Global Information Assurance Certification Paper

Solaris 9 Secure File Transfer Server Audit

Julie L Baumler
April 2nd, 2003

GCUX Practical Assignment Version 1.9 Option 2

Executive Summary

I was hired by the City of GIAC[1] to perform a security audit of its secure FTP server "flipper" as well as to determine that several of the file transfers the server is used for were ready for their upcoming move to production status. This document details the audit methodology, findings and recommendations.

The audit was carried out via interviews with City of GIAC staff, using system and third-party audit tools, and by physical inspection. The city technical staff had already made numerous effective changes in the system to secure it beyond its default vendor supplied state. There are still improvements to be made, but the city's technical staff has done the majority of the work necessary to secure the system.

One of the key needed improvements is best dealt with by management. The technical staff does not have a security policy or objectives to use in determining procedures and installing and maintaining systems. Management, not technical staff, should be determining the acceptable level of security risk, and security policies are the best means for management to do so[2]. Without a security policy, it is difficult to determine whether effort to make a system more secure is a necessary measure or a waste of organizational resources. Joel Weise and Charles R. Martin's article "Developing a Security Policy" is a good management resource on security policy development.

The remaining key issues for this server involve patching, continued server minimization, improving user logging and access control, further securing ftp user access, installing and upgrading security software, synchronizing system time, improving monitoring of user actions and system changes, and resolving differences between policy and reality for sftp connections.

Many of the recommended changes are needed because this system was installed as a secure system but is not maintained to remain a secure system. Over time, new security vulnerabilities are found and exploited, changes are made in systems that introduce new security holes, and possibly, systems are compromised. As Sun Microsystem's Alex Noordergraff puts it:

> Many organizations make the mistake of addressing security only during installation, then never revisit it. Maintaining security is an ongoing process and is something that must be reviewed and revisited periodically.[3]

The City of GIAC, at least on this server, is one of those organizations. Management leadership and attention to details like allocating money and staff time of ongoing security needs of systems and projects is necessary to bring on the paradigm shift to viewing security as a process.

Contents

Description of System and Audit Methodology

Role of the server

The audited system, flipper, is a “Secure FTP” server used by the city to transfer data between the city and it's business partners. These business partners are currently the county and state where the City of GIAC is located and a few providers of outsourced human resources services. As a government entity, much of the data the City of GIAC deals with is public record. Some of the data the City of GIAC handles is either not public record or protected by law. For instance, some payroll data sent through this server may contain non-public record personal information about employees and their dependents. There is currently some discussion of using this server to transfer information to and from some of the city's health clinics, although the exact nature of the data to be transferred has not yet been determined, it is likely that some of this data would be considered Electronic Protected Health Information under HIPAA. This server provides both ftp (using the vendor provided version of wu-ftp) and sftp. The term sftp is used for a number of different ftp-like protocols that do not use clear text passwords. In the case of flipper, the sftp used is part of the secure shell suite and allows users who are unfamiliar with the the secure shell suite to use ftp commands over an ssh encrypted channel.

This system is a Sun Fire 280R, with one 750mh UltraSparc-III processor and 512 mb of memory. This is essentially a stock configuration for a 280R with the exception that the system has a GFXP graphics card installed and a single power supply/fan module. The system console is provided via an Avocent Autoview 424 graphical console sharing device and the gfxp graphics card is used for this purpose. This shared console device does not allow console access from any other locations.

As is standard for 280R's, this system has a 10/100 on board network interface, which is used to connect the server to the network. The system has 2 serial ports, an RSC card[4], and a parallel port; none of these are in use. The system is running the Solaris 9 Operating Environment[5] with the Solaris Security Toolkit (SST) version 0.3.7 installed. SST is a set of tools that produces a server that is more secure than the default installation, but is still Sun supported. Physically, the system is located in a controlled environment in the City of GIAC's computer room. From a network viewpoint, this system lives on the city's controlled access extranet. Firewalls between the extranet and the different connected networks block access to this system on a per service and per host basis. All hosts within the extranet are held to a higher security standard than other city hosts, a policy which is proactively enforced via vulnerability scanning and other measures. All city networks also host an intrusion detection system.

Like all public or semi-public FTP servers, a specific security concern is that if one or

more ftp accounts with access to the larger internet are discovered, the system can be used for illegal file distribution. In turn, this file distribution could cause enough network traffic to cause a denial of service to other hosts or services on this segment of the city's network. Another specific concern is that if an attacker were to gain access to a host on the city's extranet network, they would then be in a position to bypass the firewall in attacking any other host on the extranet, this might allow an attacker to disguise an attack against the internal networks as regular traffic, or otherwise gain a foothold in the internal networks. This system is providing semi-public ftp and ssh services, both ftp and ssh services are listed as among the top ten Unix vulnerabilities on the SANS/FBI list, The Twenty Most Critical Internet Security Vulnerabilities.[6] This is a list of the most commonly exploited services for the Unix and Windows operating systems. FTP is a particular problem because it allows plain text login, so usernames and passwords can be sniffed on the networks between the end user and the server. Since the ftp and sftp accounts on this server are for organizational, rather than personal file transfers, passwords are more likely to be shared or written down.

Audit Methodology

In any system, balances need to be made between security and usability or manageability[7] and between exposure to risk and the cost of mitigating that risk[8]. Policy is usually the medium through which decisions about the management of this balance is communicated, therefore the first step in undertaking this audit was to determine what policies, both formal and informal, existed regarding this system and from whom those policies came. The informal policies were gathered thorough a series of informal conversations with the technical staff of the City of GIAC. In the areas where policies existed, compliance to policy was checked as part of the audit. In addition, following some of the organizational policies determined what tools and methods were used in the remainder of the audit.

The next step in the audit was an inspection of the system, it's state and environment. Where possible, software tools were used to do the initial inspection and analysis, followed by direct inspection and research where the tool output seemed lacking or was vague. The tools used were Nmap[9], to scan for open network ports; John the Ripper[10], to check password security; CISscan[11], a security benchmarking tool; Tara[12], a host based security scanner; and patchdiag[13], a tool to determine needed patches for the Solaris Operating Environment. A number of Solaris Operating Environment commands were used to gather further information about the system's state and environment, such as pkginfo, which lists installed software; prtdiag, which gives basic information about system hardware and it's health; prtconf, for more detailed information about installed hardware; and df, for a list of mounted file systems and how full they are. These tools and their output are described in depth in the next section. A network based vulnerability scanning tool is commonly used when doing security audits, the City of GIAC's network staff regularly runs a commercial tool that does this, I was asked not to repeat their work in this area. I did not receive a copy of this scan output as it included information about other servers which I was not authorized to see. The network staff reported to me that there were no high priority issues found, although there may be

some issues that need investigation as the tool could not determine whether or not it applied to the system.
In addition to checking vulnerabilities and misconfigurations highlighted by these tools to determine system applicability and methods of removing unneeded risks in line with the work already done on this system, I checked this system against Sun's list of known vulnerabilities in the Solaris 9 Operating Environment, as listed in the Sun Alerts collection. Most of the manual checking of this system was to rule out indicators of vulnerabilities that did not actually exist, not to double check for risks that the tools had already ruled out. This leaves a risk that if a tool is misconfigured or poorly written, a vulnerability could be over looked. This risk is mitigated by the fact that multiple similar tools were used.

Detailed Analysis

Policy

A number of formal and informal policies exist for this system. File transfer service users are given the following policy and information statement:

> Any data that can or should not be made public is expected to be encrypted prior to being transferred to this system. The FTP Server will provide SSL transfer for all data transfers that require it. This server will be a minimally configured UNIX system whose only objective in life is to reliably transfer data to and from City of GIAC departments and business organizations. The server and its data will not be backed up, in case of a failure or compromise, the server will be rebuilt. Access to the system can be controlled at the firewalls as necessary.[14]

In general, these policies are being met. The server is minimally configured, but could be further minimized. Solaris software is installed in packages of related files, Appendix A contains a list of installed packages, packages that should be considered for removal are highlighted. No SSL service is being made available, ssh's sftp is being used instead; research shows this to be a case of documentation not being updated to match a change in policy. So far, there has not been a failure or known compromise that has required rebuilding the system, but there is a jumpstart server on another network configured to rebuild this server in case of need. This policy of rebuilding rather than recovering could be bolstered by keeping a copy of some of the configuration files that are changed when new transfers or accounts are added in a secure off-host location.

There are two other formal policies specific to this server. The first, from the login banner, "[t]his server is for authorized users from authorized systems for authorized uses" is being met but perhaps not in the manner intended. This access control is being carried out by firewalls and the choice of shells assigned to users (FTP only users have a shell of /bin/false which restricts them from logging in via the system console or ssh.) The firewall administrator listed the systems allowed access to this system, the firewall configuration matches the documentation regarding required file transfers, with the addition of ssh from a specific internal management host to allow administrative access;

however any authorized user can access this system from any authorized system. In a similar manner, authorized uses are only partially limited by system and by user. A more secure strategy would be to limit specific users to accessing specific services from specific systems. The other policy is that all new authorized systems will be approved by a specific upper-level IT manager, so that new risks can be analyzed from a high level. This policy is being met. I'd like to note that, this policy is an example of excellent risk management.

The city has a number of policies regarding what software is installed. The recommendations made in this audit take these policies into account and the tools (and tool versions) used in the audit were chosen to meet these policies. Whenever possible, the city uses vendor supported software, when this is not available or prudent, system administrators may use unsupported packages from several specific approved sources at their discretion (mostly Sun Microsystems sources and www.sunfreeware.com). Whenever possible, package format software should be used. Perl and shell scripts can be used at the system administrators' discretion. Management approval is required to use other unsupported software.

In the process of working on this audit, two informal policies came to light. Although it is not formally documented, upper management has stated that logging filesystems should be used wherever possible. The CISscan report shows that this system is not doing filesystem logging. A second informal policy is a consensus among the system administrators of the city that it is more secure to put a lot of effort into picking a strong password, keeping it protected, and not changing it unless there is reason to believe that it has somehow been compromised than to require changing passwords regularly, which they feel leads to picking weaker passwords or writing passwords down. Current consensus in the security community seems to be leaning toward changing passwords on a regular basis, but this has been an area of strong debate for many years. It is my personal opinion that both arguments have merit, but whichever policy is used, it should be enforced. Unfortunately, as will be described in the section on configuration vulnerabilities below, the current state for this system is that several passwords are neither strong nor well protected; neither are there any mechanisms in place to enforce this policy.

Operating System Vulnerabilities and Configuration

Software tools were very useful in determining the system's configuration as well as needed improvements. In general, the tools showed that many operating system minimization and configuration measures for security had already been taken. The Solaris Security Toolkit had been installed as a part of the initial system configuration and a number of additional security measures had been taken. A number of items appear to have been missed in the original configuration and new risks and vulnerabilities have been discovered in the installed software since installation.

Center for Internet Security Benchmark

The most useful tool in looking at this system was the Center for Internet Security's Solaris benchmark scoring tool, cis-scan[15]. The benchmark tool is available from the

CIS website in Solaris package format in a package called CISscan, along with a document explaining both the output of the tool and steps necessary to meet the benchmark in each area. CIS refers to this tool as a level-one benchmark, with "recommendation[s] to secure systems to the minimum level of prudent due care, as defined through the consensus process, and are highly unlikely to affect the performance of the operating system or applications running on it."[16] The package was installed on the system using "pkgadd -d . CISscan", the program was run as the root user, using the command "/opt/CIS/cis-scan", and then the package was removed using the command "pkgrm CISscan."

This system's overall score on the benchmark is 6.32 out of 10. It is important to remember that a perfect score of 10 is not necessarily achievable or desirable, what is important is that any negatives pointed out by the scan should be necessary to meet system requirements, rather than items that have been overlooked. The full output of the CIS benchmarking tool is in Appendix B. Additional information about each item and suggested remediations are provided by The Center for Internet Security in their document "Solaris Benchmark v1.1.0," which is included with the benchmarking software or available independently from the Center for Internet Security's web site at http://www.CISecurity.org.

