Global Information Assurance Certification Paper

Real-World Solaris 8 Security Audit using CISscan

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 2

Jennifer Scalf
Sept 9, 2004

Abstract

As part of our campus's total enhancement of our server security policies we are requiring our servers to be audited. In the next year all of our servers must be audited on a routine basis. This document will cover the first CISscan audit performed on the University's heaviest traffic Solaris 8 UNIX server. This server currently provides email, web, SSH, SFTP, MySQL, and many other services for the University campus. In the past this server has provided many other applications to students, staff and faculty, and while most of these older applications were turned off, it is critical that we scan this machine make sure no vulnerabilities have been missed. If there are vulnerabilities then thousands of accounts and any other servers connected to this server could also be compromised.

The entire auditing process will be covered, from a description of the software I will use and why, to the results of the scans, to coverage of what we do to fix any problems and highlights of the positive findings. This is also an interesting study of how to handle 'legacy' servers and software and what to do when you really can't change the current security policy. This will not be an in-depth study of the actual security vulnerabilities since each one is a very lengthy discussion. Nor do I just list the commands we used because you can find most of the commands in the Solaris Benchmark PDF. Instead this case study touches on the very wide range of issues found when one undertakes auditing a heavily used student server.

This document will be useful to any Solaris UNIX system administrators who would like a case study of one type of Solaris server audit. This will be beneficial to new system administrators interested in what it means to perform a CISscan audit, what to look for and what other administrators are doing to fix the problems that the CISscan finds.

Background

The server being audited is used by thousands of students on a university campus. The server has been operational and constantly in use for approximately 3 years. At various times in the last 3 years a total of 5 system administrators have been in charge of the server. At this time there are 3 administrators. Because of the number of people who have administered the server it should be audited to make sure the programs that were installed were installed, and are running, securely.

Even though Solaris 8 was installed on the server 3 years ago, many older programs were migrated to the server to meet the demands of students familiar with older software and unwilling to change. This older software might have security vulnerabilities, such as insecure file privileges; therefore it is very important to run an audit that covers file permissions.

The server is used mainly as an email (POP and IMAP) and web (Apache)

server. Students also have shell accounts on the server. They are able to use SSH to access it. At this time Telnet has been disabled. FTP has not been disabled but there has been a lot of talk about disabling it since most universities are going that way. It will be replaced by SFTP, which is available at this time.

Students who to use SSH to connect to the server do so mostly to run Pine to check their email. While we have POP, IMAP and Webmail available to all users, some prefer to use Pine and Mutt to check their email. Other programs students run from the command line are; gcc, javac, ssh (mainly onto other University servers), pico, vi/vim, emacs, ftp, wget, lynx, and a few use the newly installed MySQL. Shells people use are; Bash, Ksh and Tcsh. The default for newly created users is Bash. There has never been a system wide audit for file permissions; however the all of our servers are constantly being scanned by Nessus. It is important for us to find out if any of the student's programs are installed and/or running insecurely.

Finding the Vulnerabilities

To find out what vulnerabilities exist on the server I used CISscan. It is a host based scoring tool created and given out by the Center for Internet Security (CIS) specifically for auditing Solaris.

It is important to choose a good auditing tool because a poor or out-of-date tool will not help improve your security and might even hurt it because it might give the system administrators a false sense of security. I chose the CISscan because it was recommended by the University's IT security staff, they have used it and were confident that it is thorough. It is referred to in the SANS Security Essentials manual in many places. And I researched it and found most people in other organizations were also happy with the scoring tool. The latest release of the CISscan was Oct 2003, which is a little dated. However I feel it will still be helpful because Solaris 8 is also a few years old.

Running the First Scan

Even before running the scan I knew there would be negative findings because this server has never had this kind of audit performed. The first scan was performed to determine exactly what the current problems were so that I could determine the risk and form a plan as to how to fix the vulnerabilities.

The server's score after the first scan was 4.11 out of 10.

