunOS 5.8 Generic 108528-26 Oct 2003

mtaserver# cat /etc/release
                Solaris 8 7/01 s28s_u5wos_08 SPARC
        Copyright 2001 Sun Microsystems, Inc.  All Rights Reserved.
                  Assembled 06 June 2001
```

Running pkgirm indicates that there are 537 packages installed on the system. This is consistent with the System administrators' statement that the system was built using Sun's full distribution. Almost all of these packages are SUNW (Sun) packages. The actual MTA application consists of only one package.

2.6 INSTALLED APPLICATIONS AND SYSTEM PROCESSES

The primary product installed on the server is PMDF, described as "a high performance, standards-based Internet messaging product suite," by its vendor, Process Software. The pmdf version command gives details:

```
>pmdf version
PMDF version is PMDF V6.1-1
libpmdf.so version V6.1-1; linked 11:06:01, Jan 22 2002
SunOS mtaserver  5.8 Generic_108528-26 sun4u sparc
```

Other system processes and applications running on the system are revealed by ps-ef:

```
mtaserver# ps -e -o "user,comm" | grep -vi "admin_user_names"
   USER COMMAND
   root sched
   root /etc/init
   root pageout
   root fsflush
   root /usr/lib/saf/sac
   root /usr/lib/inet/xntpd
   root /usr/openwin/bin/fbconsole
   root /usr/lib/picl/picld
   pmdf /pmdf/bin/job_controller
   root /usr/lib/sysevent/syseventd
   root /usr/lib/sparcv9/cpudiagd
   root /usr/sbin/rpcbind
   root /usr/lib/saf/ttymon
   root /usr/sbin/nscd
   root /usr/lib/autofs/automountd
   root /usr/lib/nfs/lockd
   root /usr/openwin/bin/Xsun
   root /usr/lib/lpsched
   root rpc.metad
   root /usr/lib/inet/in.ndpd
   root devfsadmd
   root /usr/sbin/inetd
 daemon /usr/lib/nfs/statd
   root /usr/sbin/syslogd
   root /usr/lib/power/powerd
   root /usr/sbin/cron
   root /usr/lib/osa/bin/sparcv9/rdaemon
   root /usr/lib/utmpd
   root zsh
   root /usr/lib/osa/bin/arraymon
```

root /usr/lib/osa/bin/sparcv9/rdaemon
root /usr/sbin/vold
root rpc.metamhd
root /usr/lib/saf/ttymon
root /usr/bin/dsmc
root /usr/dt/bin/dtlogin
root /usr/local/sbin/sshd
root rpc.metamhd
pmdf <HTTP>
root dtgreet
root -sh
root -sh
root /usr/local/sbin/sshd
root rpc.metad
root -sh
root zsh
pmdf /pmdf/bin/dispatcher
root /usr/dt/bin/dtlogin
root in.telnetd
root in.telnetd
root ps
root zsh
pmdf <SMTP>

The ps indicates that the server is being accessed via telnet ,a clear-text login protocol and rpc services (rpcbind, rpc.metamhd , rpc.metad) are in use. An alternative to telnet and ftp, sshd, is also running.

Further, inetd, which listens on sockets and starts servers as requested, is running indicating a review of /etc/inetd.conf is in order to see which services are available on this server.

Also note this server has a window manager, CDE (notice the processes: powerd, dtlogin, dtgreet, Xsun).

As noted earlier, nfs is running, also indicated by mountd, lockd and statd running.

The remaining processes are on the system to provide necessary services include backups, storage array management , time, host lookup caching, cron scheduled services , logging/monitoring and system processes. The dsmc process is a daemon running as a client for backups via Tivoli Storage Manager. The rdaemon process is a redundant controller resolution daemon process and arraymon is a RAID monitoring process , both for the A1000 storage array. Time of day services are provided by xntpd. The network cache daemon, nscd is commonly run on MTA systems to cache nslookups. UNIX systems use cron to run scheduled jobs. Syslogd and utmpd log system events and monitor processes. Sun's cpudiag is running to detect cpu errors.

2.7 SERVER PURPOSE AND USAGE

The server was deployed to provide gateway MTA services for GIAC University. It receives all incoming mail, scans it for viruses and then delivers it to internal mail systems with user mailboxes. All outgoing mail is transmitted to the internet from this server after being virus scanned.

Since the University has several internal mail systems for different categories of users, as well as various departments, an extensive directory or alias service is maintained on the server with routing information for users.

As another server ran low on disk space, a partition was created on the server to hold accounting logs from that server. This is a secondary and unplanned service, necessitated by a lack of resources to add space to another server. It is expected these files will be moved soon and are only temporarily in use on the system.

Although it does not formally serve web pages, the MTA software, the PMDF product includes an administrative web interface and starts a web server at boot to serve the administrative pages.

2.8 NETWORK ENVIRONMENT

The server is located on a subnet reserved for certain servers on the GIAC University's Class C network. Although the University is in the process of implementing a firewall, because of the nature of the MTA services provided on the server, this server will remain open to the Internet or possibly in the DMZ, depending on decisions made by the Network Group at the University.

3 . DETAILED ANALYSIS

GIAC University has a need for a written,consistent, and simple security policy or higher-level set of guidelines focusing on host-based security to guide the system administrator's in prioritizing time and resources. Although policy by it's nature is highly individualized depending on the institution or entity it serves, some basic security rules could guide the University in developing their policies:

1) Defense in Depth
2) Avoid clear-text protocols in favor of encrypted protocols
3) Use least privilege
4) Minimize the OS and running processes to those reasonably necessary
5) Use good logging and monitoring tools to detect problems
6) Stay aware of needed patches and upgrades and apply them in a timely fashion.

Model security policies are available from SANS at http://www.sans.org/resources/policies/ and can serve as examples to help the University develop a framework policy for Solaris host-based security on the University's systems. Formation of this policy will help the University realize it's goal of maximizing security with existing resources.

3.1 OPERATING SYSTEM VULNERABILTIES

The installation of the Solaris "Full" distribution cluster. The audit system has over 500 packages installed, while a core installation will result in only about 80 packages installed. The MTA product accounts for another package, so conservatively, there are probably 5 times as many packages as needed on this system. Some amenities like the admin's favorite shell, remote X11 Windowing, and documentation account for adding several more packages to the system.

Although minimization is not straightforward, once the admins have determined the appropriate "base" install of the OS, it can be adjusted as appropriate depending on the applications on any given server. For example, if it is determined that a windowing manager such as CDE will be run on servers, then, a minimized CDE without extra and often vulnerable apps, such as Calendar manager, can be developed. Also, once, the administrators determine whether a Sun or an open source version of an application such as sendmail will be run, then the appropriate packages can be retained or removed. For example, this system runs a non-sendmail MTA, yet the sendmail packages remain on the system. (In Solaris 9, the OS this system will most likely be rebuilt to, minimization at a more granular level is available, making this process easier.)

Additionally, minimizing the operating system eases day-to-day management of the system, as far fewer OS patches apply.

File system partitions. The system has only one partition for root, although the MTA product does have it's own file system for its software, mail queues and logging. Usually, separate partitions are recommended for /var and /usr. Since logging can fill up the /var filesystem, separating it from root will prevent the root file system from being filled up. The /usr file system , containing system binaries, can and should be mounted read only, if it is a separate file system. (cis-scan 6.1)

3.2 SECURITY PATCH INSTALLATION

The emphasis on timely review and installation of OS patches, particularly security patches brought out in the System Administrator interview is evident in a review of the current patch status of the system. Running the Sun contract tool, patchdiag, indicates that only a few patches are out or rev. Although a few patches are listed in the Security section as uninstalled, the System administrators note that these are patches which require one or more packages not installed on the system. See the Appendices for the output of patchdiag | grep -vi current. As mentioned above, the time requirements for managing patches could be reduced by installing a minimized OS.

The system firmware is at the current level per the prtdiag command information and information from the current patch: 111292-15.

Fix-modes not run. Casper Dik's fix-modes program changes the permissions on many files and is recommended to be run both post-install and post-patching sessions to increase filesystem security. The program does not appear to have been run on this system. (cis-scan 6.9)

3.3 CONFIGURATION VULNERABILITIES

Inetd running and listening for unneeded services. A consequence of installing the "Full" distribution is that many services are included in inetd. Both the cis-scan and nessus tools noted many unnecessary running services, including: time,echo,discard,daytime,chargen,exec,comsat, uucp,100146/1, 100147/1, 100150/1,rstatd, sprayd, telnet, ftp, rsh, rlogin, kerberos net daemon ktkt_warnd, kerberos net daemon gssd. Nessus also noted rpcbind , shell. login, uucp, lockd, X11 "sometimes-rpc" ports, general/icmp and general/udp, general/tcp,sunrpc (portmapper) , 32782/udp, xdmcp, icmp, rstatd, as open and with security notes. Cis scan recommended using tcp-wrappers for many of these services, if they have to be run. Tcp-wrappers can effectively limit which IPs or system names can connect via the wrapped service and is preferable to leaving a vulnerability-prone service wide-open to the campus, or possibly, even the Internet. (cis-scan 1.2, 2.1,2.2,2.3,2.4,2.10,3.3) (nessus List of open ports and security warnings. Cis-scan also noted many IP6 services available. Since the system admins indicated these are not in use, they should be disabled. (cis-scan 1.2) If inetd is run, connection logging with the -t option is useful to monitor connections. (cis-scan 5.2)

Serial login prompt not disabled. The system administrators indicated that they are currently using the serial port for diagnostics and feel that it should not be disabled as the system is located in an access-restricted machine room. (cis-scan 3.1)

ip, tcp and arp settings should be altered. (cis-scan 4.4,4.5) Cis-scan identified a number of settings that should be reset:
--disable source routing (ip_forward_src_routed and ip6_forward_src_routed)
--set minimum tcp_conn_req_max_q0 value of 4096 and tcp_ip_abort_cinterval to at most 60,000 to avoid tcp flooding
--set ip_respond_to_timestamp and ip_respond_to_timestamp_broadcast to 0.
--set ip_ignore_redirect and ip6_ignore_redirect to 1.
--set ARP timers to at least 60,000 (arp_cleanup_interval, ip_ire_arp_interval)
--activate strict multihoming (ip_strict_dst_multihoming and ip6_strict_dst_multihoming)
--set ip_send_redirects to 0

Syslog allowing remote logging. This is another default as-installed setting. It is recommended that syslog be run with the -t switch to disable this functionality. (cis-san 3.4)

Multiple programs not disabled in the rc boot scripts. A number of default services are

started or available on the system. Unless there is a specific need for a service, it should not be available or running. These include: nfs.server services in.rarpd,and rpc.bootparamd. Although the system is an nfs client, it does not serve nfs and does not need these present. (cis-scan 3.6)

The following were determined to not be deactivated: llc2, uucp, slpd, PRESERVE, bdconfig, wbem,ncalogd, ncad, mipagent, autoinstall, asppp, cachefs.daemon, cacheos.finish, power, autofs, rpc, LDAP cache manager, lp, spc, volume manager, dtlogin, apache, coredumps (cis-scan 3.7, 3.9,3.10,3.11,3.14,3.15,3.16,3.17,3.18,3.19,4.1)

NFS clients aren't restricted to privileged ports. Again, the system has not been altered from it's default as-installed state. (cis-scan 4.3)

Neither accounting or kernel auditing enabled. (cis-scan 5.4,5.5,5.6)

3.4 RISKS FROM INSTALLED THIRD-PARTY SOFTWARE

Openssh version is vulnerable. Debug version information indicates that the installed version has not been updated to 3.71p1 which is not vulnerable to the latest reported vulnerability:

ssh -vv localhost
OpenSSH_3.6.1p1, SSH protocols 1.5/2.0, OpenSSL 0x0090702f

OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability

http://securityfocus.org/bid/7467/discussion/

A discussion about this vulnerability with the system admins revealed that they were aware of it and while they had made some use of the ssh package prior to this last announced vulnerability, there had been some reluctance to move more fully to ssh because of it's security track record. Also, the version of ssh in use on this system came in an easily installed package form from Sunfreeware, but because of the hurricane and possibly other considerations, it took over a week for the new version to be posted. This led the admins to postpone further implementation until a firm decision is reached on the version of ssh to use. The admins are considering Openssh or non-commercial ssh as alternatives, but want to weight the decision carefully, as once implemented across all the Solaris systems, a change will be disruptive to make.