The following are key diagnostics annotated with additional information and recommendations:

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

This system has not been patched since OS installation (at which time there were no patches available for Solaris 9.) Patches close known security vulnerabilities and repair software defects that could cause system failures. A list of needed patches is in appendix D.

Negative: 2.2 telnet not deactivated.

The secure shell (ssh) or the system console are used for administrative connections to this system, therefore telnet should be deactivated. Telnet uses clear text authentication, which allows passwords to be gathered while traversing the network.

Negative: 2.3 FTP not deactivated.

As an FTP server, FTP is a required service for this server; this can be ignored for this server.

Negative: 3.1 cachefs.daemon not deactivated.
Negative: 3.1 cacheos.finish not deactivated.

These messages refer to the cachefs, which allows system administrators to setup and run cacheing filesystems. Neither of these is required or in use on this system, however the startup scripts (/etc/rc2.d/S73cachefs.daemon and /etc/rc2.d/S93cacheos.finish) are in place and run each time the system starts. If the software were installed these services would start.

Positive: 3.7 LDAP directory server is deactivated.
Negative: 3.8 ldap cache manager not deactivated.

LDAP is not installed on this system, however this message is being triggered because /etc/rc2.d/S71ldap.client, the startup script for the ldap cache manager is installed on the system and would start ldap if the client software were installed.

Negative: 3.16 System is running syslogd without the -t switch, accepting remote logging.

Since this host is not a syslog server, the syslog daemon should not be listening for connections from remote servers. This could be used to forge system messages or fill the /var filesystem, possibly resulting in a denial of service.

Negative: 3.17 inetd is still active.

Inetd is being used to run the FTP server, therefore, it is necessary for proper function on this server.

Negative: 3.18 Serial login prompt not disabled.

The serial ports on this system are setup to allow logins via attached modems and terminals; since this is not an intended method of connecting to this system, this should be turned off.

Negative: 4.1 Coredumps aren't deactivated.

Coredumps can contain sensitive data and fill filesystems causing other problems. Since this is not a development system, coredumps are unlikely to be useful or desirable.

Negative: 4.4 tcp_ip_abort_cinterval should be at most 60,000 to avoid TCP flood problems.

This network parameter setting attempts to prevent TCP flooding problems.

Negative: 4.5 ip6_strict_dst_multihoming isn't activated.
Negative: 4.5 ip6_ignore_redirect isn't set to 1.

These messages can be ignored. This system uses the Sun Security Toolkit's /etc/init.d/nddconfig script and will set these parameters if IPv6 is enabled on the system. These messages are showing up because IPv6 is not currently configured.

Negative: 5.2 ftp is running out of inetd on port ftp, but does not do "-d" debug logging.

Although session logging has been turned on for the FTP daemon, debug level logging has not.

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

Logging failed logins allows you to catch attempted password guessing attacks, it also can be used to provide better proactive customer service.

Negative: 5.5 Couldn't read the /etc/rc2.d/S21perf file to check for system acctg.
Negative: 5.5 Couldn't open /var/spool/cron/crontabs/sys to look for sa1 and sa2 -- no system accounting.

System accounting provides an additional way to watch what is going on on a system, monitor normal behavior, and gather information in the event of a penetration. It has long been considered a key first step in maintaining Unix security.

Negative: 5.6 BSM should at least be auditing failed "file create" (fc) events on flags line.
Negative: 5.6 BSM should at least be auditing failed "file delete" (fd) events on flags line.
Negative: 5.6 BSM should at least be auditing failed "file attribute modify" (fm) events on flags line.
Negative: 5.6 BSM should at least be auditing failed "file write" (fw) events on flags line.
Negative: 5.6 BSM should at least be auditing all "administrative" (ad) events on naflags line.
Negative: 5.6 BSM should at least be auditing all "network" (nt) events on naflags line.

These comments are referring to kernel level auditing, called BSM in Solaris. Kernel level auditing logs commands and system calls, it provides a lot more information than system accounting, making it possible to recreate what was done on a system in many cases.

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

The /usr file system is intended to hold system binaries (and contains most or all of the critical system binaries). These files should only change when patches or new software is installed; these binaries can be protected by mounting this filesystem read-only, to avoid unauthorized changes. If system files need to be changed, a privileged user can remount the filesystem read-write without impacting service.

Negative: 6.1 /transfer is not mounted nosuid.
Negative: 6.1 /transfer2 is not mounted nosuid.

These two filesystems are user home directories. Setuid executables are programs that take on the owner's privileges when run. These can be useful to allow specific access to privileged resources to non-privileged users, but there is no reason why users on this system need their own personal setuid executables (and they can be used for privilege escalation exploits.)

Negative: 6.2 logging option isn't set on root file system

Filesystem logging is a City of GIAC standard for all Solaris 8 and later filesystems. From a security standpoint, logging on the root file system prevents an attacker with physical access from corrupting the root file system, causing the system to boot into single user mode.

Negative: 7.6 Couldn't open /etc/dt/config/Xservers to check that Xserver TCP listening had been disabled.

Xserver software is not installed. It might be worth creating this and other X configuration files to ensure that even if X software is installed, it will run securely.

The X window system uses /usr/dt for system supplied configuration files and /etc/dt for administrator supplied configuration files. The files in /etc/dt are used preferentially, this allows an administrator to make configuration changes that are not overwritten when software is added or patched. This allows making the configuration changes necessary for more secure X server use, in the event this software is installed in the future.

Negative: 7.11 /etc/default/login allows non-console root logins

Root should not be allowed to login other than via the console. Among other things, this prevents remote password guessing on a known, privileged user's account.

Negative: 7.13 EEPROM isn't password-protected.

The Center for Internet Security recommends password protecting the EEPROM on Solaris SPARC systems to prevent unauthorized users from doing anything except a normal multi-user boot. Due to the difficulty of recovering the system in an emergency if this password is unknown, I recommend this only for systems that are not in a secure, access controlled environment, since this system is in such an environment, I would not recommend implementing such a measure on this system.

The following messages appeared for most of the system administrator and FTP user logins:

Negative: 8.2 User <login> should have a minimum password life of at least 7 days.
Negative: 8.2 User <login> should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User <login> should have a password expiration warning of at least 7 days.

This issue is addressed in detail in the section on configuration vulnerabilities.

Negative: 8.7 User user1 has a group writable homedir!

Negative: 8.7 User user1 has a world-executable homedir!
Negative: 8.7 User user1 has a world-readable homedir!
Negative: 8.7 User user2 has a group writable homedir!
Negative: 8.7 User user2 has a world-executable homedir!
Negative: 8.7 User user2 has a world-readable homedir!
Negative: 8.7 User user3 has a group writable homedir!
Negative: 8.7 User user3 has a world-executable homedir!
Negative: 8.7 User user3 has a world-readable homedir!

These logins are used for file transfer via FTP and sftp. They share a home directory for ease in sharing files. These logins share a special group and separate logins were used to allow restriction of services (FTP versus sftp) and remote hosts and for ease in logging transfers. This situation makes group read and execute permissions reasonable, world permissions should be removed so that other users cannot place files in these directories. The usual risk in having a group or world writable home directory is that many users sometime (or always) have their home directory in there path, and an attacker can install a trojan program with the same name as a system program in the home directory, allowing the attacker to gain access to the users account. In this situation, a more likely risk is that a user could be tricked into downloading a substitute data file containing false data.

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.

This makes the device file used to provide the user's session more secure. If the device file can be read or written to by an attacker, the attacker can access or amplify the information the user is viewing or inputing. There is no need to use the write or talk commands on this system, so this is security at no cost.

Negative: 9.1 tcp6-protocol service telnet in inetd.conf is not wrapped.
Negative: 9.1 tcp6-protocol service ftp in inetd.conf is not wrapped.

Although the wording of these messages makes it look like they are referring to IPv6 services, these are the FTP and telnet services for this system for both IPv6 and IPv4. TCP Wrappers makes it possible to limit access to services to authorized users only if they are coming from a system authorized for access to that service. It also allows better logging of connections to the system.

Negative: 9.2 sshd_config parameter MaxAuthTries, currently 6, should be set to no more than 3.
Negative: 9.2 sshd_config parameter MaxAuthTriesLog, currently 3, should be set to 0.

These parameters determine how many attempts a connection is allowed at authentication before the connection is closed (MaxAuthTries) and how many failures

are allowed before the attempt is logged (MaxAuthTriesLog). Setting these parameters as recommended will make username/password guessing attacks more difficult and log such attempts so that countermeasures can be taken.

Negative: 9.3 Fix-modes has not been run here.

The Fix-modes program resets file, device, and directory permissions on a Solaris system to a more secure state, reducing a number of risks; it also changes configuration files so that the package checking tools accept these changes as valid. This software needs to be run each time packages or patches are added to the system.[17]

Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/foo/aaa-output
Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/foo/aab-output
Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/foo/aac-output
Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/foo/aad-output
Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/foo/aba-output
Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/bar/abb-output
Negative: 6.7 Non-standard world-writable file: /export/home/admin1/opt/user1/foo/abc-output

These files are all test data in a system administrators account.

Negative: 6.8 Non-standard SUID program /opt/sfw/bin/sudo

Sudo, which stands for "superuser do" allows users to be assigned the ability to run specific commands or all commands as root or another defined user.[18] Sudo logs the commands and arguments each user runs via syslog. while logging the commands and arguments. It is a local standard that system administrators have full sudo access and use sudo rather than logging in as root whenever possible so that their actions are logged. This message can be ignored. See the section on Third Party Software, below, for specific information on the risks of the currently installed version of sudo.

Negative: 6.8 Non-standard SGID program /usr/SUNWale/bin/mailx

This is a false positive, in the sense that this version of the mailx program is part of the standard for Solaris 9 SUNWale package, which provides support for Asian languages. However, since this server is not using any languages other than English and we've seen several problems in the last few years due to software interactions

with locales, the SUNWale package is unnecessary, a possible risk, and should probably be removed.

TARA host based vulnerability scanner

A second host based scan, TARA[19], was also run. TARA is a set of shell scripts, it comes as a compressed tar file which was uncompressed and untared onto the system, run, and then removed. The command issued was simply "./tiger". TARA is not really designed to run on a minimized system. It uses the "strings" command, which is only installed on Solaris if you install the programming tools and the "whoami" command which is part of the BSD compatibility commands. "Strings" was copied from another Solaris system in order to run TARA, it was removed after running TARA. The "whoami" command was replaced by creating a temporary script called "whoami" that returned the expected output - "root." Much of the information reported by TARA was a repeat of that given by the CIS benchmarking tool or a benign operating system setting, but there was some useful new information. The new information, with annotations is below, the full output from TARA, including the TARA explanations is in Appendix C.

```
# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc005w] Login ID adm is disabled, but has a 'cron' file or cron
        entries.
--WARN-- [acc006w] Login ID adm's home directory (/var/adm) has group `sys'
        write access.
```

These warnings can be ignored, these are standard and appropriate settings for the Solaris Operating Environment.

```
# Performing check of /etc/default/login, /securetty, and /etc/ttytab...

--WARN-- [root001w] Remote root login allowed in /etc/default/login.

# Performing check of `cron' entries...
--WARN-- Unusual cron file `root.au' found.
```

This is a normal file created as a part of the installation of the Solaris Security Toolkit.

```
# Performing check of system file permissions...
--WARN-- [perm021w] Disk device /dev/dsk/c1t0d0s0 has read access for group sys.
```

This message was repeated for each filesystem. This appears to be a result of the standard setup for backups at this site (the backup process is run as a member of the sys group), but since this system is not backed up, this setting is unneeded on this system.

```
# Performing checks for SunOS/5...
```

--WARN-- [misc008w] NFS port checking disabled in kernel.

This system is not an NFS server, so this message can be ignored.