Negative Results from the First CIS Scan

```
Negative: 1.1 System appears not to have been patched within the last
month.
Negative: 1.2 udp-protocol service comsat in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service finger in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service krbinfo in inetd.conf is not
wrapped.
Negative: 1.2 tcp-protocol service mackrbinfo in inetd.conf is not
wrapped.
Negative: 1.2 udp-protocol service talk in inetd.conf is not wrapped.
Negative: 2.1 inetd listens on port comsat -- this port's line should
be commented out or deleted in inetd.conf.
Negative: 2.1 inetd listens on port talk -- this port's line should be
commented out or deleted in inetd.conf.
Negative: 2.1 inetd listens on port finger -- this port's line should
be commented out or deleted in inetd.conf.
Negative: 2.2 telnet not deactivated.
Negative: 2.4 rlogin (rlogin) should be deactivated.
Negative: 3.1 Serial login prompt not disabled.
Negative: 3.3 inetd is still active.
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 PRESERVE not deactivated.
Negative: 3.7 bdconfig not deactivated.
Negative: 3.7 ncalogd not deactivated.
Negative: 3.7 ncad not deactivated.
Negative: 3.7 autoinstall not deactivated.
Negative: 3.9 NFS Server script nfs.server not deactivated.
Negative: 3.10 NFS script nfs.client not deactivated.
Negative: 3.11 rpc rc-script (rpcbind) not deactivated.
Negative: 3.14 LDAP cache manager not deactivated.
Negative: 3.18 Web server not deactivated.
Negative: 4.1 Coredumps aren't deactivated.
Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be
deactivated
```

```
Negative: 4.4 ip6_ignore_redirect isn't set to 1.
Negative: 4.4 ARP timer (arp_cleanup_interval) should be at most
60,000.
Negative: 4.4 ARP timer (ip_ire_arp_interval) should be at most 60,000
Negative: 4.5 ip6_strict_dst_multihoming isn't activated.
Negative: 5.1 syslog does not permanently capture auth messages.
Negative: 5.2 syslog does not permanently capture daemon.debug
messages.
Negative: 5.2 inetd is running, but does not do "-t" connection
tracking.
Negative: 5.3 /var/adm/loginlog doesn't exist to track failed logins.
Negative: 5.3 SYSLOG_FAILED_LOGINS should be 0 in /etc/default/login.
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.
Negative: 6.1 /usr is not mounted read-only.
Negative: 6.5 /etc/shadow is not owned by group sys!
Negative: 6.9 Fix-modes has not been run here.
Negative: 7.3 /etc/ftpusers doesn't exist
Negative: 7.5 /etc/dt/config/Xaccess needs a global deny !* line.
Negative: 7.5 /etc/dt/config/Xaccess needs a global deny !* CHOOSER
BROADCAST line.
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 Non-root accounts are in 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/sys are not
sufficiently restrictive.
Negative: 7.9 The permissions on /var/spool/cron/crontabs/uucp are not
sufficiently restrictive.
Negative: 7.10 EEPROM banner isn't on.
Negative: 7.10 /etc/issue doesn't have a authorized-use banner.
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.
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 smtp 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 adm has a valid shell of /sbin/sh.
```

```
Negative: 8.1 daemon has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 bin has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 lp has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 noaccess has a valid shell of /bin/sh.  Remember, an
empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.3 User <username removed> should have a minimum password
life of at least 7 days.
Negative: 8.3 User <username removed> should have a maximum password
life of between 1 and 91 days.
Negative: 8.3 User <username removed> should have a password expiration
warning of at least 7 days.
.
. <100+ similar lines cut for the sake of saving paper>
.
Negative: 8.3 /etc/default/passwd doesn't have a value for MAXWEEKS.
Negative: 8.3 /etc/default/passwd doesn't have a value for MINWEEKS.
Negative: 8.3 /etc/default/passwd doesn't have a value for WARNWEEKS.
Negative: 8.6 Directory /usr/openwin/bin is in root's PATH and is
group-writable.
Negative: 8.7 User <username1 removed> has a world-executable homedir!
Negative: 8.7 User <username1 removed> has a world-readable homedir!
Negative: 8.7 User <username2 removed> has a world-executable homedir!
Negative: 8.7 User <username2 removed> has a world-readable homedir!
Negative: 8.7 User <username3 removed> has a world-executable homedir!
Negative: 8.7 User <username3 removed> has a world-readable homedir!
Negative: 8.7 User <username3 removed> has a world-executable homedir!
Negative: 8.7 User <username4 removed> has a world-readable homedir!
Negative: 8.7 User <username5 removed> has a world-executable homedir!
Negative: 8.7 User <username5 removed> has a world-readable homedir!
Negative: 8.7 User <username6 removed> has a world-executable homedir!
Negative: 8.7 User <username6 removed> has a world-readable homedir!
.
. <13,000+ lines cut for the sake of saving paper>
.
Negative: 8.8 User <username1 removed> has world/group-writable dot-
files (.*) in his/her home directory.
Negative: 8.8 User <username2 removed> has world/group-writable dot-
files (.*) in his/her home directory.
Negative: 8.8 User <username3 removed> has world/group-writable dot-
files (.*) in his/her home directory.
.
. <100+ similar lines cut for the sake of saving paper>
.
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.
Negative: 6.7 Non-standard world-writable file: /etc/minor_perm
Negative: 6.7 Non-standard world-writable file: /etc/driver_classes
Negative: 6.7 Non-standard world-writable file: /etc/name_to_major
Negative: 6.7 Non-standard world-writable file:
/usr/kernel/drv/sparcv9/syncsort_sa.conf
Negative: 6.7 Non-standard world-writable file: /etc/driver_aliases
Negative: 6.7 Non-standard world-writable file:
/usr/kernel/drv/syncsort_sa.conf
Negative: 6.8 Non-standard SGID program /etc/mlock
```

Positive results from the First CIS Scan

```
Positive: 1.3 System is running sshd and it's configured well.
Positive: 2.3 ftp is 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.
Positive: 2.10 kerberos network daemons are deactivated.
Positive: 3.2 Found a good daemon umask of 022 in /etc/default/init.
Positive: 3.4 System is not running syslogd, thus syslogd is not
listening to the network.
Positive: 3.15 The printer init scripts are deactivated.
Positive: 3.16 volume manager is deactivated.
Positive: 3.17 Graphical login scripts are all deactivated.
Positive: 3.19 SNMP daemon is deactivated.
Positive: 4.2 Stack is set non-executable and logs violations.
Positive: 4.3 NFS clients use privileged ports.
Positive: 4.6 TCP sequence numbers strong enough.
Positive: 5.4 cron usage is being logged.
Positive: 5.7 All logfile permissions and owners match benchmark
recommendations.
Positive: 6.2 logging option is set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 /etc/dfs/dfstab doesn't have any non-fully qualified
pathname share commands.
Positive: 6.6 all temporary directories have sticky bits set.
Positive: 7.1 pam.conf appears to have rhost auth deactivated.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either
don't exist or are links to /dev/null.
Positive: 7.4 /etc/shells exists and has good permissions.
Positive: 7.11 Root is only allowed to login on console
Positive: 8.2 All users have passwords
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.9 No user has a .netrc file.
```

Analysis of the Negative Findings and Proposed Solutions

I have broken the findings down into the numbered sections created by the scoring tool. I am using the CIS Sun Solaris Benchmark as a guide, along with outside sources listed in the Reference section to evaluate each section or item. Since I am certain that the scanning tool I have chosen has accurately assessed the server. I will use its results as the definition of risk.

After each result or group of results I will answer the following questions based on their relevance to the result or group of results. The best way to address such a long list of issues is to; Address what the issue is, why the server was configured the way it was, and then what changes may or may not be made.

- What does the Negative or Positive result mean? - Depending on the clarity of the item, I will elaborate on or interpret its meaning.
- Why did the vulnerability exist? - Depending on the item, I will explain the history of the vulnerability.
- What changes are going to be made? - After discussing the findings with the other system administrators and researching the impact on our current system installation, I will discuss what changes will be made.

Or

- Why changes will not be made? - After discussing the findings with the other system administrators and researching the impact on our current system installation, I will discuss why changes cannot or will not be made.

Negative Section 1

```
Negative: 1.1 System appears not to have been patched within the last
month.
```

- What does the Negative or Positive result mean? The negative result is because the system has not been patched with Sun Microsystems patch in the last month.
- Why did the vulnerability exist? The system was not patched in the month before the scan was run because there were no Solaris 8 patches that were relevant to our installation. In June 2004, Sun released the following Sun Alert ID in their Patch Report; 57575, 57577, 57578, 57582, 57524, 57539. None of these are relevant to our architecture. 2 of the alerts were for Sun Ray servers (our server is a v440), one was for the Sun Crypto Accelerator, which we don't use, one dealt with CDE, which is not installed on our server, another was related to the wheel mouse (there is no mouse connected to our server), and another was for power management software that we don't use.
- Why changes will not be made? Since we have the latest security related patches installed (every patch relevant up to kernel patch 117000-05) no changes will be made.

```
Negative: 1.2 udp-protocol service comsat in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service finger in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service krbinfo in inetd.conf is not
wrapped.
Negative: 1.2 tcp-protocol service mackrbinfo in inetd.conf is not
wrapped.
Negative: 1.2 udp-protocol service talk in inetd.conf is not wrapped.
```

- What does the Negative or Positive result mean? These Negative results are because the named programs are not wrapped by tcp_wrapper in the configuration file /etc/inet/inetd.conf.
- Why did the vulnerability exist? Sun's version of finger is not used on the server because historically there have been many vulnerabilities in the software, such as the ability to list all accounts on the server that have never been used. Since the senior administrator of the server is also familiar with the operating system OpenBSD, he prefers its port of the finger program. The installed finger program is from the OpenBSD port's CVS checkout and has all of the latest patches. This version is wrapped in /etc/hosts.allow.
- What changes are going to be made? All of the services will be wrapped.