PMDF EXPN and VRFY. Nessus indicated that the PMDF program responded to these commands. The configuration should be changed to disallow these commands which give out information about users. (nessus Security warning)

PMDF RELAYING. Nessus claims PMDF is open to relaying. Since PMDF acts as the MTA, it is properly configured to allow relaying from a small group of internal servers. (nessus Security warnings.)

SMTP server running. Since mtaserver is a mail server, this is expected. (It is interesting to note that nessus fingerprints PMDF as the Sun Internet Mail Server. In fact, Sun bought the PMDF vendor, Innosoft ,and incorporated PMDF into it's Mail Server product. The original PMDF product was then purchased by Process Software, the current vendor.)

Lack of banners on services. Appropriate banners should be used to indicate that only authorized use is allowed and that usage may be monitored.

FTP vulnerability. Nessus indicated an ftp vulnerability. The ftp service is installed as part of the OS and appears to be patched to the latest level. No Sun Alert indicates that the service is vulnerable to the glob heap corruption vulnerability. Note that nessus clearly indicates that this vulnerability is based solely on the banner. (nessus Security hole)

3.5 ADMINISTRATIVE PRACTICES

Administration with RSH, TELNET and FTP. As noted in the system administrator's interview and indicated by the presence of a .rhosts file for a system administrator's account, rsh (shell) is in use for management purposes (CIS-scan 7.1) Openssh or non-commercial SSH should be used instead to provide encrypted services. (cis-scan 2.4) It is appropriate that root does not have a . rhosts file. (cis-scan 7.2) (nessus Security warnings) Nessus also notes that rlogin is enabled and should be disabled for the same reasons. (nessus Security Warniings.) In addition, X11 is in use, yet another clear-text protocol. (nessus Security Warnings. XDMCP, CIS-scan 7.5) The use of X11 forwarding through SSH or Openssh would provide an encrypted tunnel for the X11 sessions

Cleartext protocols in use. As noted above, telnet and ftp are in use both for administrative access and for automated file transfer. (cis-scan 2.2,2.3) (nessus List of open ports and security warnings)

Openssh or the non-commercial version of SSH a (along with sftp) are considered appropriate replacements for telnet and ftp. (Although Solaris 9 has Sun's version of Openssh available, Solaris 8 did not have a Sun ssh package.)

Multiple conf files limiting access or system usage do not exist. Including : /etc/shells., /etc/default/login (CIS-scan 7.4, 7.12

EEPROM not password protected. When queried the administrators stated that they purposely choose not to password protect the eeprom because of the difficulty of replacement if the password is lost and because good physical security exists for the system's location. (CIS-scan 7.13)

3.6 IDENTIFICATION AND PROTECTION OF SENSITIVE DATA ON THE HOST

The email queues on the MTA contain messages bound into and out of the University and are moderately sensitive. Most users recognize that unencrypted email is not secure and therefore

should not have a high expectation of privacy in these communications. However, realistically, much sensitive data and information is transmitted via email on a regular basis and this information must be treated with care.

Certainly, the queues should be protected from ordinary users; they in fact are- owned 700 by the user pmdf, and further, no ordinary users have accounts on the system.

At present, accounting files from another system are being stored on this MTA system. The information is primarily used for forensics and data compilation as to usage patterns, but does constitute a record of user usage of system applications and resources and while not highly sensitive should be considered private information only available to administrators. These files are owned 700 by a nonexistent user (20311.) and should be owned by root instead.

3.7 PROTECTION OF SENSITIVE DATA IN TRANSIT OVER THE NETWORK OR INTERNET

Data is transferred between a web server and this system by ftp. The data consists of email forwarding aliases used in the directory channel. This data is not extremely sensitive, but iit s private to each user and select administrative and support personnel. The use of sftp between the systems would be preferable.

3.8 ACCESS CONTROLS

Excess privilege. As noted in the Systems Administrator's interview, a junior staff member performs Postmaster duties as root. File permissions and ownership along with ACL's should be used as appropriate along with sudo or RBAC to allow these tasks to be performed without the necessity of root access.

Password policies . Passwords are set at the default as installed with no minimum or maximum lifetimes or expiration notifications. Cis-scan recommends setting a minimum or 7 days and a maximum of 1 to 91 days with an expiration notification of 7 days, to be set in the file for such purposes, /etc/default/passwd. (cis-scan 8.3)

World-accessible home directories. Two users, sshd and fwd have world readable and executable directories. A discussion with the system administrator's indicated that the sshd home directory was purposely created 755, per instructions on the Sunfreeware site, for privilege separation. http://sunfreeware.com/openssh8.html

The administrator's also indicated that he second directory, fwd, used for automated data transfer, was most likely hand-created. The use of useradd to create new accounts would avoid the accidental creation of directories with insecure permissions.

Even though no ordinary users have access to this system, the existing permissions on the fwd account are not good practice and should be changed to 700. (cis-scan 8.7)

Set SYSLOG_FAILED_LOGINS to 0 in /etc/default/login. (cis-scan 5.3)

System accounts with shell by default. Accounts uucp,listen, nobody4,adm,daemon,bin.lp.nobody and noaccess all have no listed shell in/etc/passwd by default—but cis-scan points out that this means they all have the sh shell by default. An explicit "false shell" should be set.

Insufficient umask settings. Multiple umask settings are too weak, including / etc/default/login, /etc/default/ftpd, /etc/profile and /etc/.login (CIS-scan 8.10)

Talk allowed. Reconfigure /etc/profile and .etc/.login to block. (CIS-scan 8.11)

3.9 BACKUP POLICIES AND DISASTER PREPAREDNESS

The University has an excellent backup and disaster recovery plan with backups run nightly to a local tape library located in an access-restricted machine room. For disaster recovery, the backups are copied offsite the next day to another location.

3.10 OTHER SECURITY ISSUES

System logging is not in use. The system administrator's noted that although system accounting is run on systems with many users, it is generally not judged useful on systems with few users. (cis-scan 5.5)

4. CRITICAL ISSUES AND RECOMMENDATIONS

4.1 TOP TEN VULNERABILITIES AND ISSUES

The goal of this audit was to provide Management and the Solaris System administrator's with helpful information to maximize their scarce time and money resources to secure GIAC University's Solaris servers. Given that network firewall settings are largely determined by the Network Group at the University, this audit has focused on host-based security recommendations.

4.1.1 Use of clear-text protocols – replace with encrypted protocols including ssh and sftp

Probably the biggest "bang for the buck", that is increase in security for a small investment of time, would be to replace the current reliance on clear-text protocols, notably, telnet, ftp and rsh with ssh or Openssh.

While this auditor is understanding of the administrators' desire to review the choices and make the best choice of ssh software, the decision needs to be made soon, and ssh implemented for management purposes, as well as for sensitive data transfer between the systems. If the admins choose to go with sunfreeware, they can enjoy the ease of package installation, at the possible price of some delay in updating, although it appears that the site is very well maintained, and in usual circumstances (no hurricanes on the east coast!), updates are quickly available.

If the admins choose to use non-commercial ssh or Openssh from openssh.org, then they will need to compile the source for each version of the OS they run. One recommendation is for the admins to become comfortable with the process of creating Sun packages so that they could compile and then package the ssh or openssh binaries themselves, and quickly and easily distribute them to all of their Solaris systems. While this will require the expenditure of some "learning curve " time resources, the time would be well spent in allowing quick updates as soon as patched source is available from whichever software source the admins settle on. This skill would be useful for other installs as well.

The admins can use tcp-wrappers to further limit access to ssh and access in general to servers, which can also help mitigate the issues surrounding timelines of patching by limiting the ability of others to reach the sshd server in the first place. Again, implementing tcp wrappers is fairly straghtforward, and effort spent on this process can also be applied to other inetd -started services. Theopenssh version available from Sunfreeware includes tcp-wrappers functionality.

Even if ports are blocked at the firewall, it is often said that many of a University's worst enemies are on the inside—so blocking these services at both the firewall and on all hosts where they are not needed is a good example of the well-known security principal of defense in depth.

4.1.2 Many unnecessary inetd services running – disable all but essential services; use tcp-wrappers

Another big win in terms of time spent and security gains made is the analysis of inetd-provided services to determine which are essential and must be run. All others can be disabled, which can significantly reduce the opportunities for exploitation. The rpc services are numerous on this system. (See the output of rpcinfo in the appendices.) Real consideration should be made as to whether any of these are essential on this system. Unfortuneately, since rpc services are randonly assigned ports which are registered to a portmapper daemon, blocking ports is not very effective in controlling access to these services. The better approach is to limit these as much as reasonably possible.

Tcp-wrappers was mentioned above to control ssh access. It is an easy to administer approach to controlling access to services provided through inetd and would allow the system administrator's to block access to the essential services they feel they may need to continue running out of inetd. For example, if an administrator feels strongly about retaining telnet access as an alternative or back-up to ssh, limiting telnet access to the administrators systems and VPN connections would be preferable to leaving the service open to the Internet, where anyone can attempt to connect to the server.

4.1.3 Default file system security - run fix-modes after install and patch application

Another fairly straightforward improvement to the security of Solaris servers, particularly those running Solaris 8 or earlier, like the audit server, is to run Casper Dik's fix-modes program on the system after the initial install. (Note that much of the functionality has supposedly been

incorporated into Solaris 9 although it is still recommended as a build step on Solaris 9 systems.)

The fix-modes program places more restrictive permissions on files and increases file system security. Fix-modes should also be run after patching, as the new files installed by a patch typically revert to the original default permissions and attributes.

Since fix-modes can be run with the -u argument to undo any changes made by the previous run, it appears to be quite safe. In fact, at the UNIX Solaris training course, San Diego 2003, instructor Hal Pomeranz commented that he has never had any problems from running fix-modes. The fix-modes.README file lists other arguments which can be used to limit the actions of fix-modes to suit the cautious administrator's needs.

4.1.4Junior staff with excess privilege – use sudo or RBAC to control access

Although trust in employees is important , particularly in a small staff setting, the principle of least privilege essentially states that a process or user should have no more privilege than necessary to perform the task required to be performed. (Garfunkel/Spafford, 124) The postmaster duties that are currently performed by a junior staff member, even though a trusted staff member, should be limited to conform to the tenets of least privilege.

Applying least privilege to the the postmaster's duties on this system implies that only postmaster account access and access to the directory (alias) files are needed on this system. Postmaster has duties on other systems as well, and the best solution would be for the administrators to analyze the permissions necessary and access required for the postmaster job and then build either an RBAC role for postmaster to assume on the systems affected, or perhaps configure sudo access for postmaster. One problem is that postmaster must edit files, which because of the ability to get a shell from many editors, presents an access problem. The administrator's may need to explore the use of ACLs to give this user appropriate access to certain, but not other files.

Once the most appropriate method of setting appropriate privilege for this position is determined, the same principle may well be applied to other tasks which the administrator's perform and provide a gradual shift from the use of full root access for performing administration tasks to the use of an RBAC approach.