Checking setuid executables...
--WARN-- [fsys002w] setuid program /usr/lib/fs/ufs/ufsrestore has relative pathnames.

Relative pathnames in setuid programs can allow a user to force the program to call their own version of a library or binary, gaining escallated privileges . This should be reported to Sun as a bug.

Port Scanning with Nmap

In addition to these two host-based scans, a network-based port scan, using Nmap, was run against this system from another Solaris system on the same subnet. Following site policy, a packaged version of Nmap from Sunfreeware was used[20]. This package was installed, Nmap was run using the command "nmap -sT -sU -sR -PB -oA flipper_nmap -O -T Polite 192.168.1.5" which scans TCP, UDP, and RPC ports on flipper using the default ping options, OS determination, and "Polite" timing. The default ping options are to use TCP ACK/SYN and ICMP ping to determine whether a system is available. Polite timing is a 0.4 second wait between probes. Output is returned in "Normal" (plain text), grep-able, and XML formatted output. The text output file, flipper_nmap.nmap, is displayed here.

nmap (V. 3.00) scan initiated Thu Feb 13 05:24:37 2003 as: nmap -sT -sU -sR -PB -oA flipper_nmap -O -T Polite 192.168.6.66
Interesting ports on (192.168.6.66):
(The 3066 ports scanned but not shown below are in state: closed)
Port State Service (RPC)
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
Remote operating system guess: Solaris 9 with TCP_STRONG_ISS set to 2
Uptime 142.052 days (since Tue Sep 24 05:30:40 2002)

Nmap run completed at Thu Feb 13 05:45:51 2003 -- 1 IP address (1 host up) scanned in 1274 seconds

This shows that all ports are closed except for FTP, ssh, and telnet. Experimentation from two hosts not permitted access to this system, an internal city host and a non-city host on the internet, showed that none of these ports are accessible to non-approved hosts, due to firewall filtering.

Sun Alerts

An additional method of looking for operating system vulnerabilities was to check for

known Solaris security vulnerabilities. There are numerous collections of operating system vulnerabilities, for this audit, the Sun Alert collection was used.[21] The Sun Alert collection is a collection of documents containing key information for Sun customers. Sun issues alerts for security issues of every level. No one list or set of lists contains all vulnerabilities to an operating system, if nothing else, you must assume that there are some as yet undiscovered vulnerabilities. For Solaris systems, Sun Alerts are more inclusive than CERT or other security services' advisories, although Sun Alerts do refer to CERT Advisories where applicable. Sun offers a contract customers advanced search capabilities for its document collections, and some experimentation found that you can find all Sun Security Alerts for Solaris 9 by searching for "category:security !"Solaris 9 is not impacted"" and specifying the OS as Solaris 9 in the Sun Alert Notifications collection at sunsolve.sun.com. This resulted in thirty-seven Sun Alerts, of which ten did not apply to Solaris 9 (further tuning of the search string resulted in missing applicable alerts). Of the twenty-seven applicable alerts, the system was already not vulnerable to ten alert issues due to minimization, a further three vulnerabilities could be removed with no impact on system function by further system minimization. This is a clear object lesson in the value of server minimization. The twenty-seven alerts applying to Solaris 9 are listed below along with comments on how they impact this system. Many of these vulnerabilities can be fixed by installing a patch, in that case the patch number is listed here; a full list of required patches is in Appendix D.

1. The wall(1M) Command May be Used to Send Messages Containing a Forged User ID
   Sun Alert Notifications: 51980

   The system is vulnerable to this, however this is something that can be used as part of a social engineering attack, not a direct vulnerability. Since there are no local users on the system, there should be no impact on the security of the system.

2. Security Vulnerability in the Network Services Library, libnsl(3LIB), affecting rpcbind(1M)
   Sun Alert Notifications: 51884
   20 Mar 2003

   This system already has all rpc services turned off, so is not vulnerable.

3. Solaris FTP Server (in.ftpd(1M)) is Vulnerable to Denial of Service Attack
   Sun Alert Notifications: 50240
   14 Mar 2003

   Patch 114564-01 should be installed to remove this vulnerability. Sun also recommends using the ftpaccess file to limit hosts which may open connections to the FTP server. /etc/hosts.allow and /etc/hosts.deny can provide a similar function.

4.Security Vulnerability in the ypserv(1M) and ypxfrd(1M) Daemons
Sun Alert Notifications: 47903
14 Mar 2003

NIS services are not installed on this system. This system is not at risk for this vulnerability.

5.Security Vulnerability Involving the priocntl(2) System Call
Sun Alert Notifications: 49131
13 Mar 2003

This vulnerability allows unprivileged users to run arbitrary code (a kernel module) with root privileges.[22] Installing the latest Solaris Kernel Patch (112233-04 or later) removes this vulnerability.

6.UFS File Systems With Logging Enabled are Vulnerable to a Denial of Service (DoS) Attack
Sun Alert Notifications: 51300
11 Mar 2003

File system logging is not currently implemented on this system. However, for reasons listed elsewhere in this report, it has been recommended that logging be turned on, prior to doing so, patch 113454-03 or later should be installed, to remove this denial of service risk.

7.sendmail(1M) Parses Headers Incorrectly in Certain Corner Cases
Sun Alert Notifications: 51181
6 Mar 2003

8.Sun sendmail(1M) does not Handle Some ".forward" Constructs Correctly
Sun Alert Notifications: 50904
5 Mar 2003

Since the sendmail daemon is not running on this system, the system is not at immediate risk; however, the sendmail software is installed and there has been some discussion of using mail on this server in the future. The patch to correct this vulnerability, 113575-03 or later, should be installed.

9.Security vulnerabilities in BIND and libresolv (CERT CA-2002-31)
Sun Alert Notifications: 48818
28 Feb 2003

This system is not configured as a nameserver, so is not vulnerable to this issue. However, this software is installed and in use for domain name lookup, so it should

be patched so that the system will remain invulnerable if the software is reconfigured. Patch 11434-01 or later removes this vulnerability regardless of the BIND configuration.

10.Security Issue with kcms_server Daemon
Sun Alert Notifications: 50104
20 Feb 2003

The system is not vulnerable. The KCMS packages are not installed on this system, removal of these packages constitute the suggested fix for this issue.

11.Certain UDP RPC Packets May Cause a Denial of Service
Sun Alert Notifications: 50626
18 Feb 2003

There is no RPC software running on the system, but some of it is installed as part of the core OS, therefore patch 113319-04 or later should be installed to remove any risk from this vulnerability if the software is started.

12.Security Vulnerability in mail(1) in Solaris
Sun Alert Notifications: 50751
11 Feb 2003

This system is not a mail server, so the vulnerability does not apply in the current configuration; however, patch 114134-01 should be installed since the affected software is on the system.

13.Multiple Vulnerabilities in the Tooltalk Database Server
Sun Alert Notifications: 46022
31 Jan 2003

This software is not installed on this server; the server is not vulnerable.

14.Security Vulnerability with the at(1) Command on Solaris
Sun Alert Notifications: 50161
30 Jan 2003

This vulnerability allows any unprivileged user to remove any file on the system. Since most of the security restrictions on this system depend on configuration files, this is could allow a very effective privilege escalation attack. Patch 114135-01 or later should be installed as soon as possible.

15.Several Kerberos Applications are Vulnerable to a Denial of Service (DoS)
Sun Alert Notifications: 50142

29 Jan 2003

This software is not installed on this system.

16.Security Vulnerability with the Solaris /usr/lib/utmp_update Command
Sun Alert Notifications: 50008
16 Jan 2003

Patch 113718-01 or later needs to be installed to remove the risk of a privilege escalation attack.

17.NFS Denial of Service can be Caused by a Client Application Killing the lockd(1M) Daemon
Sun Alert Notifications: 47815
2 Jan 2003

The lockd daemon (and NFS) is not running or used on this system. It is installed, and the package containing lockd, SUNWnfscu, should be removed. See Appendix A for more information on packages to remove.

18.Security Vulnerability in the Network Services Library, libnsl(3LIB)
Sun Alert Notifications: 46122
24 Dec 2002

None of the known vulnerable applications are installed on this system; however, the vulnerable library is installed on this system, and should be repaired with patches 113319-01 and 112233-02 or later.

19.On Solaris an Unprivileged User may Cause a System Panic (Denial of Service)
Sun Alert Notifications: 48267
24 Dec 2002

The system is vulnerable to this issue. Patch 112233-02 or later is needed to remove the vulnerability.

20.X Font Server Can Allow Denial of Service
Sun Alert Notifications: 48879
20 Dec 2002

The vulnerable software is not installed.

21.Buffer Overflow in the ToolTalk Library
Sun Alert Notifications: 46366

7 Oct 2002

The vulnerable software is not installed.

22.Secure Shell ("ssh") Integer Overflow can Cause a Remote Security Exploit in Solaris 9
Sun Alert Notifications: 45525
9 Sep 2002

The Secure Shell is configured in a non-vulnerable manner. Patch 113273-01 or later should be installed so that this system will remain non-vulnerable regardless of configuration.

23.Buffer Overflow in DNS Resolver Library (CA-2002-19)
Sun Alert Notifications: 46042
26 Aug 2002

The system is vulnerable to this issue, which could allow a remote attacker to run arbitrary commands in response to a DNS query. Installing patch 112970-02 or later will remove the vulnerability.

24.Security Vulnerability in the Way Apache Web Servers Handle Data Encoded in Chunks
Sun Alert Notifications: 45961
13 Aug 2002

The vulnerable software is not installed.

25.lbxproxy(1) Might Cause a Buffer Overflow in Solaris
Sun Alert Notifications: 44842
11 Jul 2002

The vulnerable software is not installed.

26.Buffer overflow in vold(1M)
Sun Alert Notifications: 45707
10 Jul 2002

The vulnerable software is not installed.

27.Security Vulnerability in the rpc.rwalld(1M) Daemon
Sun Alert Notifications: 44502
24 Jun 2002

The system is not vulnerable because the affected software (rwalld) is disabled; however it and its copackaged software are not required on this system. The SUNWrcmds package should be removed.

Security Patch Installation and Management

No patches appear to have been installed on this system and no patch management is occurring. Admittedly, at the time of initial installation, there were no patches available for Solaris 9, however, this does not mean that patches should not have been installed as they came available. In Solaris, normally, you check for installed patches using the command “showrev -p”; however the showrev command is not installed on this system and it was necessary to check the /var/sadm/patch directory to determine whether patches had been installed. If patches have been installed with the default back out option enabled, there will be a directory for each patch in this directory; if not, either the system is unpatched, backout information was directed to another location, or the system was patched without backout information. This directory was empty. In addition, the command “uname -a” returned:

SunOS flipper 5.9 Generic sun4u sparc SUNW,Sun-Fire-280R

More recent security patches often require kernel patches (and often the security fixes are a part of the kernel patch.) The current kernel patch is 112233-04. A system with a patched kernel shows the kernel patch number as a part of the version name, as shown in this example from an Ultra 10:

SunOS incubus 5.9 Generic_112233-03 sun4u sparc SUNW,Ultra-5_10

This also implies that no patches have been installed.

Sun provides a number of tools to determine which patches should be installed on a system. They all use the same data file, patchdiag.xref[23], for information about available patches; so they all return the same information. The difference is in the interface. I prefer the older tool, patchdiag[24], because it can produce patch information for local or remote systems and returns information in a format that is easily readable as well as easily parsable by software tools. In addition, patchdiag returns a list of needed patches in the order they should be installed to resolve dependencies[25], although it is dependant on the quality of the prerequisite information in patchdiag.xref, which is sometimes imperfect. To run patchdiag for a remote system, you need a file with the output of “showrev -p”, which lists the currently installed patches. Since the showrev command is not installed on this system, I couldn't do this, since I had determined that no patches had been installed, I was able to use the empty file, /dev/null. You also need a file containing the output of pkginfo -l, I called this file pkgs_flipper. I ran patchdiag using the command:

patchdiag -p /dev/null pkgs_flipper 5.9 sparc flipper

This listed all of the patches that should be installed on this system for security and

proper function, the output is listed in Appendix D. There are sixty-six patches that should be installed, of which twenty-six have specific security functions.