Negative Section 2

```
Negative: 2.1 inetd listens on port comsat -- this port's line should
be commented out or deleted in inetd.conf.
Negative: 2.1 inetd listens on port talk -- this port's line should be
commented out or deleted in inetd.conf.
Negative: 2.1 inetd listens on port finger -- this port's line should
be commented out or deleted in inetd.conf.
Negative: 2.2 telnet not deactivated.
Negative: 2.4 rlogin (rlogin) should be deactivated.
```

- What does the Negative or Positive result mean? These Negative results have to do with standard network services installed when Solaris 8 is installed. According to the Sun Solaris Benchmark most of the default items in inetd.conf should be disabled.
- Why did the vulnerability exist? The vulnerabilities existed because in the past all of these services have been used and were not wrapped properly.
- What changes are going to be made? See Section 1, they will all be wrapped.
- Why some changes will not be made? Telnet and rlogin are not in use; however they will not be disabled because both have to have banners telling users to use SSH. In the past telnet and rlogin were available, they were just recently "turned off" from the users perspective. Therefore the banner will have to stay until it is determined that it is no longer useful.

Negative Section 3

```
Negative: 3.1 Serial login prompt not disabled.
```

- What does the Negative or Positive result mean? This item relates to the use of serial terminals, modems, and "other remote access devices" (Sun Benchmark 13).
- Why did the vulnerability exist? There is a serial terminal connected to the server.
- Why changes will not be made? A serial terminal is used to access the server to perform off site maintenance, such as rebooting. The server is locked inside of a cabinet, inside two separate secure doors, we feel at this time it is unlikely unauthorized users can attach serial devices to the machine.

```
Negative: 3.3 inetd is still active.
```

- What does the Negative or Positive result mean? This program is "a daemon that is responsible for starting other daemons as they are needed" (Nemeth, Snyder, Seebass, Hein 822).

- Why did the vulnerability exist? The Daemon, inetd is being used to start various daemons named in Section 2.
- What changes are going to be made? The Daemon, inetd tracing (-t) will be enabled.
- Why changes will not be made? The daemon will not be disabled; it starts services that are still in use.

```
Negative: 3.5 Mail daemon is on and collecting mail from the network.
```

- What does the Negative or Positive result mean? The email server uses the mail daemon and that is seen as a Negative result by the auditing software.
- Why did the vulnerability exist? The server is an email server and this is considered to be a vulnerability by the auditing tool.
- Why changes will not be made? No changes will be made because the server will continue to be an email server and therefore the mail daemon will need to be on and collect 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.
```

- What does the Negative or Positive result mean? Reverse Address Resolution Protocol daemon. Used for disk less machines to receive an IP address.
- Why did the vulnerability exist? The vulnerability existed because it was mistakenly left on. It was not suppose to be on. It is not used and the firewall blocks it.
- What changes are going to be made? It will be disabled.

```
Negative: 3.7 llc2 not deactivated.
```

- What does the Negative or Positive result mean? llc2 is a driver for a number of interfaces network software, for example; NetBIOS, SNA, and OSI.
- Why did the vulnerability exist? This was left on in the past because the system administrators were not clear as to if we needed it or not for our network interfaces.
- What changes are going to be made? After looking into it I found we do

not need this for our network interfaces, it will be disabled.

```
Negative: 3.7 uucp not deactivated.
```

- What does the Negative or Positive result mean? UNIX-to-UNIX Copy Protocol**.** Solaris's PPP uses UUCP's configuration file. This is related to managing dial-up modems.
- Why did the vulnerability exist? This was mistakenly left on, it is supposed to be off; it is blocked by the firewall.
- What changes are going to be made? It will be disabled.

```
Negative: 3.7 PRESERVE not deactivated
```

- What does the Negative or Positive result mean? The text editor vi uses this to save a copy of the current file being worked on in case the editor crashes.
- Why did the vulnerability exist? It is in use on the server.
- Why changes will not be made? It is currently in use it therefore no changes will be made.

```
Negative: 3.7 bdconfig not deactivated.
```

- What does the Negative or Positive result mean? "The `bdconfig` utility is responsible for configuring the autopush facility and defining to the system what serial device to use for the `bd` stream." – UNIX bdconfig MAN (Manual) Page on Solaris 8.
- Why did the vulnerability exist? This service was mistakenly left on, is supposed to be off; it is not configured on the server.
- What changes are going to be made? It will be disabled.

```
Negative: 3.7 ncalogd not deactivated.
Negative: 3.7 ncad not deactivated.
```

- What does the Negative or Positive result mean? What does the Negative or Positive result mean? According to the white paper *The Solaris Network Cache and Accelerator Solaris,* "The Solaris Network Cache and Accelerator ("NCA ") is a kernel module designed to provide improved web server performance." Sun's Apache uses this service.
- Why did the vulnerability exist? It was mistakenly left on after it was

installed as part of the default Solaris installation.

- What changes are going to be made? The Sun default Apache web server is not being used as the server because is has historically had major vulnerabilities. It will be disabled. The web server software that is installed is the newest patched version http://www.apache.org/

```
Negative: 3.7 autoinstall not deactivated.
```

- What does the Negative or Positive result mean? This item is related to Jumpstart and installation, however I could not find out a lot of information about this service.
- Why did the vulnerability exist? It was mistakenly left on after it was installed as part of the default Solaris installation.
- What changes are going to be made? This service will also be disabled. Servers are not installed from this server; there is a separate Jumpstart server on campus.

```
Negative: 3.9 NFS Server script nfs.server not deactivated.
```

- What does the Negative or Positive result mean? This item refers to the NFS (Network File Server) server.
- Why did the vulnerability exist? This was mistakenly left on.
- What changes are going to be made? This will be disabled because this server is not a NFS server at this time.