4.1.5 Insufficient monitoring and logging – Use inted -t, system accounting, host-based firewall

The administrator's state that they do not believe this system has ever been compromised, and although they manually monitor the system log files, this auditor recommends that increased logging through the use of tcp-wrappers, use of the inetd -t option, possibly system accounting, and possibly the installation of a host-based firewall such as Suncreen Lite(Sunscreen on Solaris 9) would provide the additional information to better monitor the system.

Unfortunately, all this logging takes a lot of time to monitor, so the use of a tool such as

logcheck would be very useful to the administrators to maximize the efficiency of their time in scrutinizing the logs. A further benefit of adding logcheck is that automated system event notification can send administrators notices via pager or email about important system events, including ones that are not necessarily security-related.

4.1.6 OS "full" distribution install – Minimize the OS to a reasonable level

The administrator's can gain time savings in two ways by making their initial installation of the Solaris OS a minimized one. First, with fewer packages installed on the system to begin with, there are fewer services installed by default requiring further evaluation and potential removal. With fewer services and programs available, there are fewer avenues of attack, so the system is more secure just by virtue of being simpler. Finally, when day-to-day maintenance is concerned, the patching process is less complex, because fewer patches need to be applied to a smaller OS.

The downside to minimization is producing the minimized OS in the first place. None of the distribution clusters will provide the exact set of packages to suit the needs of every server. Most security experts recommend the choice of the core cluster, with subsequent modification to add and remove packages to achieve the desired final OS state. For example, man pages may be desired, but are not included, nor are utilities to read them, in the Core distribution. Likewise, sendmail is included in the Core distribution but may not be desired on some systems, such as the audited system, which runs a different MTA. Note, however (see patchdiag output in the Appendices) that the sendmail package was never removed from this system. It is good practice to remove unneeded packages both for minimization and to avoid leaving binaries which go unpatched because of possible interactions with another installed product.

While minimization requires a perhaps substanial initial time expenditure, if well-planned, a basic core system can be built (standalone or with jumpstart archives) for all servers at GIAC University. After the base install, some additional work may be required to determine the remaining necessary packages to add. Sun Blueprints, written by Alex Noordergraaf, detail several aspects of the process. The "Minimization " Blueprint, gives general information on the process and includes some package templates or lists of packages to provide certain "Infrastructure" services.

Although not immediately obvious, excellent additional suggestions are detailed in two subsequent Blueprints about Minimizing SunFire domains, that have applicability to non-domained systems minimization. Alex suggests having a test server which has been installed with the Full distribution available, to aid in determining the package origin of specific files. Alex also provides methods to detect dependent files using truss; finding dynamic library dependencies using the ldd command, and finding package dependencies using the depend-tree.pl script . Additionally, a methodology for installing applications and removing unneeded dependent applications is explained. Since some products, such as Sunscreen , explicitly claim to require the full distribution, knowing how to remove unneeded dependent packages is very helpful in the minimization process.

In summary, minimization is admittedly a rather complex and not entirely straightforward process—particularly if carried to the nth degree. However, a reasonable minimization approach may be well suited to GIAC University, in which, either the core or end user Distribution is chosen and

obvious unneeded packages are removed from the chosen distribution. Being a compromise, this approach would increase security somewhat without requiring an undue investment of the administrator's limited time resources. The real key to making minimization work for the administrators is for them to develop a base install which is complete enough to provide most needed functionality for most servers without weighing down the servers with unneeded packages better suited to desktop installs.

4.1.7Unexpiring passwords – Improve password expiration policy

Poor password management makes getting shell access simple for intruders. The cis-scan pointed out that the default password policy was in place with essentially no expiration of passwords and no maximum or minimum time limits on password duration. Setting these limits forces password changes and makes inactive accounts more apparent so that they can be handled accordingly. (Perhaps the account is no longer needed or can be locked.)

While not as big a problem on a server with a limited number of accounts, such as the audited system, a good password policy should be developed and used on all Solaris systems at GIAC University. Systems with many accounts may need to have a somewhat different and more manageable policy than servers with limited access, but a general policy with specific refinements for special cases should be formed. This auditor suggests that the administrators of this system run Jack the Ripper or a similar password cracking program against at least all elevated privilege account passwords including those for system administrators and root to determine that adequately chosen passwords are in use.

4.1.8Openssh vulnerable – Upgrade/closely monitor 3rd party software applications

Software needs to be upgraded on a regular basis, and particularly quickly when a security vulnerability is found and a patch or new version becomes available. The administrators and the auditor have discussed the issue of the Openssh software being out-of-date on this system.It is unwise to leave a vulnerable application in place, whether it is regularly run, or only used by an administrator occasionally.

Security programs, in particular, must be closely monitored and upgraded when vulnerabilities are found. In addition to tracking versions in use on different systems, the administrators are monitoring security news to keep up-to-date. The administrators do need to prioritize security upgrades ahead of other duties.

4.1.9Banners reveal version information – Replace with "Authorized use/monitoring language"

Banners serve several important purposes. First, default banners can be an unnecessary

source of information about a system's OS and the versions of apps it is running. Because of this, it is best to configure banners to provide minimal information of use to would-be attackers or scanners.

Second, banners should be used to notify those accessing a system service on a system that the system is only for authorized use and that usage of the system may be monitored, to comply with federal laws regarding monitoring, such as the Patriot Act.

Finally, as Hal Pomeranz points out, in Solaris Security, Step by Step, appropriate notices in /etc//issue and /etc/motd as well as banners for telnet (/etc/default/telnetd (if telnet) and other services may bolster the likelihood of criminal prosecutions of attackers. The notices and banners should make two points—THAT only authorized use is allowed and that use constitutes consent to monitoring. Good examples of sample notices and banners can be found in the above mentioned Step by Step guide.

4.1.10No written Solaris host-based security guidelines or policy - formulate written policy

It's hard to know where you're going to end up when you don't have a plan. In order to effectively administer security in a Solaris environment where time and money resources are limited, it is important to prioritize the most important actions to take based on a plan which implements a given policy. The security needs of a University, where free exchange of ideas is promoted, are quite different from the corporate environment, where trade secrets and proprietary information may be well-defined and clearly in need of protection. Universities have business and confidential information protection needs similar to those of businesses, yet usually do not have the power to enforce the tightness of security found in corporate or regular business environments.

Policy does vary a great deal from even one University to another, but formulation of a reasonable policy is essential to guide the system administrators in determining the best allocation of their time and budget in creating an appropriately secure environment. In some ways, creation of a written policy may actually be the most important recommendation that this auditor can make, however, it also requires investments in time and substantial planning which may practically mean that policy has to be created over time, and sculpted from a rough framework into a more elegant and applicable form incrementally..

4.2FURTHER RECOMMENDATIONS AND CONCLUSION

The administrators can learn a great deal from simply studying the output of the CIS-scan and nessus scan tools, which is included in the Appendices. The rating produced by the CIS-scan was quite low and it would be interesting as well as instructive for the administrators to make the initial changes recommended above and then run cis-scan and nessus for themselves and see how the rating changes.

In addition to the Top Ten vulnerabilities listed in this section, the weaknesses in Section three of this document should be carefully reviewed and the indicated fixes considered for

application by the system administrators in a teimely fashion.

There are several excellent guides available which focus on securing Solaris systems, including Sun Blueprint publications and the SANS Securing Solaris publication. Review of these publications and application of suggested security changes to a test build followed by running the cis-scan and nessus tools against the newly built server would provide excellent feedback to the administrators about the security choices they've incorporated. The administrators current approach to building systems using their own customized scripts is quite refined and an excellent framework for expansion to include additional system hardening.

It is helpful, that unlike many Universities only a few years ago, GIAC University sees a need for increasing security to a reasonable level and is willing to put efforts into improving the state of security at the institution. As is not uncommon, human and budgetary resources will most likely continue to be at a premium at GIAC University, but with a reasonable devotion of time to the security framework and recommendations presented here, the base level of Solaris host-based security can be increased substantially within the University's means.

References

- Noordergraff, Alex, "Solaris Operating Environment Minimization for Security: A Simple, Reproductible, and Secure Application Installation Methodology Updated for the Solaris 9 Operating Environment" November 2002 URL:http://www.sun.com/solutions/blueprints/1102/816-5241.pdf (accessed 25 October 2003)

- Noordergraff, Alex, "Jumpstart Architecture and Security Scripts for the Solaris Operating Environement – Part 1." http://www.sun.com/solutions/blueprints/1100/jssec-updt1.pdf (accessed 25 October 2003)

- Noodrergraff, Alex, "Jumpstart Architecture and Security Scripts for the Solaris Operating Environement – Part 2." http://www.sun.com/solutions/blueprints/1100/jssec2-updt1.pdf (accessed 25 October 2003)

- Noordergraff, Alex, "Jumpstart Architecture and Security Scripts for the Solaris Operating Environement – Part 3." http://www.sun.com/solutions/blueprints/1100/jssec3-updt1.pdf (accessed 25 October 2003)

- Pomeranz, Hal, Solaris Security :Step-by-Step" URL: http://www.deer-run.com/~hal/SolarisWebcast.pdf (accessed 25 October 2003)

- SANS INSTITUTE, drafted and edited by Hal Pomeranz, Derr Run Associates, Solaris Security Step by Step Version 2.0 2001.

- Spitzner, Lance, Armoring Solaris: II, Preparing Solaris 8 64-bit for CheckPoint Firewall-1 NG" URL:http://www.spitzner.net/armoring2.html

- Softpanorama Open Source Software Educational Society ,"Solaris hardening page" URL: http://www.softpanorama.org/Security/Solaris/index.shtml (accessed 15 November 2003)

- Security Focus Vulnerabilities URL:http://securityfocus.org/bid/vendor/ (accessed 1 December 2003)

- SANS INSTITUE, "The SANS Security Policy Project", URL:http://www.sans.org/resources/policies/#top (accessed 1December 2003)

- Christensen, Steve, "Sunfreeware.com Freeware for Solaris." URL:http://sunfreeware.com Solaris 8 nessus 2.0.5 Solaris package.(accessed 25 November 2003)

- Center for Internet Security, CIS Benchmarks/Security Tools. URL:http://cisecurity.org/ Solaris cis-scan package (accessed 28 November 2003)

- Garfinkel. Simson and Spafford, Gene, Practical UNIX & Internet Security. Cambridge, O'Reilly & Assocaites, Inc., Second Edition, 1996.

- Gregory, Peter H., Solaris Security. Upper Saddle River, New Jersey, Sun Microsystems Press, A Prentice Hall Title, 2000.

Acknowledgments

Assignment format example from:

Poer, Geoffrey, "Auditing a University Solaris System." Geoffrey_Poer_GCUX.pdf
http://www.giac.org/GCUX.php

Trademark acknowledgment example from:

Bailey, Jeffrey, "Operating Environment Minimisation for Security."
http://www.sans.org/rr/papers/index.php?id=539

Appendices

CIS SCAN RESULTS