Configuration Vulnerabilities

A number of configuration vulnerabilities were found as part of the automated scanning tools, and detailed in the previous section; these will not be addressed here unless there is a need to go into further detail.

System Time

Although not a vulnerability, per se, the system time is almost seven minutes behind clock time (all other city servers I had access to agreed with clock time.) In the event of an intrusion or other multi-system event, it can be impossible to determine the sequence of events if all systems do not keep synchronized time. The city uses NTP (Network Time Protocol) to synchronize time for other city servers, this should be done for this server as well.

Passwords

A more serious configuration vulnerability has to do with passwords. As mentioned earlier, the informal password policy is to set secure passwords, protect those passwords, and change them if they are believed to have been compromised; so the system is not configured to require or limit changing passwords. However, there are no measures in place to ensure that this policy is followed.

A password cracking tool, John the Ripper[26], was used to determine whether secure passwords are in fact being used. Although you cannot decrypt Unix passwords, you can guess them. John the Ripper uses a word list (a dictionary) and some rules about how to alter or combine words in the list (permutation) and makes a series of guesses until it guesses the password correctly or runs out of guesses. Because John the Ripper(JtR) can expose passwords, I did not install it on this host, instead I downloaded and installed the software on a workstation used only by myself. In addition to the included word list, I created my own word list consisting of the names of most city servers, I called this dictionary “giac_hosts.txt”. I also downloaded several word lists intended for password cracking from the internet and combined them along with /usr/dict words, this is detailed in Appendix E. A final John the Ripper configuration I made was to edit the permutation rules to do some standard number and symbol for letter substitutions for all tests. This is done by copying the lines in john.ini under “-single” mode from the comment referring to the “3l33t rules” to the next comment and placing them in the section for “-wordlist” mode rules.[27] To actually attempt to guess passwords, I copied the /etc/password and /etc/group files from flipper to John the Ripper's “run” directory on that workstation. I ran the unshadow command to create a single old-style password file (flippertestfile) with account information and encrypted passwords using the syntax “./unshadow passwd shadow > flippertestfile”.

John the Ripper discovered three user passwords out of about twenty in a matter of seconds in “single” mode, which tries different permutations of the user's full name and username, “john -single flippertestfile”. Next, I tried using several word lists in wordfile

mode. I started with the included word list, passwd.lst, using the syntax:

./john -wordfile:password.lst -rules flippertestfile

This did not result in any guessed passwords. Using the word list of local host names (giac_hosts.txt) instead of password.lst, did not disclose any further passwords. Finally, using the large dictionary I had compiled, mydict.dict, resulted in finding three more passwords after several hours of processing; interestingly these all belonged to administrators who believed they had chosen passwords that would be very difficult to crack.

Testing with John the Ripper showed that secure passwords are not always being used. An opportunity arose that also showed that passwords are also not being kept secure or changed when disclosed. In addition to a security audit, I had been asked to check that the system configuration allowed several FTP connections that had been tested several months previously and were to go into production shortly, I received an email containing the user name and passwords to be used for each connection. A look at trouble tickets for this system showed that in many cases, the usernames and passwords were being entered into trouble tickets. Some of these were the same usernames that JtR had cracked or I had been given, and the passwords had not been changed after being disclosed via entry in the trouble ticket. If a password is known, this greatly increases the range of exploits available to an attacker; it also allows attackers to use system resources for their own ends.

FTP Configuration

This system is running the FTP server included with Solaris 9, which is based on wu-ftpd. Gaining access to a system via the FTP daemon usually gives an attacker root access, gaining access to an FTP account usually gives a hacker a way to transfer further hacking tools onto the system. Hal Pomeranz calls wu-ftpd “the server they love to hack”[28], due to it's ubiquitous on the internet and recommends using it only if you need its special features - the strict controls it can provide for anonymous uploads and the ability to have restricted guest user access. Neither of these features are currently being used, however, I would recommend implementing the FTP-only users on this system as wu-ftpd guest users, rather than their current implementation as regular users with a shell of /bin/false to prevent them from logging in. Setting the users up as guest users would allows them to FTP in, but would restricts them to specified directories for file transfer. Commonly, the individual users home directories are used as the restricted directories, however, since the FTP users have been configured to all share one home directory, it makes more sense to create a single file transfer area for these users to share and restrict them to that area.

SFTP Configuration

Users who have access to sftp also have access to ssh. This means that these users can upload an arbitrary file and then use ssh to run it on the system. It also means that they can login. Both of these scenarios allow more access than desired. Actions that block ssh access, such as using /bin/false for the shell or locking out ssh via tcp wrappers, also block sftp access. It might be possible to limit access appropriately by

using key based authentication setting the command options to allow only file transfer, however installing ssh authentication keys is more work than desired for the end users. One solution might be to install a chrooted ssh server, limiting the available ssh commands, as well as their potential effects.

Risks from Installed Third Party Software

The only installed third party software is sudo. Sudo, in general, is a security asset. However, a locally exploitable security hole that may allow a user to use sudo to gain unrestricted and unlogged root access exists in sudo versions 1.5.7 to 1.6.5p2[29], version 1.6.5p2 is installed on this system.

Administrative Practices

This system is a victim of benign neglect. It is not being patched or maintained. Because of it's isolated location on the network, this server is not part of the City's centralized logging, maintenance and patching infrastructure. Administrators acknowledge that no one is regularly checking logs, although the operators do check that the system is running on a regular basis. This means that were the system compromised, an intruder could probably escape detection for an indeterminate period of time. Because the system is not being maintained regularly, as security holes are found in the operating system, they are not being fixed; this leaves the system open to attack using published vulnerabilities, the firewalls do provide partial protection from this risk, but are only a single layer of defense.

The user and administrative practices regarding passwords are also a concern. These risks were addressed in detail in the section on configuration vulnerabilities.

Identification and Protection of Sensitive Data on the Host and In Transit Over the Network or Internet

The policy for this system is that sensitive data is not to be transferred to this system unless it is encrypted in a manner appropriate for the sensitivity of the data. Although I did not audit policy compliance, the city does audit appropriate handling of sensitive data; these audits have not shown problems regarding the data transfers on this system. The administrators and users that I spoke with were aware of the importance of protecting sensitive data and how to determine whether data was sensitive if they did not know.

The remaining piece of sensitive data related to this system is passwords. On the system, passwords are protected by being encrypted and kept in the /etc/shadow file, which is not readable by users. In transit, with one exception, only sftp, which does not use clear text authentication, is used for connection to and from this host from outside the City's networks. The one exception is a key business partner whose security policies restrict them from installing sftp client software; efforts are currently underway to find a method of transferring this data that meet both sides' security policies, but in the meantime management has determined that using FTP for that transfer is the best choice. Administrators connect to this system via ssh or on the system console. FTP connections from within the city's networks do use clear text authentication. Due to the

increased access control that FTP allows compared to sftp, this seems to be a reasonable measure.

Access Controls

Electronic access controls for this system have been covered in other areas of this report, particularly in the section on Operating System Vulnerabilities.

This system has excellent physical access controls. The server and its restricted access network are in a restricted access room of a restricted access building. Employees and contractors who work in the building or who are allowed to visit the building unescorted are required to undergo a background check by the city's police department. (Cleaning contractors are also bonded.) Access to server room is limited to specific technical employees who need to physically access the hardware or system consoles. Other employees and guests are allowed into the server room only with an upper manager's approval. Access to the building and the server room are subject to both physical (doors with logging electronic locks) and human controls. Efforts are underway to further limit physical access to this and other systems by creating a secured console area and a secured hardware area with separate access controls and limits for each. The server room is also physically protected by being below ground and having a monitored, controlled environment (water sensors, temperature control, power conditioning, and backup power via batteries and a generator) with a chemical fire suppressant system.

Backup Policies and Disaster Preparedness

It has been determined that the city could do business for up to several weeks with little or no disruption without this server. This is checked when users request new FTP accounts. The only non-operating system data on this system is transient, so backups are unlikely to save any user data, and in fact, saving user data is often undesired. As a result, the backup policy for this system is to rebuild it if there is a failure or compromise rather than back it up. There is a jumpstart server on another network which is configured to rebuild this server if necessary. Due to the long period of time the city can go without this server, it is not a part of disaster recovery plans; however the jumpstart server and its data are covered by disaster recovery plans. In the event this system fails or is compromised, some configuration changes will be lost, since the server will be rebuilt to its initial state (with the exception that the jumpstart server is configured to install the latest version of the OS and most recent patches). Although the information in these files could be recreated using existing documentation, the time involved might cause an administrator to err on the side of risk in the event of a suspected system compromise and leave the system running. In addition, if the system needed to be rebuilt at a particularly busy time, stress and time pressure could cause the system to be accidentally reconfigured in a less secure manner.

Other Issues

This system does not have any type of file integrity assessment tools installed. File integrity assessment tools monitor whether system files and binaries have been altered. If key system files, for instance, the FTP daemon or the ls command, are replaced with

trojaned versions, an attacker can cause arbitrary actions, such as executing commands or gathering data. Rootkits usually included several trojaned programs used to hide the presence of a hacker. Examples of such tools are Tripwire, Sun's ASET, and Sun's Solaris Fingerprint Database Companion and Sidekick. Kernel auditing logs may also give some clues regarding file integrity, depending on what is audited.

Critical Issues and Recommendations

Critical Issues

The ten most critical security issues on this system involve:

Patching
Server Minimization
Policy
Improve Logging and Access Controls for User Connections
Treat All FTP Users as Guest Users
Install fixmodes
Upgrade sudo
Synchronize System Time
Improve Monitoring of User Actions and System Changes
Resolve Differences Between SFTP Configuration and Policy

These issues are the most critical because they affect multiple areas or vulnerabilities and involve key system services or security software. I have attempted to list these items in order of the most value for the effort, but in many cases, the relative importance of these areas depends on outside factors.

Recommendations

Patching

Patching removes many know security vulnerabilities. Download the patches listed in Appendix D from sunsolve.sun.com. Use the patchadd command to install them. A system reboot will be necessary for all of the changes to take effect.

To allow patch management in the future, the SUNWadmc package should be installed from the Solaris CD's to provide the showrev command.

Implement controls to ensure the system is patched regularly.

Server Minimization

Use the pkgrm command to remove unneeded packages, as listed in Appendix A. Server minimization is the most effective way of reducing unknown security vulnerabilities.

Policy

Management needs to provide the technical staff with security policy or objectives to use in determining procedures and installing and maintaining systems. Management, not technical staff, should be determining the acceptable level of security risk, and

security policies are the best means for management to do so[30]. Without a security policy, it is difficult to determine whether effort to make a system more secure is a necessary measure or a waste of organizational resources. Joel Weise and Charles R. Martin's article "Developing a Security Policy" is a good management resource on security policy development.

The current password policy is not being followed and it is very difficult to implement controls to enforce it. Due to the importance of passwords in system security, the password policy should be changed so that it can be enforced via automated controls. User training in choosing good passwords and keeping passwords secret should be implemented.

Improve Logging and Access Controls for User Connections.

Solaris 9 inetd can provide host based access control using /etc/hosts.allow and /etc/hosts.deny files.[31] Sshd will also use these files if SUNWtcpd is installed.[32] Install the SUNWtcpd package and set ENABLE_TCPWRAPPERS=YES and ENABLE_CONNECTION_LOGGING =YES in /etc/default/inetd. The hosts.deny file should contain the line ALL:ALL. Determine which hosts need access to which services. In the /etc/hosts.allow file, create entries of the form:

```
ftp: host1,host2,...
ssh: host3,host4,...
```

You will need to force inetd to reread its configuration files by running the command "pkill -HUP inetd".