```
Negative: 3.10 NFS script nfs.client not deactivated.
```

- What does the Negative or Positive result mean? This item refers to the NFS (Network File Server) client which enables the server to mount directories from the separate NFS server on campus.
- Why did the vulnerability exist? This is an NFS client therefore it needs the nfs.client script; the CISscan considers this a vulnerability.
- Why changes will not be made? Because the server is an NFS client the script cannot be deactivated at this time.

```
Negative: 3.11 rpc rc-script (rpcbind) not deactivated.
```

- What does the Negative or Positive result mean? According to the rpcbind

man (manual) page, "rpcbind is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine."

- Why did the vulnerability exist? Sun's rcpbind is not used on the server and is blocked by the firewall, however it is still installed. It was mistakenly not deactivated.
- Why changes will not be made? 3rd party rcpbind is installed on the server that is more secure than Sun's default. This version of rpcbind is wrapped with tcp_wrapper in our /etc/hosts.allow, therefore no changes will be made.

```
Negative: 3.14 LDAP cache manager not deactivated.
```

- What does the Negative or Positive result mean? The LDAP cache manager is needed for LDAP (Lightweight Directory Access Protocol).
- Why did the vulnerability exist? LDAP is not installed on the server; this daemon was installed by default and was mistakenly left on.
- What changes are going to be made? It will be disabled.

```
Negative: 3.18 Web server not deactivated.
```

- What does the Negative or Positive result mean? This item indicates this server has a web server daemon running.
- Why did the vulnerability exist? The server is a web server and this is considered to be a vulnerability by the auditing tool.
- Why changes will not be made? None, the server will continue to be a web server.

Negative Section 4

```
Negative: 4.1 Coredumps aren't deactivated.
```

- What does the Negative or Positive result mean? When certain programs fail they "dump core". This file can contain sensitive information. However, coredumps are useful for debugging because they contain information about why the process failed.
- Why did the vulnerability exist? The system administrators on the servers and the student developers learning to program on the server use coredumps for debugging.
- Why changes will not be made? No changes will be made because we will

continue to use coredumps, they are helpful for the system administrators and the student programmers. We also use the coreadm utility recommended in the Sun Solaris Benchmark.

```
Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be
deactivated
Negative: 4.4 ip6_ignore_redirect isn't set to 1.
```

- What does the Negative or Positive result mean? "*IPv6* is the network layer protocol used by the Internet protocol version 6" (FreeBSD Manual Pages)
- Why did the vulnerability exist? This was installed by default and mistakenly not turned off.
- What changes are going to be made? Because we do not use ip6, it will be disabled.

```
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
```

- What does the Negative or Positive result mean? The both variables have to do with identifying how long ARP information is stored.
- Why did the vulnerability exist? There are many custom scripts and custom configurations on the server. This is a good example where a customization was written campus wide and installed on the server.
- What changes are going to be made? Both arp_cleanup_interval, and ip_ire_arp_interval will be set to a value inside the correct parameters to fix this vulnerablity.

```
Negative: 4.5 ip6_strict_dst_multihoming isn't activated.
```

- What does the Negative or Positive result mean? This item also has to do with ip6 security. "Strict destination multihoming prevents packet spoofing on non-routing multihomed systems." (Prentice Hall Professional Technical Reference)
- Why did the vulnerability exist? On the server, ip6 is not used so this isn't really a vulnerability.
- Why changes will not be made? Nothing will be changed because ip6 filtering does not need to be strengthened because ip6 is not used on the server.

Negative Section 5

```
Negative: 5.1 syslog does not permanently capture auth messages.
Negative: 5.2 syslog does not permanently capture daemon.debug
messages.
```

- What does the Negative or Positive result mean? Syslog is a central logging system. Instead of programmers writing their own logs, they can use syslog. Administrators can then forward their log messages to where ever they like. (Nemeth, Snyder, Seebass, Hein 210)
- Why did the vulnerability exist? The server's syslogs are forwarded to a central hold location. However since it is not the default holding area the scan does not know that and reported it as a vulnerability.
- Why changes will not be made? Since we do permanently capture the auth messages and the daemon.debug messages, just not in the default way, there is nothing to change.

```
Negative: 5.2 inetd is running, but does not do "-t" connection
tracking.
```

- What does the Negative or Positive result mean? See Section 3.
- What changes are going to be made? We will enable tracing (-t) so that connections are tracked.

```
Negative: 5.3 /var/adm/loginlog doesn't exist to track failed logins.
```

- What does the Negative or Positive result mean? Failed login attempts can be logged in this file. If a user types in a bad password 5 times in a row then that information is logged. There are options to also drop a user (hang up) after a number of attempts. (Garfinkel and Spafford 299)
- Why did the vulnerability exist? On the server syslog captures unsuccessful logins so it hasn't been an issue in the past.
- What changes are going to be made? After reviewing it with the senior system administrator, failed logins will be tracked with loginlog.

```
Negative: 5.3 SYSLOG_FAILED_LOGINS should be 0 in /etc/default/login.
```

- What does the Negative or Positive result mean? The SYSLOG_FAILED_LOGINS variable is how many times a user has to fail logging in before it's logged in /var/adm/loginlog
- Why did the vulnerability exist? There are thousands of users everyday login and hundreds who make many failed attempts to login therefore our

SYSLOG_FAILED_LOGINS is set to 5.

- Why changes will not be made? No changes will be made because the logs would become huge.

```
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.
```

- What does the Negative or Positive result mean? These items are related to Sun's SAR (System Activity Reporter). This is a package Sun's include to perform advanced system reporting.
- Why did the vulnerability exist? Sun's SAR (System Activity Reporter) is not used on the server and therefore the result returned that it is not configured.
- Why changes will not be made? No changes will be made because there are no plans to use this software in the near future. There are already system-reporting logs that reviewed on a daily basis.

```
Negative: 5.6 kernel-level auditing isn't enabled.
```

- What does the Negative or Positive result mean? Kernel-level auditing basically records every process, command and system call performed on the server. (CIS Solaris Benchmark 32)
- Why did the vulnerability exist? The logs would have grown very large, very fast if this was enabled, therefore it has not been.
- Why changes will not be made? In the future we might tightly configure what is logged so that the log does not become large, however this is past the scope of this project.

Negative Section 6

```
Negative: 6.1 /usr is not mounted read-only.
```

- What does the Negative or Positive result mean? According to the Sun Solaris Benchmark, the /usr directory must be mounted with read-only permissions for maximum security.
- Why did the vulnerability exist? It caused too many problems while patching and installing new software when /usr was tested with read-only permissions. Right now the directory is world read and executable. There are non-root accounts that run programs that need /usr to have more

relaxed permissions.

- Why changes will not be made? In the future this idea will be explored further. This is defiantly something that will be investigated for possible changes on all of the servers. Also at this time nothing in /usr is world-write-able and many files under it are user or group read-only.