```
  mtaserver# cat /opt/CIS/cis-ruler-log.20031201-20:12:55.958
*** CIS Ruler Run ***
Starting at time 20031201-20:12:55

Positive: 1.1 System appears 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 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 tcp-protocol service uucp 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.
Positive: 1.3 System is running sshd and it's configured well.
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 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 uucp -- 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 rstatd/2-4 -- 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: 2.2 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.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 BSD-compatible printer server is deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Not applicable: 2.9 Not applicable on Solaris versions prior to 9.
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.
Positive: 3.2 Found a good daemon umask of 022 in /etc/default/init.
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 cachefs.daemon not deactivated.
Negative: 3.7 cacheos.finish not deactivated.
Negative: 3.7 power not deactivated.
Not Applicable: 3.8 Not applicable to Solaris versions prior to 9.
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.
Not Applicable: 3.12 This item is not applicable to releases prior to Solaris 9.
Not Applicable: 3.13 This item is not applicable to releases prior to Solaris 9.
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.
Positive: 3.19 SNMP daemon is deactivated.
Not Applicable: 3.20 Not applicable to Solaris versions prior to 9.
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 Stack is set non-executable and logs violations.
Negative: 4.3 NFS clients aren't restricted to privileged ports.
Negative: 4.4 Source routing (ip_forward_src_routed) should be deactivated
Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be deactivated
Negative: 4.4 tcp_conn_req_max_q0 should be at least 4096 to avoid TCP flood problems.
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 ip_ignore_redirect isn't set to 1.
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 ip_strict_dst_multihoming isn't activated.
Negative: 4.5 ip6_strict_dst_multihoming isn't activated.
Negative: 4.5 ip_send_redirects isn't set to 0.