Set "MaxAuthTries 3" and "MaxAuthTriesLog 0" in /etc/ssh/sshd config.

Remove telnet from /etc/inetd.conf

Turn on debug level logging for FTP by adding the -d option to in.ftpd in /etc/inetd.conf.

Remove, rather than comment out, all unused services and comments from inetd.conf, allowing administrators to see at a glance that only approved services are included.[33]

Remove the ability for the root user to login over the network other by uncommenting the "#CONSOLE=/dev/console" line in /etc/default/login. Log all failed logins by adding the line "SYSLOG_FAILED_LOGINS=0".

Increase the security of user tty's by adding the line "mesg n" to /etc/profile and /etc/.login.

Disable serial logins by removing the line:

```
sc:234:respawn:/usr/lib/saf/sac -t 300
```

from /etc/inittab.

Treat All FTP Users as Guest Users

Choose a directory to use as the restricted area; /transfer/home appears to be appropriate for this server, but another could be chosen. Create an appropriate

chrooted environment by running “ftpconfig -d /transfer/home”. This command will need to be rerun whenever patches are added or system files are updated.[34]

Add the following lines to /etc/ftp/ftpaccess:

```
class gst    guest        *
log command               guest
log transfers                          guest
log security              guest
guestuser   *
noretrieve   /etc /usr /dev /bin
guest-root   /transfer/home
loginfails 0
```

Create password entries for FTP users in /transfer/home/etc/password using the following ksh command:

```
for user in <login>
do
grep $user /etc/passwd \
        | awk -F: '{print “$1::$3:$3::/pub:”}'\
         |  sudo tee -a /transfer/home/etc/passwd
done
```

If the grep happens to match any extra entries, you will see this on your terminal. If this happens, you will need to remove the extra lines from /transfer/home/etc/passwd. As new FTP users are added, they will need to be added to the guest user passwd file in a similar manner.

Install fixmodes

Download and run the fixmodes program from http://www.sun.com/solutions/blueprints/tools/[35]

Setup a root cron job to run it on at least a weekly basis.

Upgrade sudo

Upgrade sudo to version 1.6.6. Sudo version 1.6.6 is available from sunfreeware, the source of the currently installed version[36]. The easiest way to upgrade is to save the sudoers file, remove the current sudo package (SFWsudo) and install the new package.

Synchronize System Time

Assuming the address of the city's timeserver is 10.20.30.40, create an /etc/ntp.conf file containing the following:

```
server 10.20.30.40
restrict  nomodify
```

driftfile /etc/inet/ntp.drift

Start NTP by running "/etc/init.d/xntpd start"

Improve Monitoring of User Actions and System Changes

System accounting can be turned on by installing the SUNWaccr and SUNWaccu packages, and then following the comments in the sys crontab and /etc/init.d/perf with regards to which lines to uncomment to enable system accounting.

The Center for Internet Security supplies a recommended configuration for kernel auditing in the CISscan package; the following recommendations are heavily based on that configuration with one or two very minor changes for this environment. A good summary of kernel auditing usage, and the source of the explanations below, is Darren J Moffat's article FOCUS on Sun:Solaris BSM Auditing[37]. Kernel auditing (BSM auditing) is turned on by running the program /etc/security/bsmconv. Since this server is in a secure environment, reenable the ability to use the <stop-A> keyboard abort feature by removing the line "abort_enable=0" from /etc/system. Configure auditing by creating the file /etc/security/audit_control containing:

```
dir:/var/audit
flags: lo,ad,fm,-fw,-fc,-fd,na
naflags:lo,ad,fm,-fw,-fc,-fd,nt
minfree:20
```

This will audit login events, administration events (like user creation), and failed file create, delete, write, and attribute modify events whether or not they can be attributed to a user. It also logs all network events that cannot be attributed to a user. All user executed commands can be logged as well, by adding ex to the flags and naflags lines.

Add the line "auditconfig -setpolicy +argv,arge" to /etc/security/audit_startup to include command line arguments and environment variables for command in logs.

If you would like to start a new audit file daily, add a line to root's crontab to run "/usr/sbin/audit -n" every night at midnight.[38]

Choose, install,l and run a file integrity assessment tool. For this site, the best choice is probably Sun's Solaris Fingerprint Database Companion and Sidekick. These tools use the Solaris Fingerprint Database, which is able to determine whether an operating system command was distributed by Sun (either as part of the OS distribution or as a patch.) This is a good choice for the city because unlike most file integrity assessment tools, it can identify files that were altered before the tools were installed, so it is equally useful on a new or existing system. Because it recognizes and identifies Sun provided software, it does not give false warnings if a system is patched and the database is not updated. It is also free and comes from a preferred software source, so there is no need to wait for the next budget cycle to implement it.

Resolve Differences Between SFTP Configuration and Policy

Current policy dictates that file transfer users should not be able to login to the system. Sftp users can login and run commands via ssh. A technical solution to this issue needs to be found or policies should be changed to take this risk into account.

Additional Actions for Increased Security

The following items would further increase system security. The system is already protected against these vulnerabilities by at least one layer of defense; however, most of these items are fairly simple and would not take a significant amount of time or effort to implement.

Add mount options for better security to /etc/vfstab

Turn on filesystem logging for all the file systems by placing the word "logging" in the mount options field (the last field) in /etc/vfstab. Use "ro,logging" for /usr to make it a read-only file system. Use "nosuid,logging" for /transfer and /transfer2 to keep suid executables from being created in user home directories and FTP file transfer areas. Use "remount.ro" for the root filesystem, since the root filesystem must be mounted before /etc/vfstab can be read.

Turn off listening for remote syslog messages

This can be fixed by altering /etc/init.d/syslog to start syslogd with the -t switch

/etc/system changes

Disable coredumps by adding "set sys:coredumpsize = 0" to /etc/system.

Network parameter settings

This system sets network parameters via the /etc/init.d/nddconfig script supplied by the Sun Security Toolkit, alter the script so that tcp_ip_abort_cinterval is set to a 60,000.

System Cleanup

Remove group read permission from the filesystem device files (/dev/dsk/c1t*d*s*).

Remove the setuid bit from ufsrestore. Report the relative pathnames in ufsrestore as bug.

The startup scripts for most unused services on this system have been renamed to "_original name." This should be done for /etc/rc2.d/S73cachefs.daemon, /etc/rc2.d/S93cacheos.finish and /etc/rc2.d/S71ldap.client as well.

Remove the unowned files in /export/home/admin1/opt.

Planning for system recovery

Improve the ability to rebuild the system in case of failure or intrusion by implementing a process to regularly copy key configuration files to a floppy disk or another host for ease in rebuilding. These changes could also be added to the waiting jumpstart configuration, although the time and effort involved may not make this worthwhile.

Setup X window security.

Keep any future X server from listening for messages from remote clients by creating a /etc/dt/config/Xservers file containing the line:

:0 Local local_uid@console root /usr/openwin/bin/Xsun :0 -nobanner -nolisten tcp

This file should be owned by root, with group sys and read-only permissions for everyone. Authorized users will still be able to display windows on the local system by using SSH to forward X events.

Remove the potential to allow remote GUI login services by creating the file /etc/dt/config/Xaccess containing the following two lines:

```
!*
!*              CHOOSER BROADCAST
```

NOTES

[1]The City of GIAC was originally the company town for GIAC Industries, the fortune cookie fortune company, however, when GIAC industries moved to e-commerce, the City of GIAC became a regular municipality.

[2]Joel Weise and Charles R. Martin, "Developing a Security Policy", Sun BluePrints OnLine December 2001, 1 Feb. 2003 <http://www.sun.com/blueprints>, 3.

[3]Alex Noordergraf, et al., Enterprise Security: Solaris Operating Environment, (Upper Saddle River, NJ: Sun Microsystems Press-Prentice Hall, 2002) 129.

[4]RSC cards are a hardware device included in some Sun servers. They are designed to allow remote console access via IP network, secured dial-in, or serial access in a more secure manner than is easily available through the use of standard modems and terminal servers. RSC software has not been installed on this server, so RSC security will not be addressed.

[5]This is the initial version of Solaris 9 from May 2002; updated versions have a month/year tag.

[6]The SANS Institute, SANS/FBI Top 20 List, ver 3.22, 20 March, 2003 <http://www.sans.org/top20/top20.pdf>.

[7]Alex Noordergraf, et al., 3.

[8]Geoff Haprin, A System Administrators Guide to Auditing, Short Topics in System Adminstration 6, (Berkeley: The USENIX Association, 2000) 9.

[9]Nmap, ver. 3.00, 12 Feb. 2003, <http://www.sunfreeware.com>.

[10]John the Ripper, Ver. 1.6, 12 Feb. 2003, <http://www.openwall.com/john/>.

[11]CISscan, The Center for Internet Security, ver. 1.3.0, Feb. 12, 2003, <http://www.cisecurity.com/>.

[12]Bob Todd, TARA, version 3.0.2, 12 Feb. 2003, <http://www-arc.com/tara/index.shtml>.

[13]Patchdiag rev 1.25 ver. 1.0.4, 31 October, 2000 <http://sunsolve.sun.com/private-cgi/show.pl?target=resources/patchdiag>.

[14]City of GIAC Technical Services, "FTP Server Account Request", 2002.

[15]CISscan, version 1.3.0.

[16]Bert Miuccio, "New and Updated CIS Benchmarks," online posting, 21 Mar. 2003, <cis@cisecurity.org>.

[17]"Solaris Benchmark v1.1.0", The Center for Internet Security (http://www.CISecurity.org), 2001-2002, p. 47.

[18]Todd Miller, Sudo Main Page, 4 March 2003 <http://www.courtesan.com/sudo/>.

[19]Bob Todd.

[20]Nmap, ver. 3.00.

[21]Sun Alerts Collection, Sun Microsystems, 25 March, 2003, <http://sunsolve.sun.com/priviate-cgi/search.pl><http://sunsolve.sun.com/pub-cgi/search.pl?mode=results&origin=advanced&range=20&so=date&coll=fsallert&zone_32=category:security>.

[22]Carnegie Mellon Software Engineering Institute Cert Coordination Center, Cert CC Vulnerability Note VU#683673, 21 March 2003 <http://www.kb.cert.org/vuls/id/683673>.

[23]Sun Microsystems, patchdiag.xref, 20 Mar 2003 <http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=patchdiag.xref&method=H>.

[24]Patchdiag rev 1.25 ver. 1.0.4.

[25]Miq Milman, Personal Conversation, October 2000.

[26]John the Ripper, Ver. 1.6.

[27]Hal Pomeranz, UNIX Security Tools, Track 6 – Securing UNIX Systems 6.2 (The SANS Institute, 2002) 68.

[28]Hal Pomeranz, Running UNIX Applications Securely, Track 6 – Securing UNIX Systems 6.4 (The SANS Institute, 2002) 112-113.

[29]Todd Miller, Sudo Prompt Buffer Overflow, 4 March, 2003, <http://www.courtesan.com/sudo/alerts/prompt.html>

[30]Joel Weise and Charles R. Martin, "Developing a Security Policy", Sun BluePrints OnLine December 2001, 1 Feb. 2003 <http://www.sun.com/blueprints>, 3.

[31]Sun Microsystems, What's New in the Solaris 9 Operating Environment, (Santa Clara: Sun Microsystems, Inc., 2002) 3 March, 2003 <http://docs.sun.com/db/doc/806-5202/6je7shk4c?q=%22tcp+wrappers%22+solaris+9&a=view> Chapter 2.

[32]Sun Microsystems, Solaris 9 Reference Manual Collection, 2 April, 2003 <http://docs.sun.com/db/coll/40.7>, Sshd(1m).

[33]Hal Pomeranz, UNIX Practicum, Track 6 – Securing UNIX Systems 6.5 (The SANS Institute, 2002) 38.

[34]Sun Microsystems, Solaris 9 Reference Manual Collection, 2 April, 2003 <http://docs.sun.com/db/coll/40.7> ftpconfig(1m).