```
Negative: 6.5 /etc/shadow is not owned by group sys!
```

- What does the Negative or Positive result mean? According to many sources the file /etc/shadow, which contains user encrypted password information, should be owned by the group 'root'.
- Why did the vulnerability exist? There are various 3rd party programs that feel /etc/shadow should be group owned by either 'root' or 'sys', that have been installed on the server. Therefore at the time of this scan it was group owned by 'root'.
- What changes are going to be made? It will be changed to group-owned by 'sys'.

```
Negative: 6.9 Fix-modes has not been run here.
```

- What does the Negative or Positive result mean? In the Sun Solaris Benchmark the fix-mode package is explained as a tool to correct important system file privileges.
- Why did the vulnerability exist? There are too many customized and 3rd party software packages to have used this in the past.
- Why changes will not be made? In the future this tool will be looked into, possible as an addition to our installation process. No changes will be made that this time because this is a mission critical machine and I cannot risk changing the wrong permissions on important software.

Negative Section 7

```
Negative: 7.3 /etc/ftpusers doesn't exist
```

- What does the Negative or Positive result mean? This is a file used by Sun's FTP program where administrators list which users they do not want to let FTP onto the server.
- Why did the vulnerability exist? Sun's FTP program is not used on the server, therefore the file /etc/ftpusers doesn't exist.
- Why changes will not be made? PureFTP is used on the server instead of Sun's ftp server software. It does not use this file therefore the ftpusers file

will not be added to the server.

```
Negative: 7.5 /etc/dt/config/Xaccess needs a global deny !* line.
Negative: 7.5 /etc/dt/config/Xaccess needs a global deny !* CHOOSER
BROADCAST line.
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.
```

- What does the Negative or Positive result mean? These files are configuration files for the Sun X server.
- Why did the vulnerability exist? Even though this server is not an X server, and the files are not being used, the CISscan considers this a vulnerability.
- Why changes will not be made? No changes will be made because this is not an X server. Also, in the file '/etc/dt/config/Xaccess' the line ' CHOOSER BROADCAST' is commented out.

```
Negative: 7.8 Non-root accounts are in cron.allow.
```

- What does the Negative or Positive result mean? Cron.allow is where the list of users allowed to create cron jobs is kept.
- Why did the vulnerability exist? There are users that create their own cron jobs and more importantly the system administrators run a lot of services and programs under unprivileged accounts for security reasons. For example there is an account in cron.tab that owns our tapeback up cron job, a printing program, and other jobs that should not be owned by root. These programs must own cron jobs to function correctly, however the CISscan considers this a vulnerability.
- Why changes will not be made? Since the programs using unprivileged accounts will need to run cron jobs they will have to have entries in cron.allow, therefore nothing will be changed.

```
Negative: 7.8 Couldn't open at.allow
```

- What does the Negative or Positive result mean? The ‘at’ program is an older program that is similar to cron, except it's used for deferred jobs that will only run once. (Garfinkel and Spafford 352)
- Why did the vulnerability exist? It is not installed on the server; therefore there are no configuration files for it. Even though it is not installed and

neither are its configuration files, CISscan considers this a vulnerability.

- Why changes will not be made? There is an at.deny file, which denies everyone from using it. Therefore nothing will be changed.

```
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/sys are not
sufficiently restrictive.
Negative: 7.9 The permissions on /var/spool/cron/crontabs/uucp are not
sufficiently restrictive.
```

- What does the Negative or Positive result mean? The permissions on these files should be tightened.
- Why did the vulnerability exist? These files were part of the default Solaris install and are not actually being used; the default permissions were owner, group and world read-able.
- What changes are going to be made? The files will be secured by changing their permission to 400 – owner read-only.

```
Negative: 7.10 EEPROM banner isn't on.
```

- What does the Negative or Positive result mean? This is the banner people would see when logging in via the console.
- Why did the vulnerability exist? Users do not log into the server via the console, they connect via SSH or FTP. There is a banner for SSH. They also have to agree to the user account policy which includes most of what the Sun Solaris Benchmark recommends before they are allowed an account.
- What changes are going to be made? In the future an EEPROM banner maybe added.
- Why changes will not be made? At the present time no one would see the banner because no one logs into a monitor connected to the server, therefore, at this time, no changes will be made.

```
Negative: 7.10 /etc/issue doesn't have a authorized-use banner.
```

- What does the Negative or Positive result mean? The /etc/issue banner would appear when users SSH-ed onto the server.
- Why did the vulnerability exist? The server has a MOTD (Message of the Day). It has never been part of the security policy to have an additional issue banner.

- Why changes will not be made? New users must accept an account policy agreement when they are filling out the new account form. In this agreement they are told what they can and cannot do on the server. The university policy makers, at this time, feel that this policy is enough therefore no changes will be made.

```
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.
```

- What does the Negative or Positive result mean? These are configuration files for the Sun X server.
- Why did the vulnerability exist? This server is not and never will be an X server; therefore it will not have any GUI welcome messages. CISscan considers this a vulnerability.
- Why changes will not be made? None of those files exist because the server is not an X server therefore no changes will be made.

```
Negative: 7.12 /etc/default/login doesn't limit login attempts (RETRIES
setting).
```

- What does the Negative or Positive result mean? Login attempts should be tracked because they can be used to identify unauthorized users and break-ins. There is a variable 'RETRIES' that can be set to limit the number of times a user can try to login before they are prevented from logging in.
- Why did the vulnerability exist? This is not set on the server because there are hundreds of users who would lock themselves out every week. At this time the variable is not set University wide.
- Why changes will not be made? This will probably change in the near future, but not yet, it is a larger issue than the cope of this project.