Positive: 4.6 TCP sequence numbers strong enough.
Positive: 5.1 syslog captures auth messages.
Negative: 5.2 inetd is running, but does not do "-t" connection tracking.
Negative: 5.3 SYSLOG_FAILED_LOGINS should be 0 in /etc/default/login.
Positive: 5.4 cron usage is being logged.
Negative: 5.5 Couldn't find an active sadc line in /etc/rc2.d/S21perf to verify system acctg.
Negative: 5.5 No sa1 line in /var/spool/cron/crontabs/sys -- no system accounting.
Negative: 5.5 No sa2 line in /var/spool/cron/crontabs/sys -- no system accounting.
Negative: 5.6 kernel-level auditing isn't enabled.
Positive: 5.7 All logfile permissions and owners match benchmark recommendations.
Negative: 6.1 Never found separate /usr partition, so it couldn't be mounted read-only.
Negative: 6.1 /opt/pmdf is not mounted non-SUID-capable (nosuid) or read-only (ro).
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.
Negative: 6.9 Fix-modes has not been run here.
Negative: 7.1 /etc/pam.conf appears to support rhost auth.
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
Negative: 7.4 /etc/shells does not exist.
Negative: 7.5 /etc/dt/config/Xaccess doesn't exist, thus permits remote X-terminal login.
Not Applicable: 7.6 Not applicable to Solaris versions prior to 9.
Negative: 7.7 /etc/dt/config/en_US.UTF-8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 7.7 /etc/dt/config/C/sys.resources doesn't exist, so screenlocker can't be set.
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/sys 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 No banner line in /etc/default/ftpd.
Negative: 7.10 /etc/dt/config/en_US.UTF-8/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Negative: 7.10 /etc/dt/config/C/Xresources doesn't exist, so alternate GUI welcome message can't be set.
Positive: 7.11 Root is only allowed to login on console
Negative: 7.12 /etc/default/login doesn't limit login attempts (RETRIES setting).
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.
Positive: 8.2 All users have passwords
Negative: 8.3 User admin1 should have a minimum password life of at least 7 days.
Negative: 8.3 User admin1should have a maximum password life of between 1 and 91 days.
Negative: 8.3 User admin1 should have a password expiration warning of at least 7 days.
Negative: 8.3 User admin2 should have a minimum password life of at least 7 days.
Negative: 8.3 User admin2 should have a maximum password life of between 1 and 91 days.
Negative: 8.3 User admin2 should have a password expiration warning of at least 7 days.
Negative: 8.3 User pmdf should have a minimum password life of at least 7 days.
Negative: 8.3 User pmdf should have a maximum password life of between 1 and 91 days.
Negative: 8.3 User pmdf should have a password expiration warning of at least 7 days.
Negative: 8.3 User pmdfuser should have a minimum password life of at least 7 days.
Negative: 8.3 User pmdfuser should have a maximum password life of between 1 and 91 days.
Negative: 8.3 User pmdfuser should have a password expiration warning of at least 7 days.
Negative: 8.3 User postmaster should have a minimum password life of at least 7 days.
Negative: 8.3 User postmaster should have a maximum password life of between 1 and 91 days.
Negative: 8.3 User postmaster should have a password expiration warning of at least 7 days.
Negative: 8.3 User fwd should have a minimum password life of at least 7 days.
Negative: 8.3 User fwd should have a maximum password life of between 1 and 91 days.
Negative: 8.3 User fwd 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.
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: 8.6 root's PATH is clean of group/world writable directories or the current-directory link.
Negative: 8.7 User www has a world-executable homedir!
Negative: 8.7 User www has a world-readable homedir!
Negative: 8.7 User sshd has a world-executable homedir!
Negative: 8.7 User sshd has a world-readable homedir!

Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc file.
Negative: 8.10 Current umask setting in file /etc/default/login is 000 -- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/default/login is 000 -- it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/default/ftpd is 000 -- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/default/ftpd is 000 -- it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/profile is 022 -- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/profile is 022 -- it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/.login is 000 -- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/.login is 000 -- it should be stronger to block group-read/write/execute.
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.
Preliminary rating given at time: Mon Dec 1 20:12:55 2003

Preliminary rating = 3.70 / 10.00

Negative: 6.7 Non-standard world-writable file: /etc/.java/.systemPrefs/.systemRootModFile
Negative: 6.7 Non-standard world-writable file: /etc/.java/.systemPrefs/.system.lock
Negative: 6.7 Non-standard world-writable file: /etc/init.d/dsmerror.log
Negative: 6.8 Non-standard SUID program /usr/lib/sendmail.org
Ending run at time: Mon Dec 1 20:12:59 2003

Final rating = 3.70 / 10.00

NESSUS RESULTS

Nessus Scan Report

SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 2
- Number of security warnings found : 19
- Number of security notes found : 44

TESTED HOSTS

10.10.10.25 (Security holes found)

DETAILS

+ 10.10.10.25 :
. List of open ports :
  o smtp (25/tcp) (Security warnings found)
  o telnet (23/tcp) (Security warnings found)
  o ssh (22/tcp) (Security notes found)
  o ftp (21/tcp) (Security hole found)
  o chargen (19/tcp) (Security warnings found)
  o daytime (13/tcp) (Security warnings found)
  o discard (9/tcp) (Security warnings found)

o echo (7/tcp) (Security warnings found)
o time (37/tcp) (Security notes found)
o rpcbind (111/tcp) (Security notes found)
o shell (514/tcp) (Security warnings found)
o login (513/tcp) (Security warnings found)
o exec (512/tcp) (Security warnings found)
o uucp (540/tcp) (Security notes found)
o submission (587/tcp)
o lockd (4045/tcp) (Security notes found)
o X11 (6000/tcp) (Security notes found)
o sometimes-rpc11 (32774/tcp)
o sometimes-rpc15 (32776/tcp)
o sometimes-rpc13 (32775/tcp) (Security notes found)
o sometimes-rpc21 (32779/tcp) (Security notes found)
o sometimes-rpc19 (32778/tcp)
o sometimes-rpc17 (32777/tcp) (Security notes found)
o general/icmp (Security warnings found)
o general/udp (Security notes found)
o general/tcp (Security notes found)
o sunrpc (111/udp) (Security notes found)
o sometimes-rpc18 (32777/udp) (Security warnings found)
o sometimes-rpc22 (32779/udp) (Security warnings found)
o unknown (32782/udp) (Security hole found)
o sometimes-rpc24 (32780/udp) (Security notes found)
o lockd (4045/udp) (Security warnings found)
o xdmcp (177/udp) (Security warnings found)
o echo (7/udp) (Security warnings found)
o daytime (13/udp) (Security warnings found)

. 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 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.

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)

An SMTP server is running on this port
Here is its banner :
220 mtaserver.giac.edu -- Server ESMTP (PMDF V6.1-1#40460)

. Information found on port smtp (25/tcp)

This server could be fingerprinted as being Sun Internet Mail Server sims.4.0.2001.07.26.11.50.p9

. Information found on port smtp (25/tcp)

Remote SMTP server banner :
220 mtaserver.giac..edu -- Server ESMTP (PMDF V6.1-1#40460)

. 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)

A telnet server seems to be running on this port

. Information found on port telnet (23/tcp)

Remote telnet banner :

SunOS 5.8

. Information found on port telnet (23/tcp)

Remote telnet banner :

SunOS 5.8

. Information found on port ssh (22/tcp)

An unknown service is running on this port.
It is usually reserved for SSH

. Information found on port ssh (22/tcp)

An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
Adore sshd
Shaft

Unless you know for sure what is behind it, you'd better
check your system

** Anyway, don't panic, Nessus only found an open port. It may
** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner
Risk factor : Low

. Vulnerability found on port ftp (21/tcp) :

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.

*** Nessus relied solely on the banner of the server to issue this warning,
*** so this alert might be a false positive

Solution : Upgrade your ftp server software to the latest version.
Risk factor : High

CVE : CAN-2001-0249, CVE-2001-0550
BID : 2550, 3581

. Information found on port ftp (21/tcp)

An FTP server is running on this port.
Here is its banner :
220 mtaserver FTP server (SunOS 5.8) ready.

. Information found on port ftp (21/tcp)

Remote FTP server banner :

220 mtaserver FTP server (SunOS 5.8) ready.

. 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 characters (something like all the characters in the alphabet in a row). 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' in which an attacker spoofs a packet between two
machines running chargen. This will cause them to spew 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 chargen (19/tcp)

Chargen is running on this port

. 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

. Information found on port daytime (13/tcp)

An unknown server is running on this port.
If you know what it is, please send this banner to the Nessus team:
00: 4d 6f 6e 20 44 65 63 20 20 31 20 32 30 3a 30 39 Mon Dec 1 20:09
10: 3a 32 30 20 32 30 30 33 0a 0d   :20 2003..

. Warning found on port discard (9/tcp)

The 'discard' port is open. This port is
not of any use nowadays, and may be a source of problems,

Solution : comment out 'discard' in /etc/inetd.conf

Risk factor : Low
CVE : CAN-1999-0636

. 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 : disable this service
CVE : CVE-1999-0103

. Information found on port echo (7/tcp)

An echo server is running on this port

. Information found on port time (37/tcp)

A time server seems to be running on this port

. Information found on port rpcbind (111/tcp)

The RPC portmapper is running on this port.

An attacker may use it to enumerate your list
of RPC services. We recommand you filter traffic
going to this port.

Risk factor : Low
CVE : CAN-1999-0632, CVE-1999-0189
BID : 205

. Information found on port rpcbind (111/tcp)

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

. Information found on port rpcbind (111/tcp)

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

. Information found on port rpcbind (111/tcp)

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

. 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

. 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 exec (512/tcp)

The rexecd service is open.
Because rexecd does not provide any good
means of authentication, it can be
used by an attacker 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

. Information found on port uucp (540/tcp)

An UUCP server seems to be running on this port

. Information found on port lockd (4045/tcp)

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

. Information found on port lockd (4045/tcp)

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

. Information found on port lockd (4045/tcp)

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

. Information found on port lockd (4045/tcp)

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

. Information found on port X11 (6000/tcp)

An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
The Thing

Unless you know for sure what is behind it, you'd better
check your system

** Anyway, don't panic, Nessus only found an open port. It may
** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner
Risk factor : Low

. Information found on port sometimes-rpc13 (32775/tcp)

RPC program #100229 version 1 is running on this port

. Information found on port sometimes-rpc21 (32779/tcp)

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

. Information found on port sometimes-rpc21 (32779/tcp)

RPC program #100133 version 1 is running on this port

. Information found on port sometimes-rpc17 (32777/tcp)

RPC program #100230 version 1 is running on this port

. Warning found on port general/icmp

The remote host answered to an ICMP_MASKREQ
query and sent us its netmask (255.255.255.0)

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 general/icmp

The remote host answers to an ICMP timestamp
request. This allows an attacker to know the
date which is set on your machine.

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

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

Risk factor : Low
CVE : CAN-1999-0524

. Information found on port general/udp

For your information, here is the traceroute to 10.10.10.25 :
10.10.43.1
10.10.34.78
10.10.10.25

. Information found on port general/tcp

Remote OS guess : Solaris 8 early access beta through actual release

CVE : CAN-1999-0454

. Information found on port sunrpc (111/udp)

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

. Information found on port sunrpc (111/udp)

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

. Information found on port sunrpc (111/udp)

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

. Warning found on port sometimes-rpc18 (32777/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

. Information found on port sometimes-rpc18 (32777/udp)

RPC program #100012 version 1 'sprayd' (spray) is running on this port

. Warning found on port sometimes-rpc22 (32779/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

Usually, it is not a good idea to let this
service open

Risk factor : Low
CVE : CAN-1999-0624

. Information found on port sometimes-rpc22 (32779/udp)

RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is
running on this port

. Information found on port sometimes-rpc22 (32779/udp)

RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is
running on this port

. Information found on port sometimes-rpc22 (32779/udp)

RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port

. Vulnerability found on port unknown (32782/udp) :

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

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

*** Nessus reports this vulnerability using only
*** information that was gathered. Use caution
*** when testing without safe checks enabled.

Solution : upgrade to the latest version of rpc.statd
Risk factor : High
CVE : CVE-2000-0666
BID : 1480

. 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 HOLES REGARDING THIS
PROGRAM HAVE BEEN TESTED, SO
THIS MIGHT BE A FALSE POSITIVE *

We suggest that you disable this
service.

Risk factor : High

CVE : CVE-1999-0018, CVE-1999-0019, CVE-1999-0493
BID : 127, 450

. Information found on port unknown (32782/udp)

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

. Information found on port unknown (32782/udp)

RPC program #100133 version 1 is running on this port

. Information found on port sometimes-rpc24 (32780/udp)

RPC program #100153 version 1 is running on this port

. Warning found on port lockd (4045/udp)

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

Risk factor : Low
CVE : CVE-2000-0508
BID : 1372

. Information found on port lockd (4045/udp)

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

. Information found on port lockd (4045/udp)

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

. Information found on port lockd (4045/udp)

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

. Information found on port lockd (4045/udp)

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

. Warning found on port xdmcp (177/udp)

The remote host is running XDMCP.

This protocol is used to provide X display connections for
X terminals. XDMCP is completely insecure, since the traffic and
passwords are not encrypted.

An attacker may use this flaw to capture all the keystrokes of
the users using this host through their X terminal, including
passwords.

Risk factor : Medium
Solution : Disable XDMCP

. 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 : disable this service
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

This file was generated by the Nessus Security Scanner

rpcinfo output:

```
rpci   program version netid     address          service    owner
   100000    4    ticots    mtaserver.rpc      rpcbind    superuser
   100000    3    ticots    mtaserver.rpc      rpcbind    superuser
   100000    4    ticotsord mtaserver.rpc      rpcbind    superuser
   100000    3    ticotsord mtaserver.rpc      rpcbind    superuser
   100000    4    ticlts    mtaserver.rpc      rpcbind    superuser
   100000    3    ticlts    mtaserver.rpc      rpcbind    superuser
   100000    4    tcp       0.0.0.0.0.111      rpcbind    superuser
   100000    3    tcp       0.0.0.0.0.111      rpcbind    superuser
   100000    2    tcp       0.0.0.0.0.111      rpcbind    superuser
   100000    4    udp       0.0.0.0.0.111      rpcbind    superuser
   100000    3    udp       0.0.0.0.0.111      rpcbind    superuser
   100000    2    udp       0.0.0.0.0.111      rpcbind    superuser
   100000    4    tcp6      ::.0.111           rpcbind    superuser
   100000    3    tcp6      ::.0.111           rpcbind    superuser
   100000    4    udp6      ::.0.111           rpcbind    superuser
   100000    3    udp6      ::.0.111           rpcbind    superuser
   100012    1    udp6      ::.128.8           sprayd     superuser
   100012    1    udp       0.0.0.0.128.9      sprayd     superuser
   100012    1    ticlts    \000\000\020\015   sprayd     superuser
   100001    2    udp6      ::.128.10          rstatd     superuser
   100001    3    udp6      ::.128.10          rstatd     superuser
   100001    4    udp6      ::.128.10          rstatd     superuser
   100001    2    udp       0.0.0.0.128.11     rstatd     superuser
   100001    3    udp       0.0.0.0.128.11     rstatd     superuser
   100001    4    udp       0.0.0.0.128.11     rstatd     superuser
   100001    2    ticlts    \000\000\020\030   rstatd     superuser
   100001    3    ticlts    \000\000\020\030   rstatd     superuser
   100001    4    ticlts    \000\000\020\030   rstatd     superuser
   100134    1    ticotsord \000\000\020\035   -          superuser
   100234    1    ticotsord \000\000\020       -          superuser
   100146    1    ticotsord \000\000\020#      amiserv    superuser
   100147    1    ticotsord \000\000\020&      amiaux    superuser
   100150    1    ticotsord \000\000\020)      ocfserv    superuser
   100229    1    tcp6      ::.128.6           -          superuser
   100229    1    tcp       0.0.0.0.128.7      -          superuser
```

```
100230    1    tcp6       ::.128.8            -          superuser
100230    1    tcp        0.0.0.0.128.9       -          superuser
100024    1    udp6       ::.128.13           status     superuser
100024    1    tcp6       ::.128.10           status     superuser
100024    1    udp        0.0.0.0.128.14      status     superuser
100024    1    tcp        0.0.0.0.128.11      status     superuser
100024    1    ticlts     \000\000\020:       status     superuser
100024    1    ticotsord \000\000\020=        status     superuser
100024    1    ticots     \000\000\020@       status     superuser
100133    1    udp6       ::.128.13           -          superuser
100133    1    tcp6       ::.128.10           -          superuser
100153    1    udp        0.0.0.0.128.12      -          superuser
100133    1    udp        0.0.0.0.128.14      -          superuser
100133    1    tcp        0.0.0.0.128.11      -          superuser
100133    1    ticlts     \000\000\020:       -          superuser
100133    1    ticotsord \000\000\020=        -          superuser
100133    1    ticots     \000\000\020@       -          superuser
100021    1    udp6       ::.15.205           nlockmgr   superuser
100021    2    udp6       ::.15.205           nlockmgr   superuser
100021    3    udp6       ::.15.205           nlockmgr   superuser
100021    4    udp6       ::.15.205           nlockmgr   superuser
100021    1    tcp6       ::.15.205           nlockmgr   superuser
100021    2    tcp6       ::.15.205           nlockmgr   superuser
100021    3    tcp6       ::.15.205           nlockmgr   superuser
100021    4    tcp6       ::.15.205           nlockmgr   superuser
100021    1    udp        0.0.0.0.15.205      nlockmgr   superuser
100021    2    udp        0.0.0.0.15.205      nlockmgr   superuser
100021    3    udp        0.0.0.0.15.205      nlockmgr   superuser
100021    4    udp        0.0.0.0.15.205      nlockmgr   superuser
100021    1    tcp        0.0.0.0.15.205      nlockmgr   superuser
100021    2    tcp        0.0.0.0.15.205      nlockmgr   superuser
100021    3    tcp        0.0.0.0.15.205      nlockmgr   superuser
100021    4    tcp        0.0.0.0.15.205      nlockmgr   superuser
100099    4    ticotsord mtaserver.autofs     -          superusernfo:
```

PATCHDIAG OUTPUT

> patchdiag | grep -vi current

```
================================================================================
======================
System Name: mtaserver   SunOS Vers: 5.8        Arch: sparc
Cross Reference File Date: Nov/21/03

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  Installed Latest   Synopsis
  ID   Revision  Revision
------ --------- -------- ------------------------------------------------------------
108820   01        02    SunOS 5.8: nss_compat.so.1 patch
108921   17        18    CDE 1.4: dtwm patch
109244   02       -------
109318   33        34    SunOS 5.8: suninstall Patch
109887   17        18    SunOS 5.8: smartcard and usr/sbin/ocfserv patch
109896   21        22    SunOS 5.8: USB and Audio Framework patch
110423   02       -------
110615   01        10    SunOS 5.8: sendmail patch
110843   02        03    Obsoleted by: 110849-06 SunOS 5.8: libprtdiag_psr.so.1 patch for S
110849   14        15    SunOS 5.8: PICL support for SUNW,Sun-Fire-880
```

```
110943    01       02    SunOS 5.8: /usr/bin/tcsh patch
110951    04       05    SunOS 5.8: /usr/sbin/tar and /usr/sbin/static/tar patch
110988    04    -------
111019    06    -------
111021    03    -------
111382    01    -------
================================================================================
======================
```

UNINSTALLED RECOMMENDED PATCHES

```
Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev       ID         ID
------ --- --- --- --------- --------- ----------------------------------------
108576 N/A  45  90                 SunOS 5.8: Expert3D IFB Graphics Patch
1
109951 N/A  01 1201                SunOS 5.8: jserver buffer overflow
111879 N/A  01 826                 SunOS 5.8: Solaris Product Registry patch SUNWwsr
112279 N/A  02 549                 SunOS 5.8: pkgrm failed during upgrade from Solaris 8
to Solaris 9
114152 N/A  01 356                 SunOS 5.8: Japanese SunOS 4.x Binary Compatibility
(BCP) patch
114251 N/A  01 200                 SunOS 5.8: pkgrm failed if upgrade from S8U7 to upper
release with
================================================================================
======================
```

UNINSTALLED SECURITY PATCHES

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

```
Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev       ID         ID
------ --- --- --- --------- --------- ----------------------------------------
1
109951 N/A  01 1201                SunOS 5.8: jserver buffer overflow

110416 N/A  03 851                 SunOS 5.8: ATOK12 patch
111332 N/A  06 329                 SunOS 5.8: /usr/lib/dcs patch
111647 N/A  01 847                 BCP libmle buffer overflow
112390 N/A  08  25 109223-02       SunOS 5.8: Supplemental Encryption Kerberos V5:
mech_krb5.so.1 pat
113652 N/A  03 343 108528-17 108528-18 (or newer) SunOS 5.8: Supplemental Kernel
Update Patch for 108528-17
114045 N/A  03 192                 SunOS 5.8: Netscape Portable Runtime(4.1.4)/Network
Security Syste
```

114146 N/A 01 357 108528-16 108528-17 (or newer) SunOS 5.8: Supplemental Kernel Update Patch for 108528-16

==========

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

All Y2K patches installed!