[35]Sun Microsystems, Sun Blueprints Online – Scripts and Tools, 10 March 2003, <http://www.sun.com/solutions/blueprints/tools/>.

[36]Steven M. Christensen and Associates, Freeware for Solaris, 4 March, 2003 <http://www.sunfreeware.com>.

[37]Darren J Moffat, FOCUS on Sun: Solaris BSM Auditing, 11 March, 2003 <http://www.securityfocus.com/infocus/1362>.

[38]Sun Microsystems, Solaris 9 Reference Manual Collection, 2 April, 2003 <http://docs.sun.com/db/coll/40.7> audit(1m).

Appendix A

Listing of all installed packages as displayed by the "pkginfo" command

Packages in italics are recommended for consideration for removal. Additional packages may also be potentially removable.

system	SFWsudo	Sudo - superuser do
system	SUNWadmr	System & Network Administration Root
ALE	*SUNWale*	*Asian Language Environment Common Files*
ALE	*SUNWalex*	*Asian Language Environment Common Files (64-bit)*
system	*SUNWatfsr*	*AutoFS, (Root)*
system	*SUNWatfsu*	*AutoFS, (Usr)*
system	*SUNWauda*	*Audio Applications*
system	*SUNWaudd*	*Audio Drivers*
system	*SUNWauddx*	*Audio Drivers (64-bit)*
system	SUNWbip	Basic IP commands (Usr)
system	*SUNWbsr*	*Boot Server daemons (Root)*
system	*SUNWbsu*	*Boot Server daemons (Usr)*
system	SUNWbzip	The bzip compression utility
system	SUNWcar	Core Architecture, (Root)
system	SUNWcarx	Core Architecture, (Root) (64-bit)
system	*SUNWced*	*Sun GigaSwift Ethernet Adapter (32-bit Driver)*
system	*SUNWcedx*	*Sun GigaSwift Ethernet Adapter (64-bit Driver)*
system	SUNWcsd	Core Solaris Devices
system	SUNWcsl	Core Solaris, (Shared Libs)
system	SUNWcslx	Core Solaris Libraries (64-bit)
system	SUNWcsr	Core Solaris, (Root)
system	SUNWcsu	Core Solaris, (Usr)
system	SUNWcsxu	Core Solaris (Usr) (64-bit)
system	SUNWdfb	Dumb Frame Buffer Device Drivers
system	*SUNWdtcor*	*Solaris Desktop /usr/dt filesystem anchor*
system	SUNWeridx	Sun RIO 10/100 Mb Ethernet Drivers (64-bit)

system SUNWesu Extended System Utilities

system SUNWeu8os American English/UTF-8 L10N For OS Environment User Files

system SUNWeu8ox American English/UTF-8 L10N For OS Env User Files (64-bit)

system SUNWeuhed UTF-8 L10N For CDE Help Developer Environment

system SUNWeuluf UTF-8 L10N For Language Environment User Files

system SUNWeulux UTF-8 L10N For Language Environment User Files (64-bit)

system SUNWfcip Sun FCIP IP/ARP over FibreChannel Device Driver

system SUNWfcipx Sun FCIP IP/ARP over FibreChannel Device Driver (64-bit)

system SUNWfcp Sun FCP SCSI Device Driver

system SUNWfcpx Sun FCP SCSI Device Driver (64-bit)

system SUNWfctl Sun Fibre Channel Transport layer

system SUNWfctlx Sun Fibre Channel Transport layer (64-bit)

system SUNWftpr FTP Server, (Root)

system SUNWftpu FTP Server, (Usr)

system SUNWged Sun Gigabit Ethernet Adapter Driver

system SUNWgedx Sun Gigabit Ethernet Adapter Driver (64-bit)

system SUNWhmd SunSwift Adapter Drivers

system SUNWhmdx SunSwift Adapter Drivers (64-bit)

system SUNWi15cs X11 ISO8859-15 Codeset Support

system SUNWi1cs X11 ISO8859-1 Codeset Support

system SUNWinamd Internet Domain Name Server

system SUNWinleu Indic Locale Environment User Files

system SUNWinlex Indic Language Environment user files (64-bit)

system SUNWkey Keyboard configuration tables

system SUNWkrbr Kerberos version 5 support (Root)

system SUNWkrbu Kerberos version 5 support (Usr)

system SUNWkvm Core Architecture, (Kvm)

system SUNWkvmx Core Architecture (Kvm) (64-bit)

system SUNWlibms Forte Developer Bundled shared libm

system SUNWlldap LDAP Libraries

system	SUNWlmsx	Forte Developer Bundled 64-bit shared libm
system	SUNWloc	System Localization
system	SUNWlocx	System Localization (64-bit)
system	SUNWluxop	Sun Enterprise Network Array firmware and utilities
system	SUNWluxox	Sun Enterprise Network Array libraries (64-bit)
system	SUNWmdi	Sun Multipath I/O Drivers
system	SUNWmdix	Sun Multipath I/O Drivers (64-bit)
system	SUNWnamos	Northern America OS Support
system	SUNWnamow	Northern America OW Support
system	SUNWnamox	Northern America 64-bit OS Support
system	*SUNWnfscr*	*Network File System (NFS) client support (Root)*
system	*SUNWnfscu*	*Network File System (NFS) client support (Usr)*
system (64-bit)	*SUNWnfscx*	*Network File System (NFS) client support (Root) (64-*
system	*SUNWnfssr*	*Network File System (NFS) server support (Root)*
system	*SUNWnfssu*	*Network File System (NFS) server support (Usr)*
system (64-bit)	*SUNWnfssx*	*Network File System (NFS) server support (Root) (64-*
system	*SUNWnisr*	*Network Information System, (Root)*
system	*SUNWnisu*	*Network Information System, (Usr)*
system	SUNWntpr	NTP, (Root)
system	SUNWpd	PCI Drivers
system	SUNWpdx	PCI Drivers (64-bit)
system	SUNWpiclr	PICL Framework (Root)
system	SUNWpiclu	PICL Libraries, and Plugin Modules (Usr)
system	SUNWpiclx	PICL Libraries (64-bit)
system	SUNWpl5u	Perl 5.6.1 (core)
system	SUNWpl5v	Perl 5.6.1 (non-core)
system	*SUNWqfed*	*Sun Quad FastEthernet Adapter Driver*
system	*SUNWqfedx*	*Sun Quad FastEthernet Adapter Driver (64-bit)*
system	SUNWqlc	Qlogic ISP 2200/2202 Fibre Channel Device Driver
system (64-bit)	SUNWqlcx	Qlogic ISP 2200/2202 Fibre Channel Device Driver

system	*SUNWrcmdc*	*Remote Network Client Commands*
system	*SUNWrcmdr*	*Remote Network Server Commands (Root)*
system	*SUNWrcmds*	*Remote Network Server Commands (Usr)*
system	SUNWrmodu	Realmode Modules, (Usr)
system	SUNWroute	Network Routing daemons/commands (Usr)
system	SUNWses	SCSI Enclosure Services Device Driver
system	SUNWsesx	SCSI Enclosure Services Device Driver (64-bit)
system	SUNWsndmr	Sendmail root
system	SUNWsndmu	Sendmail user
system	SUNWsolnm	Solaris Naming Enabler
system	*SUNWssad*	*SPARCstorage Array Drivers*
system	*SUNWssadx*	*SPARCstorage Array Drivers (64-bit)*
system	*SUNWssaop*	*SPARCstorage Array Utility*
system	SUNWsshcu	SSH Common, (Usr)
system	SUNWsshdr	SSH Server, (Root)
system	SUNWsshdu	SSH Server, (Usr)
system	SUNWsshr	SSH Client and utilities, (Root)
system	SUNWsshu	SSH Client and utilities, (Usr)
system	SUNWswmt	Install and Patch Utilities
system	*SUNWtftp*	*Trivial File Transfer Server*
system	*SUNWtftpr*	*Trivial File Transfer Server (Root)*
system	*SUNWtleu*	*Thai Locale Environment User Files*
system	*SUNWtleux*	*Thai Language Environment user files (64-bit)*
system	*SUNWtnamd*	*Trivial Name Server (Usr)*
system	*SUNWtnamr*	*Trivial Name Server (Root)*
system	SUNWtnetc	Telnet Command (client)
system	SUNWtnetd	Telnet Server Daemon (Usr)
system	SUNWtnetr	Telnet Server Daemon (Root)
system	SUNWudf	Universal Disk Format 1.50, (Usr)
system	SUNWudfr	Universal Disk Format 1.50
system	SUNWudfrx	Universal Disk Format 1.50 (64-bit)
system	SUNWusb	USB Device Drivers
system	SUNWusbx	USB Device Drivers (64-bit)

system	*SUNWwsr2*	*Solaris Product Registry & Web Start runtime support*
system	*SUNWxwdv*	*X Windows System Window Drivers*
system	*SUNWxwdvx*	*X Windows System Window Drivers (64-bit)*
system	*SUNWxwmod*	*X Window System kernel modules*
system	*SUNWxwmox*	*X Window System kernel modules (64-bit)*

Appendix B

Output of Center for Internet Security (CIS) Solaris Benchmark Scoring Tool.

Output from running the benchmark:

```
% /opt/sfw/bin/sudo /opt/CIS/cis-scan

*****************************************************************************
******************** CIS Security Benchmark Checker v1.3.0 ********************
*                                                                           *
* Lead Developer                                : Jay Beale         *
* Benchmark Coordinator and Gadfly                    : Hal Pomeranz      *
*                                                                           *
* Copright 2001, 2002, The Center for Internet Security  www.cisecurity.org *
*                                                                           *
* Please send feedback to sol-scan@cisecurity.org.                          *
*****************************************************************************

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

                        ******

Now a final check for non-standard world-writable files, Set-UID and Set-GID
programs -- this can take a whole lot of time if you have a large filesystem.
Your score if there are no extra world-writable files or SUID/SGID programs
found will be 6.58 / 10.00 .  If there are extra SUID/SGID programs or
world-writable files, your score could be as low as 6.32 / 10.00 .

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

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

                        ******

          Rating = 6.32 / 10.00

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

  All results/diagnostics:
     more /opt/CIS/cis-ruler-log.20030227-18:00:03.27864
  Positive Results Only:
     egrep "^Positive" /opt/CIS/cis-ruler-log.20030227-18:00:03.27864
  Negative Results Only:
```

egrep "^Negative" /opt/CIS/cis-ruler-log.20030227-18:00:03.27864

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

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

http://www.cisecurity.org

Full Results and Diagnostics

(/opt/CIS/cis-ruler-log.20030227-18:00:03.27864)