```
Negative: 7.13 EEPROM isn't password-protected.
```

- What does the Negative or Positive result mean? If the EEPROM were password protected a password would have to be entered at the console when the system was rebooted.
- Why did the vulnerability exist? The terminal server is rebooted remotely sometimes, if the EEPROM was password protected this could not be done because a password would have to be entered at the console.

- Why changes will not be made? The terminal server will continue to be used; therefore EEPROM will not be password-protected. The server is locked inside of a cabinet, inside two separate locked doors, so it is physically secure.

Negative Section 8

```
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 smtp 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 adm has a valid shell of /sbin/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.
```

- What does the Negative or Positive result mean? The above accounts should not have shells according the scoring tool. Many security books and articles also recommend this.
- Why did the vulnerability exist? A few of these accounts needed shells because they owned cron jobs.
- What changes are going to be made? After reviewing what accounts own cron jobs and which do not I found that the following accounts do not own cron jobs and will have their shells removed: smtp, listen, daemon, bin, nobody, noaccess.
- Why changes will not be made? The following accounts will not have their shells removed because they own cron jobs: adm, lp, uucp

```
Negative: 8.3 User <username removed> should have a minimum password
life of at least 7 days.
Negative: 8.3 User <username removed> should have a maximum password
life of between 1 and 91 days.
Negative: 8.3 User <username removed> 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.
```

- What does the Negative or Positive result mean? These results have to do with passwords, their life span, and the warning that should go out saying they need to be changed.
- Why did the vulnerability exist? This University on the whole does not have password life span in its account policy.
- What changes are going to be made? To require all of the thousands of users on our campus to start changing their passwords on set intervals is bigger than the scope of this project. Therefore no changes will be made until the University wide policy is changed.

```
Negative: 8.6 Directory /usr/openwin/bin is in root's PATH and is
group-writable.
```

- What does the Negative or Positive result mean? This is the where all of the files related to OpenWin, the Sun X server, are stored.
- Why did the vulnerability exist? The server is never logged into as root therefore this hasn't really been an issue that this directory is in root's PATH. The directory /usr/openwin/bin was mistakenly left in root's path as I was not aware that it was a problem before this scan.
- What changes are going to be made? The directory will be changed to not group-writable and it will be removed from root's PATH.

```
Negative: 8.7 User <username1 removed> has a world-executable homedir!
Negative: 8.7 User <username1 removed> has a world-readable homedir!
Negative: 8.7 User <username2 removed> has a world-executable homedir!
Negative: 8.7 User <username2 removed> has a world-readable homedir!
Negative: 8.7 User <username3 removed> has a world-executable homedir!
Negative: 8.7 User <username3 removed> has a world-readable homedir!
Negative: 8.7 User <username3 removed> has a world-executable homedir!
Negative: 8.7 User <username4 removed> has a world-readable homedir!
Negative: 8.7 User <username5 removed> has a world-executable homedir!
Negative: 8.7 User <username5 removed> has a world-readable homedir!
Negative: 8.7 User <username6 removed> has a world-executable homedir!
Negative: 8.7 User <username6 removed> has a world-readable homedir!
```

- What does the Negative or Positive result mean? User home directories should not be world readable because that means any other user on the system can at least list all of the files in their home directories.
- Why did the vulnerability exist? The umask for home directories was 022 until about 2 years ago therefore there are a number of home directories that are world-read and executable.
- Why changes will not be made? Nothing at this time, however user's who have world readable home directories have been instructed on how to fix

the permissions and the umask for files is 066. There is also a web tool at will be installed for users not familiar with the command line.

```
Negative: 8.8 User <username1 removed> has world/group-writable dot-
files (.*) in his/her home directory.
Negative: 8.8 User <username2 removed> has world/group-writable dot-
files (.*) in his/her home directory.
Negative: 8.8 User <username3 removed> has world/group-writable dot-
files (.*) in his/her home directory.
```

- What does the Negative or Positive result mean? Users should never have world/group-writable dot files; this is a widely known security recommendation.
- Why did the vulnerability exist? Users can and do create their own files and all sorts of permissions. In the past file permissions were not enforced in user's home directories. Also certain programs set very permissive permissions sometimes without users knowing it.
- What changes are going to be made? The very few files that were world-writable will be changed. The following command was used to change the user's world writeable dot files (Where list_of_user_dirs.txt was the list of user directories where there were dot files that were world writeable.):
    - for i in `cat list_of_user_dirs.txt`
    - do
    - cd $i
    - chmod 600 `.[!.]*`
    - done
- Why changes will not be made? At this time most of the file permissions will not be fixed because they appear mostly to be group-writable files not world-writable, which does not make this a critical problem. The users with group-writable files will be notified that they need to change their file permissions.

```
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.
```

- What does the Negative or Positive result mean? This has to do with Sun's FTP program and permissions on the files created when someone moves files onto the server via FTP.
- Why did the vulnerability exist? We don't use Sun's FTP, we use PureFTP

as explained in Section 7.3. The senior system administrator feels that Sun's FTP program is not patched as frequently as PureFTP and therefore prefers the PureFTP program.

- What changes are going to be made? The umask will be tightened even though we don't use Sun's FTP program.

```
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.
```

- What does the Negative or Positive result mean? The default permissions created by an umask of 022 would be world-read and execute.
- Why did the vulnerability exist? It was not changed from the default in /etc/profile.
- Why changes will not be made? I cannot change this at this time because it affects a large amount of users. However it is going to be looked into in the future. In the future, after discussing it will the larger University campuses the default might be changed but that it outside of the scope and time-line of this project

```
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.
```

- What does the Negative or Positive result mean? This is the configuration file for the C Shell. The umask should be much more restrictive.
- Why did the vulnerability exist? This was a default login configuration. It should never be this permissive. It was mistaken left so permissive.
- What changes are going to be made? The permissions will be tightened to umask 022.

```
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.
```

- What does the Negative or Positive result mean? If the mesg command was give a 'n' in the configuration files then users could not use the talk or write commands to print messages to other users screens.

- Why did the vulnerability exist? The talk and write programs have been used on the server for many years, the CISscan considers them vulnerabilities.
- Why changes will not be made? Nothing at this time, however this issue will be brought up as a larger security policy change in the future. While I can see why it is more secure to disable these programs, no changes will be made at this time because talk and write are still used on the server.

Negative Section Final 6

These are Negative 6 items that showed up at the end of the log.

```
Negative: 6.7 Non-standard world-writable file: /etc/minor_perm
Negative: 6.7 Non-standard world-writable file: /etc/driver_classes
Negative: 6.7 Non-standard world-writable file: /etc/name_to_major
Negative: 6.7 Non-standard world-writable file:
/usr/kernel/drv/sparcv9/syncsort_sa.conf
Negative: 6.7 Non-standard world-writable file: /etc/driver_aliases
Negative: 6.7 Non-standard world-writable file:
/usr/kernel/drv/syncsort_sa.conf
```

- What does the Negative or Positive result mean? The permissions are very insecure on these files. At the current setting, if a user connected to the server via SSH and knew that these files existed they could potentially write to them.
- Why did the vulnerability exist? The permissions were likely set so permissive by a software install or patch. This will be further researched by the server system administrators.
- What changes are going to be made? The permissions will be change to only owner read and executable.