*** CIS Ruler Run ***
Starting at time 20030227-18:00:03

Negative: 1.1 System appears not to have been patched within the last month.
Negative: 2.2 telnet not deactivated.
Negative: 2.3 ftp not deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 network printing is deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Positive: 2.9 Disksuite-related network daemons are all deactivated.
Positive: 2.10 kerberos network daemons are deactivated.
Negative: 3.1 cachefs.daemon not deactivated.
Negative: 3.1 cacheos.finish not deactivated.
Positive: 3.2 Windows compatibility servers (samba) are deactivated.
Positive: 3.3 NFS Server script nfs.server is deactivated.
Positive: 3.4 This machine isn't being used as an NFS client.
Positive: 3.5 rpc rc-script is deactivated.
Positive: 3.6 Kerberos server daemons are deactivated.
Positive: 3.7 LDAP directory server is deactivated.
Negative: 3.8 ldap cache manager not deactivated.
Positive: 3.9 The printer init scripts are deactivated.
Positive: 3.10 volume manager is deactivated.
Positive: 3.11 Graphical login scripts are all deactivated.
Positive: 3.12 Mail daemon is not listening on TCP 25.
Positive: 3.13 Web server is deactivated.
Positive: 3.14 snmp daemon is deactivated.
Positive: 3.15 DHCP server start script (dhcp) is deactivated.
Negative: 3.16 System is running syslogd without the -t switch, accepting remote

logging.
Negative: 3.17 inetd is still active.
Negative: 3.18 Serial login prompt not disabled.
Positive: 3.19 Found a good daemon umask of 022 in /etc/default/init.
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 Stack is set non-executable
Positive: 4.3 NFS clients use privileged ports.
Negative: 4.4 tcp_ip_abort_cinterval should be at most 60,000 to avoid TCP flood problems.
Negative: 4.5 ip6_strict_dst_multihoming isn't activated.
Negative: 4.5 ip6_ignore_redirect isn't set to 1.
Positive: 4.6 TCP sequence numbers strong enough.
Positive: 5.1 syslog captures auth messages.
Negative: 5.2 ftp is running out of inetd on port ftp, but does not do "-d" debug logging.
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 read the /etc/rc2.d/S21perf file to check for system acctg.
Negative: 5.5 Couldn't open /var/spool/cron/crontabs/sys to look for sa1 and sa2 -- no system accounting.
Negative: 5.6 BSM should at least be auditing failed "file create" (fc) events on flags line.
Negative: 5.6 BSM should at least be auditing failed "file delete" (fd) events on flags line.
Negative: 5.6 BSM should at least be auditing failed "file attribute modify" (fm) events on flags line.
Negative: 5.6 BSM should at least be auditing failed "file write" (fw) events on flags line.
Negative: 5.6 BSM should at least be auditing all "administrative" (ad) events on naflags line.
Negative: 5.6 BSM should at least be auditing all "network" (nt) events on naflags line.
Positive: 5.7 All logfile permissions and owners match benchmark recommendations.
Negative: 6.1 /usr is not mounted read-only.
Negative: 6.1 /transfer is not mounted nosuid.
Negative: 6.1 /transfer2 is not mounted nosuid.
Negative: 6.2 logging option isn't 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/ftpd/ftpusers
Positive: 7.4 /etc/shells exists and has good permissions.
Positive: 7.5 Global X-terminal login is denied or not available.
Negative: 7.6 Couldn't open /etc/dt/config/Xservers to check that Xserver TCP listening had been disabled.
Positive: 7.7 CDE is either not present or locks the screen after a set timeout period.
Positive: 7.8 cron.allow and at.allow are configured correctly.
Positive: 7.9 crontabs all have good ownerships and modes
Negative: 7.11 /etc/default/login allows non-console root logins
Positive: 7.12 /etc/default/login allows 3 login attempts.
Negative: 7.13 EEPROM isn't password-protected.
Positive: 8.1 All system accounts are locked/deleted
Negative: 8.2 User admin1 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin1 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin1 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin2 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin2 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin2 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin3 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin3 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin3 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin4 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin4 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin4 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin5 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin5 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin5 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin6 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin6 should have a maximum password life of between 1

and 91 days.
Negative: 8.2 User admin6 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin7 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin7 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin7 should have a password expiration warning of at least 7 days.
Negative: 8.2 User admin8 should have a minimum password life of at least 7 days.
Negative: 8.2 User admin8 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User admin8 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user20 should have a minimum password life of at least 7 days.
Negative: 8.2 User user20 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user20 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user9 should have a minimum password life of at least 7 days.
Negative: 8.2 User user9 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user9 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user7 should have a minimum password life of at least 7 days.
Negative: 8.2 User user7 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user7 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user2 should have a minimum password life of at least 7 days.
Negative: 8.2 User user2 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user2 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user6 should have a minimum password life of at least 7 days.
Negative: 8.2 User user6 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user6 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user1 should have a minimum password life of at least 7

days.
Negative: 8.2 User user1 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user1 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user3 should have a minimum password life of at least 7 days.
Negative: 8.2 User user3 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user3 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user4 should have a minimum password life of at least 7 days.
Negative: 8.2 User user4 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user4 should have a password expiration warning of at least 7 days.
Negative: 8.2 User user5 should have a minimum password life of at least 7 days.
Negative: 8.2 User user5 should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User user5 should have a password expiration warning of at least 7 days.
Positive: 8.3 There were no +: entries in passwd, shadow or group maps.
Positive: 8.4 All users have passwords
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 user1 has a group writable homedir!
Negative: 8.7 User user1 has a world-executable homedir!
Negative: 8.7 User user1 has a world-readable homedir!
Negative: 8.7 User user2 has a group writable homedir!
Negative: 8.7 User user2 has a world-executable homedir!
Negative: 8.7 User user2 has a world-readable homedir!
Negative: 8.7 User user3 has a group writable homedir!
Negative: 8.7 User user3 has a world-executable homedir!
Negative: 8.7 User user3 has a world-readable homedir!
Positive: 8.9 No user has a .netrc file.
Positive: 8.10 Umasks in all global shell configuration files appears to be good.
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: 9.1 tcp6-protocol service telnet in inetd.conf is not wrapped.
Negative: 9.1 tcp6-protocol service ftp in inetd.conf is not wrapped.
Negative: 9.2 sshd_config parameter MaxAuthTries, currently 6, should be set to

no more than 3.
Negative: 9.2 sshd_config parameter MaxAuthTriesLog, currently 3, should be set to 0.
Negative: 9.3 Fix-modes has not been run here.
Preliminary rating given at time: Thu Feb 27 18:00:03 2003

Preliminary rating = 6.32 / 10.00

Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/foo/aaa-output
Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/foo/aab-output
Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/foo/aac-output
Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/foo/aad-output
Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/foo/aba-output
Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/bar/abb-output
Negative: 6.7 Non-standard world-writable file:
/export/home/admin1/opt/user1/foo/abc-output
Negative: 6.8 Non-standard SUID program /opt/sfw/bin/sudo
Negative: 6.8 Non-standard SGID program /usr/SUNWale/bin/mailx
Ending run at time: Thu Feb 27 18:00:04 2003

Final rating = 6.32 / 10.00

Appendix C

TARA Output

The explanations, in order of appearance, of the TARA codes follow the security report.

TARA security report

security.report.flipper.030213-0645

Security scripts *** 3.0.2 ARC, 2002.0513.2100 ***
Thu Feb 13 06:45:07 PST 2003
06:45> Beginning security report for flipper (sun4u SunOS 5.9).

Performing check of passwd files...

Performing check of group files...

Performing check of user accounts...
Checking accounts from /etc/passwd.
--WARN-- [acc005w] Login ID adm is disabled, but has a 'cron' file or cron
entries.

--WARN-- [acc006w] Login ID adm's home directory (/var/adm) has group `sys'
write access.
--WARN-- [acc006w] Login ID user2's home directory (/transfer/handover)
has group `ftpuser' write access.
--WARN-- [acc006w] Login ID user1's home directory (/transfer/handover)
has group `ftpuser' write access.
--WARN-- [acc006w] Login ID user3's home directory (/transfer/handover)
has group `ftpuser' write access.

Performing check of /etc/hosts.equiv and .rhosts files...

Checking accounts from /etc/passwd...

Performing check of .netrc files...

Checking accounts from /etc/passwd...

Performing check of /etc/default/login, /securetty, and /etc/ttytab...

```
--WARN-- [root001w] Remote root login allowed in /etc/default/login.


# Performing check of PATH components...
# Only checking user 'root'

# Performing check of anonymous FTP...

# Performing checks of mail aliases...
# Checking aliases from /etc/mail/aliases.

# Performing check of `cron' entries...
--WARN-- Unusual cron file `root.au' found.

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
# Checking inetd entries from /etc/inet/inetd.conf
--WARN-- [inet098w] Use ssh/sftp instead of ftp.
--WARN-- [inet099w] 'ftp' is not protected by tcp wrappers.
--WARN-- [inet098w] Use ssh instead of telnet.
--WARN-- [inet099w] 'telnet' is not protected by tcp wrappers.
--WARN-- [inet005w] Service telnet is using /usr/sbin/in.telnetd instead of
        /usr/sbin/tcpd.

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm021w] Disk device /dev/dsk/c1t0d0s0 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c1t0d0s0 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c1t0d0s4 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c1t0d0s4 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c1t1d0s3 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c1t1d0s3 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c1t0d0s6 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c1t0d0s6 has read access for group
        sys.

# Performing signature check of system binaries...

# Checking for known intrusion signs...
```

Testing for promiscuous interfaces
Testing for backdoors in inetd.conf

Explanations of TARA Codes

Code [acc005w]
The listed login ID is disabled in some manner ('*' in passwd field, etc), but has a 'cron' file or 'cron' entries. This allows commands to be executed on behalf of the login ID, potentially allowing access to the login ID. These should be removed unless specifically set up to provide a service.

Code [acc006w]
The home directory of the listed login ID has group write permission, world write permission or both enabled. This allows new files to be added (and existing files potentially removed) by others. The write permissions should be removed.

Code [root001w]
The indicated file allows remote (i.e., other than system console). root logins for telnet and other services. For /etc/default/login, be sure that the line "CONSOLE=/dev/console" exists. For /etc/securetty, be sure that there are no ttyp entries.

Code [inet005w]
'inetd' is using the indicated binary for the listed service instead of what is
normally expected there. Unexpected differences should be checked, and if anything unusual is found, the system should be checked for other signs of intrusion.

Code [inet098w]
Services that pass sensitive information (including passwords) should be replaced with the family of programs that comprise secure shell (ssh).

Code [inet099w]
The indicated service is not protected by tcp wrappers or xinetd access control.
The use of this facility is encouraged to limit access and to improve logging.

Code [perm021w]
The indicated disk device file is group readable, writable or both by the indicated group. This allows users in this group to bypass the file access controls. Many systems allow a group such as `operator' to have read access so that backups can be performed. Group write access is *not* needed and should be removed. If backups are performed by the `root' account, then group read permissions are not needed and should be removed.

Code [misc008w]
The running kernel is not checking to see if the source port for NFS requests is a privileged port. If the machine is not doing NFS serving, this is not a problem. If it is, this means that any user on an authorized client that can obtain a file handle for an exported file-system can gain unauthorized access to files, and possibly gain unauthorized privileges. If port checking is also disabled for the

NFS mount daemon [misc006w], this becomes very easy to do. To enable port checking, the kernel variable 'nfs_portmon' should be set to a non-zero value. On SunOS 4.x systems, an 'adb' command exists in the /etc/rc.local script to set this variable during boot up. This command is normally only executed for systems which have enabled Sun's C2 security. Removing the command from the surrounding 'if' block will enable it for non-C2 systems.
For SunOS 5.x systems, add the line
set nfs:nfs_portmon = 1
to the /etc/system file and reboot.
NOTE: Enabling NFS port checking may break certain older NFS implementations which do not use a privileged port. You should verify that any clients do not have this problem.

Code [fsys002w]
The listed program is a setuid executable, and it appears to contain relative pathnames (do not start with a '/'). This often represents a security hole in the program. These relative pathnames can be caused by system()* or popen()* calls which do not use full pathnames to the executable, or, on systems which support dynamic linking, relative pathnames indicating the directories containing the libraries. In any case, these need to be checked.
*Note: system() and popen() should *never* be used from a program which is executing with privileges.

Code [fsys003c]
The database of setuid programs for this platform does not exist, thus all setuid programs will be listed. When fully configured for a platform, only those setuid programs that do not appear in the distribution will be listed

Appendix D

Patchdiag Output

This is a list of needed security and recommended patches, in approximately the order of installation.

```
================================================================================
==============
System Name: senegal  SunOS Vers: 5.9      Arch: sparc
Cross Reference File Date: Mar/20/03

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
------ --------- -------- -----------------------------------------
--------------
================================================================================
==============

UNINSTALLED RECOMMENDED PATCHES

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev      ID         ID
------ --- --- --- --------- --------- --------------------------------
---------
112233 N/A  04  49                     SunOS 5.9: Kernel Patch
112601 N/A  05 105                     WITHDRAWN PATCH SunOS 5.9: PGX32
Graphics
112764 N/A  04  74                     SunOS 5.9: Sun Quad FastEthernet
qfe driver
112785 N/A  12  69                     X11 6.6.1: Xsun patch
112808 N/A  03 173                     OpenWindows 3.6.3: Tooltalk
patch
112817 N/A  06  78                     SunOS 5.9: Sun GigaSwift
Ethernet 1.0 driver patch
112834 N/A  02 175                     SunOS 5.9: patch scsi
112875 N/A  01 277                     SunOS 5.9: patch
```

```
/usr/lib/netsvc/rwall/rpc.rwalld
112902 N/A  11   8 112233-01          SunOS 5.9: kernel/drv/ip Patch
112907 N/A  01 188                   SunOS 5.9: libgss Patch
112908 N/A  07  56 112907-01         SunOS 5.9: gl_kmech_krb5 Patch
112951 N/A  04 103                   SunOS 5.9: patchadd and patchrm
Patch
112963 N/A  05 109                   SunOS 5.9: linker patch
112964 N/A  03  27                   SunOS 5.9: ksh patch
112970 N/A  03  27                   SunOS 5.9: patch libresolv.so.2
112975 N/A  01 259                   SunOS 5.9: patch
/kernel/sys/kaio
112998 N/A  02 176                   SunOS 5.9: patch
/usr/sbin/syslogd
113023 N/A  01 152                   SunOS 5.9: Broken preremove
scripts in S9 ALC packages
113033 N/A  03  91                   SunOS 5.9: patch /kernel/drv/isp
and /kernel/drv/sparcv9/isp
113068 N/A  01 246                   SunOS 5.9: hpc3130 patch
113146 N/A  01 231                   SunOS 5.9: Apache Security Patch
113273 N/A  01 200                   SunOS 5.9: /usr/lib/ssh/sshd
Patch
113277 N/A  05  12 112233-02         SunOS 5.9: sd and ssd Patch
                   112834-02
113278 N/A  01 189                   SunOS 5.9: NFS Daemon Patch
113279 N/A  01 189                   SunOS 5.9: klmmod Patch
113319 N/A  05  48                   SunOS 5.9: patch
/usr/lib/libnsl.so.1
113333 N/A  02 127                   SunOS 5.9: libmeta Patch
113454 N/A  04  43                   SunOS 5.9: ufs Patch
113492 N/A  01 160                   SunOS 5.9: fsck Patch
113575 N/A  03  22                   SunOS 5.9: sendmail Patch
113579 N/A  01 137                   SunOS 5.9: ypserv/ypxfrd Patch
113713 N/A  02  11                   SunOS 5.9: pkginstall Patch
113718 N/A  01  76                   SunOS 5.9: usr/lib/utmp_update
Patch
113923 N/A  02  97                   X11 6.6.1: security font server
patch
113993 N/A  01  99                   SunOS 5.9: mkfs Patch
114133 N/A  01  50                   SunOS 5.9: mail Patch
114135 N/A  01  62                   SunOS 5.9: at utility Patch
114153 N/A  01 105                   SunOS 5.9: Japanese SunOS 4.x
Binary Compatibility(BCP) patch
114359 N/A  01  22                   SunOS 5.9: mc-us3 Patch
114564 N/A  01  13                   SunOS 5.9: /usr/sbin/in.ftpd
Patch
================================================================
==============

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
------ --- --- --- --------- --------- --------------------------------
---------
112233 N/A  04  49                   SunOS 5.9: Kernel Patch
```

```
112617 N/A  02  69                    CDE 1.5: rpc.cmsd patch
112785 N/A  12  69                    X11 6.6.1: Xsun patch
112808 N/A  03 173                    OpenWindows 3.6.3: Tooltalk
patch
112874 N/A  12  56                    SunOS 5.9: patch libc
112875 N/A  01 277                    SunOS 5.9: patch
/usr/lib/netsvc/rwall/rpc.rwalld
112902 N/A  11   8 112233-01         SunOS 5.9: kernel/drv/ip Patch
112908 N/A  07  56 112907-01         SunOS 5.9: gl_kmech_krb5 Patch
112926 N/A  03 147                    SunOS 5.9: smartcard Patch
112970 N/A  03  27                    SunOS 5.9: patch libresolv.so.2
113030 N/A  02  97                    SunOS 5.9: /kernel/sys/doorfs
Patch
113146 N/A  01 231                    SunOS 5.9: Apache Security Patch
113240 N/A  03  19                    CDE 1.5: dtsession patch
113273 N/A  01 200                    SunOS 5.9: /usr/lib/ssh/sshd
Patch
113278 N/A  01 189                    SunOS 5.9: NFS Daemon Patch
113279 N/A  01 189                    SunOS 5.9: klmmod Patch
113319 N/A  05  48                    SunOS 5.9: patch
/usr/lib/libnsl.so.1
113454 N/A  04  43                    SunOS 5.9: ufs Patch
113575 N/A  03  22                    SunOS 5.9: sendmail Patch
113579 N/A  01 137                    SunOS 5.9: ypserv/ypxfrd Patch
113718 N/A  01  76                    SunOS 5.9: usr/lib/utmp_update
Patch
113923 N/A  02  97                    X11 6.6.1: security font server
patch
114008 N/A  01   6                    SunOS 5.9: cachefsd Patch
114133 N/A  01  50                    SunOS 5.9: mail Patch
114135 N/A  01  62                    SunOS 5.9: at utility Patch
114564 N/A  01  13                    SunOS 5.9: /usr/sbin/in.ftpd
Patch
================================================================
===============

UNINSTALLED Y2K PATCHES

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

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev       ID         ID
------ --- --- --- --------- --------- --------------------------------
---------
All Y2K patches installed!
================================================================
===============

OTHER RELATED UNINSTALLED PATCHES

NOTE: This is determined by the packages that have been
      installed on the system.

      When one patch refers to multiple packages, we list the
      additional packages in the next lines.

      The various 'S','R','*' marks denote unbundled packages
```

```
      that is designated as an 'Security' or 'Recommended'.

         S = Security
         R = Recommened Unbundled
         * = Both Security and Recommended Unbundled

Patch    Package   Lat Age Synopsis
  ID     Name      Rev
------ - --------- --- --- ----------------------------------------
---------------
================================================================================
===============
```

Appendix E

Creating a Comprehensive Word List to Use in Password Guessing

Potential passwords were collected from a number of different sources:

From the large collection of dictionaries at ftp.cerias.purdue.edu:

- Common passwords as collected by Dan Klein. (/pub/dict/dictionaries/DanKlein/all_words.Z)
- Common English words. (/pub/dict/dictionaries/English/words.English.Z)
- Unix terms and commands. (/pub/dict/wordlists/dictionaries/Unix.dict.gz)
- Computer Jargon. (/pub/dict/wordlists/computer/Jargon.gz)
- More common passwords. (/pub/dict/wordlists/computer/common-passwords.txt.gz)
- Movie names and references. (/pub/dict/wordlists/movieTV/Movies.gz)
- Star Trek names and references. (/pub/dict/wordlists/movieTV/Trek.gz)
- United States ZIP codes. (/pub/dict/wordlists/places/Zipcodes.gz)
- Names of cities, countries, states, ... (/pub/dict/wordlists/places/places.gz)

Another large wordlist, “cracklib.txt” intended for password guessing kitchensink.zip at http://www.accessdata.com/downloads.htm.

The system spelling dictionary, /usr/dict/words.

These files were downloaded, kitchensink.zip was unzipped and the files were combined into a single dictionary, mydict.dict using the command:

(cat /usr/dict/words cracklib.txt passwd.lst; /opt/bin/zcat *.Z *.gz) | sort -u > mydict.dict

Bibliography

Acheson, Steve, John Green and Hal Pomeranz. Topics in UNIX Security. Track 6 – Securing UNIX Systems 6.3. The SANS Institute, 2002.

Carnegie Mellon Software Engineering Institute Cert Coordination Center. Cert CC Vulnerability Note VU#683673. 21 March 2003 <http://www.kb.cert.org/vuls/id/683673 >.

"Cerias dictionary collection." 13 Feb. 2003. <ftp://ftp.cerias.purdue.edu/pub/dict>.

Christensen, Steven M. and Associates. Freeware for Solaris. 4 March, 2003 <http://www.sunfreeware.com>.

CISscan. Version 1.3.0. 12 Feb. 2003 <http://www.cisecurity.com/>.

City of GIAC Technical Services. "FTP Server Account Request", 2002.

City of GIAC Systems and Network Administrators. Personal Interviews. February and March 2003.

"cracklib.txt" 13 Feb. 2003. <http://www.accessdata.com/downloads.htm>

Haprin, Geoff. A System Administrators Guide to Auditing. Short Topics in System Administration 6. Berkeley: The USENIX Association, 2000.

John the Ripper. Ver. 1.6 . 12 Feb. 2003 <http://www.openwall.com/john/>.

Miller, Todd. Sudo Prompt Buffer Overflow. 4 March, 2003 <http://www.courtesan.com/sudo/alerts/prompt.html>.

Milman, Miq. Personal Conversation. October 2000.

Miuccio, Bert. "New and Updated CIS Benchmarks." Online posting. 21 Mar. 2003 <cis@cisecurity.org>.

Moffat, Darren J, FOCUS on Sun:Solaris BSM Auditing, 11 March, 2003 <http://www.securityfocus.com/infocus/1362>.

Nmap. Ver. 3.00. 12 Feb. 2003 <http://www.sunfreeware.com>.

Noordergraf, Alex, et al. Enterprise Security: Solaris Operating Environment. Upper Saddle River, NJ: Sun Microsystems Press-Prentice Hall, 2002.

Patchdiag rev 1.25 ver. 1.0.4. 31 October, 2000 <http://sunsolve.sun.com/private-cgi/show.pl?target=resources/patchdiag>.

Pomeranz, Hal. Common Issues and Vulnerabilities in UNIX Security. Track 6 – Securing UNIX Systems 6.1. The SANS Institute, 2002.

---. Running UNIX Applications Securely. Track 6 – Securing UNIX Systems 6.4. The SANS Institute, 2002.

---. UNIX Practicum. Track 6 – Securing UNIX Systems 6.5. The SANS Institute, 2002.

---. UNIX Security Lab. Track 6 – Securing UNIX Systems 6.6. The SANS Institute, 2002.

---. UNIX Security Tools. Track 6 – Securing UNIX Systems 6.2. The SANS Institute, 2002.

SANS Institute, The. SANS/FBI Top 20 List, ver 3.22. 20 March, 2003 <http://www.sans.org/top20/top20.pdf>.

Sun Alerts Collection. Sun Microsystems. 25 March, 2003 <http://sunsolve.sun.com/priviate-cgi/search.pl> <http://sunsolve.sun.com/pub-cgi/search.pl?mode=results&origin=advanced&range=20&so=date&coll=fsallert&zone_32=category:security>.

Sun Microsystems. patchdiag.xref. 20 Mar 2003 <http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=patchdiag.xref&method=H>.

Sun Microsystems. Solaris 9 Reference Manual Collection, 2 April, 2003 <http://docs.sun.com/db/coll/40.7>

Sun Microsystems. Sun Blueprints Online – Scripts and Tools. 10 March 2003 <http://www.sun.com/solutions/blueprints/tools/>.

Sun Microsystems. What's New in the Solaris 9 Operating Environment? Santa Clara: Sun Microsystems, Inc., 2002. 3 March, 2003 <http://docs.sun.com/db/doc/806-5202/6je7shk4c?q=%22tcp+wrappers%22+solaris+9&a=view>.

Todd, Bob. TARA. Version 3.0.2. 12 Feb. 2003 <http://www-arc.com/tara/index.shtml>.

Weise, Joel and Charles R. Martin. "Developing a Security Policy." Sun BluePrints OnLine December 2001. 1 Feb. 2003 <http://www.sun.com/blueprints>.

Last Updated: October 23rd, 2017

Upcoming Training

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