```
Negative: 6.8 Non-standard SGID program /etc/mlock
```

- What does the Negative or Positive result mean? This is a University customized program used by all of the campuses.
- Why did the vulnerability exist? This customization has to do with the email system. It has been this way for many years.
- Why changes will not be made? This program is still being used on the server; therefore the permissions will have to stay the default for the program to run. The issue of whether this program needs the SGID will be brought up with the original program authors, however that is beyond the time-line of this project.

Changes not made

There were a few things that the scan found that will not be changed on the server. For example the following 3rd party software is installed and used; OpenBSD's finger and rpcbind port and PureFTP. The reasons why the senior system administrator chose to use these programs over Sun's default programs are because of the historical vulnerabilities in these particular pieces of software. A history of many of the vulnerabilities can be found by reviewing the bugtraq mailing list archives (http://www.securityfocus.com/archive/1).

One example is the historical vulnerability in finger posted to bugtraq in Oct 22, 2001, bugtraq ID # 3457. In the discussion section of the Security Focus web page on the bugtraq ID # 3457 it defines the problem as, "The Solaris version of fingerd may potentially disclose a list of all accounts on the host to remote attackers who make a specially crafted finger request." This is just one of the reasons that the senior administrator feels more comfortable using the latest CVS tree OpenBSD ports of the listed software.

Another reason a few changes suggested by the CISscan, and the Solaris Benchmark, were not made is because of the historical way the university campuses are intertwined and how they have been running certain programs in the past. For example the login attempt "RETRIES" variable is not set because university wide there is no policy on locking people out after a certain number of attempts. To change this variable right now would be very difficult because the larger campus management must discuss any change that would affect thousands of users. There are at least 3 other issues like this that I found. I will take my results to the larger campus system administrators for a discussion on future policies and changes.

Changes Made

After each group of results were studied and defined in the context of our server installation one of two questions were posed depending on if changes were deemed necessary. The questions were either, ‘‘What changes are going to be made?’’ or ‘‘Why changes will not be made?’’ If the question was ‘‘What changes are going to be made?’’ then the answer to the question was the actual change I made to increase the security on the server.

Here is a brief summary of the changes that were made. The extended explanations of what was changed are under each group of results in the last section.

Two services were wrapped by tcp_wrappers, krbinfo and mackrbinfo and one, finger, was wrapper by libwrap. The rarpd and rpc.bootparamd programs were disabled. Eight services were disabled at boot time; llc2, uucp, bdconfig, ncalogd, ncad, autoinstaller, nfs.server, and ldap.client.

The files /var/adm/loginlog and /etc/ftpusers were created. The group ownership of /etc/passwd and shadow were changed to ‘sys’. The permissions were tightened on the files in /var/spool/cron/crontabs/*. The following accounts had their shells changed to /bin/false; smtp, listen, daemon, bin, nobody, noaccess.

There were a few user home directories that were actually world-read/writable/executable so I changed them to world-executable only.

The umask for /etc/default/ftpd and /etc/.login were tightened to umask 066 and 022. The permissions were fixed on all of the world-writable files that the scan found except for the world-writable dot files in the users home directories, those will have to wait until I get the go head to scan everyone's home directories and change them.

After making the changes listed in the last section, and after each group of results in the section before, I ran the CISscan again to see if our score had improved.

Negative Results after the Changes Were Made

```
Negative: 1.1 System appears not to have been patched within the last
month.
Negative: 1.2 udp-protocol service comsat in inetd.conf is not wrapped.
Negative: 1.2 tcp-protocol service finger in inetd.conf is not wrapped.
Negative: 1.2 udp-protocol service talk in inetd.conf is not wrapped.
Negative: 2.1 inetd listens on port comsat -- this port's line should
be commented out or deleted in inetd.conf.
Negative: 2.1 inetd listens on port talk -- this port's line should be
commented out or deleted in inetd.conf.
Negative: 2.1 inetd listens on port finger -- this port's line should
be commented out or deleted in inetd.conf.
Negative: 2.2 telnet not deactivated.
Negative: 2.4 rlogin (rlogin) should be deactivated.
Negative: 3.1 Serial login prompt not disabled.
Negative: 3.3 inetd is still active.
Negative: 3.5 Mail daemon is on and collecting mail from the network.
Negative: 3.7 PRESERVE not deactivated.
Negative: 3.10 NFS script nfs.client not deactivated.
Negative: 3.11 rpc rc-script (rpcbind) not deactivated.
Negative: 3.18 Web server not deactivated.
Negative: 4.1 Coredumps aren't deactivated.
Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be
deactivated
Negative: 4.4 ip6_ignore_redirect isn't set to 1.
Negative: 4.4 ARP timer (ip_ire_arp_interval) should be at most 60,000
Negative: 4.5 ip6_strict_dst_multihoming isn't activated.
Negative: 5.1 syslog does not permanently capture auth messages.
Negative: 5.2 syslog does not permanently capture daemon.debug
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.
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.
Negative: 6.1 /usr is not mounted read-only.
Negative: 6.9 Fix-modes has not been run here.
Negative: 7.5 /etc/dt/config/Xaccess needs a global deny !* CHOOSER
BROADCAST line.
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 Non-root accounts are in cron.allow.
```

```
Negative: 7.8 Couldn't open at.allow
Negative: 7.10 EEPROM banner isn't on.
Negative: 7.10 /etc/issue doesn't have a authorized-use banner.
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.
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 adm has a valid shell of /sbin/sh.
Negative: 8.1 lp has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.3 User <username0 removed> should have a minimum password
life of at least 7 days.
Negative: 8.3 User <username0 removed> should have a maximum password
life of between 1 and 91 days.
Negative: 8.3 User <username0 removed> should have a password
expiration warning of at least 7 days.
Negative: 8.3 User <username1 removed> should have a minimum password
life of at least 7 days.
Negative: 8.3 User <username1 removed> should have a maximum password
life of between 1 and 91 days.
.
. <100+ similar lines cut for the sake of saving paper>
.
Negative: 8.3 /etc/default/passwd doesn't have a value for MAXWEEKS.
Negative: 8.3 /etc/default/passwd doesn't have a value for MINWEEKS.
Negative: 8.3 /etc/default/passwd doesn't have a value for WARNWEEKS.
Negative: 8.7 User <username1 removed> has a world-executable homedir!
Negative: 8.7 User <username1 removed> has a world-readable homedir!
Negative: 8.7 User <username2 removed> has a world-executable homedir!
Negative: 8.7 User <username2 removed> has a world-readable homedir!
Negative: 8.7 User <username3 removed> has a world-executable homedir!
Negative: 8.7 User <username3 removed> has a world-readable homedir!
Negative: 8.7 User <username3 removed> has a world-executable homedir!
Negative: 8.7 User <username4 removed> has a world-readable homedir!
Negative: 8.7 User <username5 removed> has a world-executable homedir!
Negative: 8.7 User <username5 removed> has a world-readable homedir!
Negative: 8.7 User <username6 removed> has a world-executable homedir!
Negative: 8.7 User <username6 removed> has a world-readable homedir!
.
. <13,000+ lines cut for the sake of saving paper>
.
Negative: 8.8 User <username1 removed> has world/group-writable dot-
files (.*) in his/her home directory.
Negative: 8.8 User <username2 removed> has world/group-writable dot-
files (.*) in his/her home directory.
Negative: 8.8 User <username3 removed> has world/group-writable dot-
files (.*) in his/her home directory.
.
. <100+ similar lines cut for the sake of saving paper>
```

```
.
Negative: 8.10 Current umask setting in file /etc/default/ftpd is 066 -
- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/default/ftpd is 066 -
- 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 022 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/.login is 022 -- 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.
Negative: 6.8 Non-standard SGID program /etc/mlock
```

Positive Results after the Changes

```
Positive: 1.3 System is running sshd and it's configured well.
Positive: 2.3 ftp is 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.
Positive: 2.10 kerberos network daemons are deactivated.
Positive: 3.2 Found a good daemon umask of 022 in /etc/default/init.
Positive: 3.4 System is not running syslogd, thus syslogd is not
listening to the network.
Positive: 3.6 in.rarpd and rpc.bootparamd have been disabled..
Positive: 3.9 NFS Server script nfs.server is deactivated.
Positive: 3.14 LDAP cache manager is deactivated.
Positive: 3.15 The printer init scripts are deactivated.
Positive: 3.16 volume manager is deactivated.
Positive: 3.17 Graphical login scripts are all deactivated.
Positive: 3.19 SNMP daemon is deactivated.
Positive: 4.2 Stack is set non-executable and logs violations.
Positive: 4.3 NFS clients use privileged ports.
Positive: 4.6 TCP sequence numbers strong enough.
Positive: 5.4 cron usage is being logged.
Positive: 5.7 All logfile permissions and owners match benchmark
recommendations.
Positive: 6.2 logging option is set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 /etc/dfs/dfstab doesn't have any non-fully qualified
pathname share commands.
Positive: 6.5 password and group files have right permissions and
owners.
Positive: 6.6 all temporary directories have sticky bits set.
Positive: 7.1 pam.conf appears to have rhost auth deactivated.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either
don't exist or are links to /dev/null.
Positive: 7.3 All users necessary are present in /etc/ftpusers
Positive: 7.4 /etc/shells exists and has good permissions.
Positive: 7.9 crontabs all have good ownerships and modes
Positive: 7.11 Root is only allowed to login on console
Positive: 8.2 All users have passwords
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.6 root's PATH is clean of group/world writable directories
or the current-directory link.
Positive: 8.9 No user has a .netrc file.
Positive: 6.7 No non-standard world-writable files.
```

Impact

After making all of the changes and running the CISscan again the score was 5.21 out of 10. I had hoped it would have increased more, however I knew there were a lot of things on the server that I would not be able to change or that would take a lot longer and would mean changes to the University security policies.

Everyone working on the server agreed that this was an excellent eye opening experience. After researching every single line of the results log, both positive and negative, I learned quite a bit. I would encourage any system administrator to run it.

There was very little impact from actually running the scan. It did not slow down the server very noticeable and it did not cause any harm. It is a very noninvasive scan, but at the same time I can't believe how thorough.

The impact from making the changes seems to be only positive. No services stopped, no one complained that, for example, their cron job file permissions changed. The users who had their home directory permissions changed did not notice, however I will email them and let them know and ask them to please not set them so permissive again.

From this point I am going to scan the other servers we control. After that I believe we need to have a good, detailed security policy for our UNIX servers put in place. A lot of the problems we had, for example the 1000s of user home directories that have world-readable permissions, can be solved by setting up monitoring and a policy of tighter permissions.

This was a bit of a backward way of coming to the conclusion that our security policies need to be better. I am aware of that, however sometimes system administrators have to have the evidence of a problem before they can suggest changes as major as I did.

References

Nemeth, Snyder, Seebass, and Hein. UNIX System Administration Handbook. Upper Saddle River: Prentice Hall, 2001.

Garfinkel and Spafford. Practical UNIX & Internet Security. Cambridge: O'Reilly, 1996.

Peek, O'Reilly, and Loukides. UNIX Power Tools. Cambridge:O'Reilly, 1997.

Cole, Fossen, Northcuttm, and Pomeranz. SANS Security Essentials with CISSP CBK Volume One and Two. USA: SANS Press, 2003.

"CIS Solaris Benchmark." 1.2.0. 2003. URL: http://www.cisecurity.org/bench_solaris.html (June 2004)

"System Administration Guide." Sun Product Documentation. 1. 2000. URL: http://docs.sun.com/db/doc/805-7228 (May 2004)

"System Administration Guide." Sun Product Documentation. 2. 2000. URL: http://docs.sun.com/db/doc/805-7229 (June 2004)

"System Administration Guide." Sun Product Documentation. 3. 2000. URL: http://docs.sun.com/db/doc/806-0916 (June 2004)

"The Solaris Network Cache and Accelerator, A Technical White Paper." 2002. URL: http://wwws.sun.com/software/whitepapers/solaris9/networkcache.pdf (May 2004)

"Manual Reference Pages - IP6 (4)." FreeBSD Man Pages. March 13, 2000. URL: http://www.gsp.com/cgi-bin/man.cgi?section=4&topic=ip6 (June 2004)

"Solaris Operating Environment Network Settings for Security." Prentice Hall Professional Technical Reference. Sept 12, 2003 URL: http://www.phptr.com/articles/article.asp?p=101138&seqNum=4 (May 2004)

"Solaris finger disclosure." Finger abuses. 2001. URL: http://cert.uni-stuttgart.de/archive/bugtraq/2002/10/msg00020.html (June 2004)

"Bugtraq ID 3457." Design Error. Oct 2001. URL: http://www.securityfocus.com/bid/3457/info/ (June 2004)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor