Global Information Assurance Certification Paper

Executive Summary

Introduction

The Sales Dept. requested changes to their Unix server and this may present security risks to the company. This document outlines what security issues should be fixed and allows the Executive Committee to judge whether or not the change(s) presents an acceptable or unacceptable risk given the potential reward.

The security auditor will recommend non-intrusive changes for the System Administrators (SAs). The auditor will also identify for management and recommend courses of action for their review.

Server Purpose

The Server, *softdemo*, is used by the Sales Computing Support Team of GIAC Enterprises. This server is used to present demonstrations of our developed software to clientèle from within our corporate intranet. Each demo is unique therefore multiple configurations and installs of our different software packages are being housed on this single box (i.e. Not the way our software was designed).

Issue

GIAC is attempting to lure a large potential client. Many are involved in this project and it has Board of Directors visibility. The potential client requests that this demonstration take place not at any of our corporate sites, but at one of our sales partners' sites. The particular sales partner has a direct connection into our network presently. There is no firewall between us and them, however, access control lists (ACLs) on the connecting routers control which ports are accessable on existing servers, sitting on that specific network. Given the rush, the GIAC network team requests the SAs to control port access on the host, rather than they. The Sales Teams, both of GIAC and our partner, have asked that not be implemented as they are unsure as to what ports may be needed. The network team is allowing one of the partner IP addresses to connect to the IP address that we establish on our subnet.

The server is scheduled for other intranet-based demos immediately prior to and following, this “partner demo”. This time constraint prevents the SA and Sales teams from reconfiguring the box to move solely to the partner network, and then moving it back with either a “re-reconfiguration” or a re-image. The box must be reconfigured to be dual-homed on both networks and run this way until all demos (both in-house & partner) are complete. Refer to Appendix A for a diagram.

Summary of Exploits

There are some “best practices” that should be implemented without user-impact. There are some fundamental changes that should be made that will be highly disruptive (i.e. Internally developed software should be redeveloped. e.g. Apache Jakarta Tomcat and OpenSSL, integral aspects of some of our software modules, are extremely out of date). Please see the Critical Issues and Recommendation section of this document. The non-intrusive changes alone are not sufficient to address the inherent insecurity of GIAC's developed software and the software to which it relies.

Table of Contents

Description of Use

This server functions to complement sales presentations by demonstrating internally developed software. The demos run from any location on the global intranet. In preparation for a large sales opportunity for GIAC Enterprises, the sales team wants to add this server to the GIAC Enterprises' Partner Subnet, a subnet which is unencumbered by firewalls. Security is normally handled by Access Control Lists (ACLs) on the switches and routers, but in this instance, there is no time for the network team to work this problem.

This system, *softdemo*, is a Sun Netra 1405 with dual 440MHz CPUs, 4GBs of RAM, 4 18GB drives, and dual 100BaseT interfaces. The disks are using *ufs* and no hardware or software RAID exists. It currently runs Solaris 8, kernel rev 26.

One of the 100BaseT interfaces, hme0, is on the primary network. The other 100BaseT interface, hme1, is currently not connected, but Sales desires to plug this interface into the partner subnet.

Our internally developed code requires a custom configured Apache web servers with Jakarta Tomcat. It runs on many different high numbered ports, not port 80. BEA Tuxedo is used to connect to Oracle databases. Users connect with telnet, ssh, X, rsh and/or ftp. The users NIS accounts have their home directories mounted via NFS. The users who connect with interactive logins (i.e. not Web or Oracle connections) are nearly all limited to PreSales Technical Support, Database administrators (DBAs), and System Administrators (SAs). The demos take place over the web ports.

Some local accounts exist to support the applications. Multiple users use these accounts. One account exists as an ftp gateway from another application on another host (i.e. That host runs an app that requires an account to ftp data to this server.) The server is being backed up by Veritas NetBackup.

Description of Audit Methodology

An initial assessment was made of the server with an interview of the owner and main interactive users, as well as the SAs. The security auditor has a NIS account which gives him access to this server as well. Research was gathered on the Internet to determine hardware details of this model of equipment. Root privilege was surrendered to the security auditor. This includes both sudo (sudo ALL) and the root password. A walk through of the facility a physical inspection of the server was conducted.

After these steps were conducted in order, recommendations were made for basic security enhancements. Certain procedures were conducted to check the existing security of the server prior to any enhancements. At the time of the audit, there was no reason to suspect the server had been compromised, but this was conducted as a precautionary measure.

The Sun supplied OS utilities which were used, were verified against Sun's site using MD5 checksums. Sun SRS NetConnect was installed for patch management and some minimal system monitoring.

A verification of best practices was completed. Many of these best practices are defined in the SANS Institute 2003 Unix Practicum. In addition, a manual check of the Unix component of the SANS.org Top 20 Vulnerabilities. And finally, an audit tool from The Center for Internet Security was used.

Detailed Analysis

Initial Binary Verification

If this machine was suspected of already being compromised, a check of the binaries would have been done initially. In this case, a subsequent check was performed for completeness. Conceptually, the procedure is: 1) generate MD5 checksums for the binaries. 2) Verify checksums against Sun's checksum database.

Since home directories are mounted from a central location, the following was downloaded on a different Solaris server: http://sunsolve.sun.com/md5/md5.tar.Z[1] The file was uncompressed and untarred ("`uncompress md5.tar.Z ; tar -Xbpf md5.tar`"). The `md5-sparc` binary was then available on *softdemo*. The following files were md5 checked: `awk, cat, crontab, df, eeprom, egrep, find, format, grep, ifconfig, inetd, less, ls, mount, more, ndd, netstat, nslookup, prtdiag, rlogin, showmount, showrev, telnet, uname, xargs, ypcat, ypwhich, in.telnet, in.rlogind, in.rexecd, in.rshd, in.ftpd`

See Appendix B for detail on how the MD5 checksums were generated. With the MD5 checksums, these were pasted into Sun's SunSolve fingerprints database. See Appendix C. The output for the first few examples is shown in Appendix D. All of the MD5 checksums displayed were validated through this process. Nothing but time precludes us from testing other Sun provided binaries. sshd was not checked as that is known to be compiled in-house and would not match any of Sun's file fingerprints.

Hardware

The Sun Netra 1405, *softdemo*, as previously mentioned, has 4 internal identically sized 18GB disks in a JBOD (Just a Bunch Of Disks, i.e. No RAID) configuration. The 4 internal drives are verified by visual inspection (no external drives) and a `df -k` & `format` (the latter as root). See Appendix E for more detail.

`df -k` reveals that the mounted partitions are all from Controller 0 (i.e. `/dev/dsk/c0*`). The following shows that they are all on the device path (assuming that `/usr/bin` is in the PATH):

```
df -k |  grep /dev/dsk/c | awk '{print $1}' | xargs ls -l
```

Sun, in the past, published hard copy documents known as "Just the Facts" which provides detailed information of their hardware in a nice summary format. Sun (USA) didn't publish these online, but old copies can be found at Univ of Alberta's SunSite[2]. It is unknown as to whether Sun still publishes these for their current new hardware. The Just the Facts document for the Netra 1405 tells us that this is not only fully populated with disk, but also RAM.[3]

The operating system disk should be mirrored and the data disks should be RAID 5, at a minimum. This would require an external disk pack with at least 2 more disks, connection to a SAN, or an assessment that the disks and partitions could be combined (i.e. Adequate freespace would be available). This would also require appropriate RAID software, either Solstice DiskSuite from Sun or Veritas VolumeManager. If one of the disks were damaged, regardless of whether this takes place by a security event, denial of service would result.

Operating System

The system is running Solaris 8 (SunOS 5.8) and kernel rev 26 (108528-26). This is reflected by the "`uname -X`" output (see Appendix E). Kernel Patch 108528-29 is current. One can gather this data from Sun's SunSolve Patch Support Portal site[4].

After interviewing the System Administrators, the company patch policy is never to be more than 6 months out of date with OS patches. The intention is that patching will take place in a rolling fashion among the company's servers (development servers at the beginning of the cycle; production servers at the end of the cycle). Patch bundles are applied, as opposed to individual patches. The patch bundles are tracked by date and/or the Solaris kernel patch revision. The application administrators have no such policy for the application software.

At the request of the security auditor, Sun's SRS NetConnect[5] was installed. SRS NetConnect provides system monitoring, hardware failure monitoring and notification, trend reporting, availability reporting, and configuration & patch reporting. The latter was the main motivation for installing this product. Data Transfer is encrypted. The inherent risk is that system information is transferred to a 3rd party, Sun, and one hopes that the information is not at risk (i.e. Inadvertently made available by Sun). NetConnect requires that Sun Explorer[6] be installed. Sun Explorer gathers much system data (e.g. Will do a "`showrev -p`" to gather patch information). Explorer will save this information locally on the server. NetConnect will upload portions of this data for use by Sun, in the event one has hardware support, and by one's company (accounts which the admin creates).

After running NetConnect, NetConnect identified *softdemo* as needing the following patches to address security issues: 113685-05, 113687-01, 114802-02, 115797-01, 116445-01, 116610-01, 117000-05, 111095-15, 113652-03, 116602-01, 114146-01. See the 4 screenshots in Appendix F.

A Google[7] search of the Internet for the Sun patch report turned up the following information regarding security patches:

```
113685-05 * SunOS 5.8: logindmux/ptsl/ms/bufmod/llc1/kb/zs/zsh/ptem
patch
113652-03 * SunOS 5.8: Supplemental Kernel Update Patch for 108528-17
113687-01 * SunOS 5.8: /kernel/misc/kbtrans patch
114146-01 * SunOS 5.8: Supplemental Kernel Update Patch for 108528-16
114802-02 * SunOS 5.8: Patch for assembler
115797-01 * CDE 1.4: dtspcd Patch
*=indicates if a security patch is not listed in the Recommended Patch
List because the patch is more application dependent, or the patch has
not been determined to be a Sun (SM) Alert patch.[8]
```

Also from that same document these were listed as "Recommended Patches" (no explicit word on security in the heading):

```
111095-15   SAN 4.4: fctl/fp/fcp/usoc driver patch
116455-01   SunOS 5.8: Solaris sadmind default security level
116602-01   SunOS 5.8: /sbin/uadmin and /sbin/hostconfig patch
116610-01   SunOS 5.8: audit_warn uses /usr/ucb/mail and writes to the
console
```

The following is described as a patch containing a security fix (and the current 5th revision can be assumed to at least have the same criticality as the 3rd).

```
117000-03   SunOS 5.8: Kernel Patch
```

This last patch, when reviewing the patch summary[9], seems to indicate there may be some denial of service by causing panics. This last patch also requires a later kernel rev (108528-29). Due to this, the latest Solaris 8 Recommended Bundle should be installed. This will address all but the SAN driver patch (111095-15), the Supplemental Kernel Update patches (113652-03 & 114146-01), and `uadmin`/`hostconfig` patch (116602-01).

The SAN driver patch is irrelevant as there are no SAN devices connected (this might change if the recommendation to add more drives is followed; and the drives turn out to be LUNs off a SAN instead).

113652 is irrelevant as it deals with UltraSPARC III chips. This system runs an UltraSPARC II.

114146 is irrelevant and should NOT be installed. This is only for kernel patch rev 108528-16. The patch report states: "**Patches which conflict with this patch:** 108528-17 (or newer)".[10]

To review, the latest Recommended Bundle should be applied. However, this may introduce issues with the existing applications (i.e. Are they compatible?).

"Any patch you add might impact the function of your system/applications."[11]

Networking

There area two 100BaseT network interfaces on this server identified by hme from the `prtdiag`. `ifconfig` shows that only one is active and that IPv6 is not setup. IPv6 is not currently used in this environment, but other configurations have been done to prepare for the day that changes are made in this environment (e.g. `/etc/inetd.conf` has `tcp6` settings). The routing tables are straightforward, as illustrated by "`netstat -rn`". There are no static routes and if packets are destined for something other than the existing subnet, they are sent to the subnet's gateway (10.2.2.1). There is no surprise that `/etc/notrouter` does not exist as this is irrelevant since the second hme interface is not active. Likewise, the prom has a setting that keeps the mac address constant for both interfaces. See Appendix G, Section 1.

The network driver settings for `/dev/arp`, `/dev/icmp`, `/dev/ip`, and `/dev/tcp`. are set to the defaults. The Sun Blueprint, Solaris Operating Environment Network Settings for Security,[12] has many recommendations that should be followed, altering the default environment. The algorithm used for generating TCP sequence numbers is set to 1, this is set by the `TCP_STRONG_ISS` entry in `/etc/default/inetinit` which is called by `/etc/rc2.d/S69inet`. See Appendix G, Section 2.

From `/etc/nsswitch.conf`, one can see the search order for name resolution is files, then DNS. And `/etc/resolv.conf` lists one too many DNS servers (illustrated by the "`nameserver`" lines.) and the 4th entry is not unique. See Appendix G, Section 3 for details. According to Sun,the maximum number of DNS servers is limited to the variable MAXNS.[13] Older Solaris versions set MAXNS to 3 in the `resolv.h`. I have not seen any documentation that this has changed. Any excess beyond MAXNS is ignored. The last entry should be removed for cleanliness.

Appendix G, Sections 4, 5 and 6 adds context to what follows: This server is a part of a NIS domain, so there will be rpc traffic. "`rpcinfo -p`" shows that the portmapper is running (`rpcbind`), as is `ypbind`. `sadmind` and `rstatd` are running, as is the NFS lock manager (`nlockmgr`). The following maps are pulled from the NIS master: password_compat, group, printers.conf, printers, netgroup and automount. (illustrated by "`egrep '^[^#]+nis( |$)' /etc/nsswitch.conf`". The NIS master is defined in `/var/yp/bind/nar/ypservers` and the servers are listed in `/etc/hosts`.

Looking at the `/etc/dfs/dfstab` and "`showmount -e`", we can see that this server is not being used for NFS. Looking at the `/etc/inetd.conf`, we can see that tcpwrappers are not being used. The following services are available via inetd: `telnet`, `name`, `shell`, `login`, `exec`, `comsat`, `sadmind` (100232/10 udp), `rstatd`, `fs`, `gssd` (100234/1 ticotsord), `amisrv` (100146/1 & 100147/1

ticotsord), dtspc, rpc.cmsd (100068/2-5), bpcd, vnetd, vopied, bpjava-msvc (the last 4 are relevant to Veritas NetBackup). We know from our interviews that users do ftp into this box. /etc/shells does not exist. /etc/ftpusers does not include root. Root should be included to prevent admins from transferring the root password in clear text. /etc/shells should exist so that we can give omit shells that are given to process accounts (like uucp). This info is found in the remaining sections of Appendix G.

Accounts

As our investigation of nsswitch.conf showed, passwords and groups are being using NIS. The following accounts exist in /etc/passwd with no user affiliation and non-locked password entries in /etc/shadow: tuxadmin, ftpsoftdemo, srsnetc. The demo accounts that were established were: demoone, demotwo, demothree...demosix. These have *NP* in their password field of /etc/shadow. Anyone with a NIS account can login to this server since there are no netgroup restrictions.

File Systems

`The general rules we want to follow are: File systems shall either be mounted "nosuid" or "ro".'[14] There is no anonymous FTP server, so with the exception of "/", we can follow this guideline ("Solaris nosuid implies nodev – devices won't work in these filesystems."[15] /devices need read-write and "no nodev". /devices needs to reside on "/"). Also, "/" should be mounted with the *ufs* logging option to prevent someone to try to get root by continually crashing the box.

Currently, none of the filesystems specified in /etc/vfstab are nosuid and "/" is not setup with logging. This should be corrected. The more complex issue is how to deal with NIS and the automounter. By grepping for "auto" in /etc/nsswitch.conf, we can determine search order of the automounter, and see that we do use NIS for the automounter. See Appendix H, section 1 for examples of everything so far in this paragraph.

Because we are dealing with direct and indirect automount maps, we will see some file systems that are *set UID* and some file systems that are *no set UID.* However, not all the filesystems defined in the automount maps are necessarily exported to this server. (They may introduce vulnerabilities, justified or otherwise for other servers, but that is out of the scope of this review). Likewise, the NFS clients defined in the exports file (or dfstab for Solaris NFS servers), might be defined using host netgroups, likely also defined in NIS. Ultimately, security may be tighter than on first examination of the NFS filesystems, but it will also be convoluted in the details.

Section 2 of Appendix H, illustrates the four indirect maps that are being exported nosuid. These can now be ignored. Section 3 illustrates the two indirect maps that are being exported suid. These should be exported read-only

as well. These are issues for the NFS servers, not *softdemo*. Section 3 further goes on by showing the output of "`showmount -e <NFS Server name>`". All of these respond by exports to snj_all, this is a NIS netgroup. At the end of section 3, a "`ypcat -k netgroup | grep softdemo`" reveals that *softdemo* is not listed in any of the netgroups as no output lines are returned, therefore, none of these file systems can be exploited by *softdemo* – though attention needs to be paid to this because of other boxes!

Section 4 breaks down the NIS indirect maps that were not defined suid or nosuid. Then we look at the individual lines. A quick explanation of the command line used:

```
ypcat -k auto.master | awk ' ! /suid/ {print $2}' | xargs ypcat -k
```

"`ypcat -k auto.master`" prints out all the automount maps at the top level. "`awk ' ! /suid/ {print $2}' `" removes anything that defines a suid or nosuid option and then prints the 2nd field – the name of the maps. "`xargs ypcat -k`" takes the names of the maps and uses that in `ypcat -k`

Again, `showmount` illuminates us to the issues. *Nfsserv4* is exporting /vol/vol0/release to many hosts defined in NIS netgroups (this is not a problem since *softdemo* is not defined in any netgroups), individual hosts, and the entire 10.2.2.* subnet. *Softdemo*'s IP address is 10.2.2.69 (see Appendix G, Section 1). So, this export needs to be changed to read-only or nosuid. Likewise, *nfsserv5* is exporting /home/test to the subnet. *Nfsserv6*'s sd-home export is okay as the exports are explicit. /vegas/home is also exported to the subnet; note: this export is listed because the filter was only looking for exports ending in "home". This export was defined as nosuid. Likewise, the *nfsserv6*:/vol/vol0/ti export was specifically listed as suid. This is a system administrator mount that is used for suid files. The subnet export should be removed however and defined explicitly. The benefit of doing this poor filter, `showmount -e nfsserv6 | egrep 'home[^-/a-zA-Z]'`, is that is caught that *nfsserv6* was exporting one file system (/vol/vol0/dev-home) to everyone.

The Center for Internet Security (CIS) tool discovered many odd Set UID and Set GID files in reference to Websphere MQ. All were of the form: `Negative: 6.8 Non-standard <SGID|SUID> program /var/sadm/pkg/mqm-upd03/save/opt/mqm/bin/<filename>` An `ls` shows that all of these are owned by the mqm user and mqm group. Regardless, these are a result of the pkgadd of mqm-upd03 and these files are saved as a backup. They should be tarred up and dropped in the `/var/sadm/pkg/mqm-upd03/save` dir and then the other files removed. See Appendix I.

If the CIS tool, cis-scan, isn't on a machine, one could do it by hand: "`find / \(-perm 4000 -o -perm -2000\) -ls`", a "`find / \(-nouser -o -nogroup \) -ls`" would be of value as well. The latter will identify files who do not have an associated username or groupname. This usually occurs when

someone untars (as root, preserving the UIDs and GIDs) a software package.

Operating System Vulnerabilities

Startup Scripts

Solaris provides a handful of startup files that are not needed. However, removing them is not sufficient. When patches are applied, if there was a patch to the particular file (for example: sendmail), then all the files that were removed are restored with the updates and started at the next relevant use of `init`. To solve this problem, move the files to "`orig.<filename>`" and then copy the script, "`rc-script-check.sh`" which can be found in the Appendix J to `/etc/init.d/`. Change permissions to 744 owned by root. This will allow root to run it and others to read it. If one wants others to run it, it could be made 755. Then create a symbolic link, preferably `S99rc-script-check.sh`, in `/etc/rc3.d` (default run level – found by "`grep def /etc/inittab`" and looking at the 2nd field). This script will monitor, again at the relevant init level, the `/etc/rc.\.d` directories to verify that the original file names of the files moved have not been restored (i.e. If after a patch, the links are restored). If a link has been restored, then the script will mail root. A `/.forward` file exists to mail root's e-mail to the SA team.

The following scripts are ones that should be moved 1) in `rc2.d`: `S30sysid.net`; `S71sysid.sys`; `S72autoinstall`; `S76nscd`; `S85power`; `S88sendmail`; `S99dtlogin` 2) in `rc3.d`: `S15nfs.server`; `S76snmpdx`. The first 3 deal with scripts needed for automatic OS installs; `S76nscd` loads the Name Server Cache Daemon. On this server, there will be little volume for name resolution and usernames. As a result, the value of this process is minimal. Suggestion is to turn it off.

`S85power` deals with power management. This has little value on servers that are on virtually 24x7 (i.e. Not a workstation). In GIAC's situation, the server is used from many different timezones around the globe and is essentially 24x7. As a result, the process should be disabled.

`S88sendmail` turns on the sendmail daemon so that it listens on port 25. This server does not need to receive mail from external sources, so sendmail should be turned off. The sendmail binary will still be called to send mail externally. `S15nfs.server` will attempt to turn on the NFS server if `/etc/dfs/dfstab` exists and has relevant content (i.e. Non-blank & non-commented lines). By removing `S15nfs.server`, if someone inadvertently or maliciously creates files here, the NFS server would also have to be started. `S76snmpdx` turns on the SNMP agent. There is no reason for us to run this.

`S99dtlogin` is for serving X and CDE sessions. This is not needed. The few users who use X on this machine should not be using it for window management. The users have Hummingbird eXceed and that allows for serving X Window

management on their PCs.

Some would suggest also disabling `S71rpc`, found in `/etc/rc2.d`. `S71rpc` needs to be run, because we need to bind to NIS. If a reboot is not in the plans (possibly it is known that OS patching will take place), then the previously listed processes should be stopped.

Networking Vulnerabilities

A startup script following `/etc/rc2.d/S69inet` should be created to alter the default setup to the network startup scripts. It is possible that we could alter this script, but again it would be vulnerable to subsequent alteration, if Sun patches this script; so a new one alphabetically following the `S69inet` should be written. I suggest that it be named `after-inet.sh` and be placed in `/etc/init.d` and owned by root with permissions of 744 with a symbolic link to `/etc/rc2.d/S70after-inet.sh`

Many changes need to be made to the defaults (these will be found in the `after-inet.sh` script found in Appendix K). To reduce vulnerability and impact to SYN floods, `/dev/tcp tcp_conn_req_max_q0` and `/dev/tcp tcp_ip_abort_cinterval` need to be changed; the former raised, the latter reduced. This Solaris 8 box would not be taken offline by a SYN flood as Solaris (2.6 and after) drops incomplete messages first anyway, but this will reduce the impact.

To limit information provided to hackers about systems on the network, the following should be implemented: turn off the following settings in the `/dev/ip` driver: `ip_respond_to_address_mask_broadcast`, `ip_respond_to_timestamp_broadcast`, `ip_respond_to_timestamp`. These are services not typically needed (e.g. Time is usually spread via NTP rather than the deprecated timestamp broadcasts). Also, there is no need for this server (or any server) to use ip_respond_to_address_mask_broadcast. The routers typically perform this function. These settings will help prevent “smurf” attacks (i.e. Amplification of network packets to bring down certain devices). The `ip_forward_directed_broadcasts` setting should also be set to “0” once the server is dual-homed.

Other settings for the `/dev/ip` driver are for ICMP. To prevent being redirected, `ip_ignore_redirects` should be set to 1 (true), while `ip_send_redirects` should be set to 0. The router on the subnet should be handling all the IP redirection. There is no need to provide this information, and no need to listen to other devices for the router's information.

If this server handled many more unique IPs, I would not make the following change due to additional network traffic. However, after discussing with the application admins how this server is used, I find it appropriate to alter the ARP settings (i.e. Making the arp requests more frequent). `arp_cleanup_interval` and `ip_ire_arp_interval` should be scaled

downward to every minute (60000 milliseconds) from 5 minutes and 20 minutes, respectively.

Because there is the intent of multi-homing this server, `/etc/notrouter` should be created which will prevent the server from routing between interfaces (i.e. Behaving as a router). This will be initiated at boot time. For redundancy, the "`/dev/ip ipforwarding 0`" should just be added to this script where we are making changes. And "`eeprom local-mac-address\? = true`" should be run, so that the default behavior of using the same network MAC address for all interfaces is turned off. Also, source routing should be turned off. To prevent others from using this server to route packets between network interfaces (i.e. Bypassing the router), the `/dev/ip` setting of `ip_forward_src_routed` needs to be turned off.

TCP Sequence Number Generation is set to 1 – random variance in increments of the TCP sequences. This should be strengthen to the 2 which generates a unique number upon every connection identifier. This is set in `/etc/default/inetinit`. But, can also be forced in the `/dev/tcp` driver. Both should be changed. The parameters for the driver is `tcp_strong_iss`. This can be seen in section 2 of Appendix G.

Within the `/etc/inetd.conf`, the following should be turned off: `name`, `comsat`, `talk`, `sadmind`, `amiserv`, `rpc.cmsd`, `dtspcd`. The `name` entry calling `in.tnamed` is deprecated in favor of BIND. This should no longer be used. `comsat` is used for the mail `biff` program. People will not be watching for e-mail on this server, this service should be disabled. talk also will not be needed on this server. The UDP services, `sadmind` and `amiserv`, can all be disabled. We are not using `sadmin` for administration. `amiserv` is a part of smartcard support, this is not needed. The `rpc.cmsd` entry relates to the CDE Calendar manager. This is not needed on this server. Likewise, the CDE subprocess control daemon which allows *remote* launching and executing of commands, `dtspcd`, should be disabled. `gssd` is a question as it would be preferable to turn this off since there is no NFS. However, it is unknown if our internally developed software would use this service to verify users.[16]

Also, inetd should be started with the "`-t`" flag which will cause it to log to syslog. Appendix L shows that it is not using "`-t`" currently.

Miscellaneous

The `CONSOLE` variable in `/etc/default/login` was commented out. The comment should be removed forcing root to only login on the system console from the console server. In `/etc/system`, "`set nfssrv: nfs_portman = 1`" should be added. In the event that this server is ever configured to be an NFS server, it will restrict the port connectivity to secure ports (i.e. Under 1024).

Another change to the `/etc/system` file would be to add

"`noexec_user_stack = 1`" and "`noexec_user_stack_log = 1`". This will prevent many buffer overflows on the user stack (the former line) and will log any attempts (the latter). This will not prevent the less known heap stack overflows.[17] The change made will be only active for future processes (it is only good on sun4u -- i.e. Ultra -- class servers). Also, it is only good for 32-bit programs as 64-bit are standard no-execute.[18] "`egrep 'nfs|noexec' /etc/system`" returns nothing, proving that these are not currently in this file.

Configuration Vulnerabilities

3rd Party Software Risks

We are not sure if all the software that Sales intends to demo is secure. They have identified ports 32444 & 32445 which will be defined via IP subnet by the software. These are not the ports that the Web server runs on. However, we are not sure that a Denial of Service can not be attempted against one of the ports on the business partner subnet.

Apache Tomcat is out of date (4.0.3) and known to be vulnerable. This needs to be addressed. It is unknown if we can restrict access to the port to which it listens. But more importantly, the version that is installed on the server is known to be vulnerable and to upgrade requires interaction with a new Java Server Pages or Java Servlet which will affect the existing code for which GIAC's software was written. http://jakarta.apache.org/tomcat/index.html[19] states that 4.0.6 is the last 4.0.x version. 4.1.30 is current, as is 5.0.24. In theory, it may be possible to just upgrade to 4.0.6, but this issue needs attention. Likewise, for the sake of the demonstrations, Apache HTTPd runs on a "non-standard" port for every individual sales environment and should get an upgrade to 1.3.29 See Appendix M.

This software also relies on OpenSSL. The OpenSSL version 0.9.6g is also in need of upgrades. According to http://www.openssl.org,[20] OpenSSL's current versions are 0.9.7d (where 0.9.7c is the latest secure version, "d" is a bug fix) and 0.9.6m.

Identification and Protection of Sensitive Data

Accounts / User Authentication

Far too many accounts have access to this server. This can be easily simplified by creating a NIS netgroup with a list of allowed users to this server and then appending `/bin/false` for the shell to the last line (`+::::::`) to the `/etc/passwd` file. A NIS user netgroup entry would look like: `SOFTDEMO-USERS (,johndoe,) (,janedoe,)` The entry in the password file would look like: `+@SOFTDEMO-USERS:x::::::` and the corresponding entry in `/etc/shadow` would be: `+SOFTDEMO-USERS:::::::::` It is important to remember that after creating the NIS `netgroup` entry, that the file will have to be pushed. On the NIS master, the location of the source `netgroup` file will be

defined in `/var/yp/Makefile`. After editing that file, change directories back to the `/var/yp` and do a `make`. This will have to be done as root (or with `sudo`).

This procedure will limit access to this server to a handful of users as opposed to the over 1000 that are in the password file. As a result, this will prevent unnecessary access to this server.

Password aging is not supported in the Sun NIS environment. One must move to NIS+ or LDAP. Due to dependencies of legacy servers in this NIS environment, a move to LDAP has not been attempted. LDAP would provide a better authentication environment for this server.

Sensitive Data Across Networks

In the past all of the data has passed over internal-only networks. The Sales Dept of GIAC Enterprises proposes that this changes. Users from foreign networks will only be accessing non-privileged ports for the middleware and web applications. If these ports are made secure, then the only concern is what takes place over on the partner network (and within the partner's network). The data will no doubt be vulnerable to “shoulder surfing” (person(s) peering over the shoulders of the user at the keyboard). Because not all of the applications data delivery methods are using encryption, the data is vulnerable to sniffing as well. These are application issues that need to be solved.

In addition, since the partners will be using NAT, there is no way for GIAC to necessarily guarantee the data is going to the intended desktop. The NATted IP on the partner site could be spoofed from another machine on the partners network.

Since only the presentation itself (i.e. To Whom the Sales Dept is selling) is the only pertinent information that is flowing, the risk should be minimal (minimal, but not zero!).

Access Control

Logins to “shared accounts” is being controlled with `sudo`. Group accounts like `demoone` through `demosix` have no usable password, but require that allowed users `sudo su - <account name>`. Backdoors need to be monitored (i.e. `~username/.rhosts`). Further interviews with the application admins are needed to see if these group accounts need to run cron jobs. If not, these accounts should be placed in the `/etc/cron.d/cron.deny` and `/etc/cron.d/at.deny` files.

Accounts which should be deleted from `/etc/passwd` & `/etc/shadow` are uucp, nuucp, listen, and nobody4. UUCP is not used on the box. Nobody4 refers to the legacy SunOS 4 nobody account. Listen is for the network listener.

For FTP access, root should be added to `/etc/ftpusers` to prevent any ftps

as root. Also, `/etc/shells` should exist and be populated with reasonable shells (e.g. `/bin/sh`, `/usr/bin/sh`, `/bin/ksh`, `/usr/bin/ksh`, `/bin/csh`, `/bin,tcsh` ,etc.). It has been recommended here that users not allowed on the server or for odd group accounts, `/bin/false` be used as their shell. This should not be found in `/etc/shells`.

Backup Policies/Disaster Recovery/Physical security

Backups currently take place over the primary interface (hme0). This should be done across the secondary interface (hme1) connected to one of the backup VLANs. However, with the intention to dual home this server, backups can continue to proceed over the hme0 interface connected to the private intranet. Ideally, a separate interface should be installed. Many of the servers in this location have a primary interface and a separate interface for backups. It is unknown why this server was not setup this way initially.

In the event of a site disaster, *softdemo* is on the "lowest priority list" as loss of this server will only impact potential sales presentations which can either be rescheduled or the presentations can proceed without the interactive demo component. In the event of loss of the server, the server is on next day service for maintenance.

The backup software being used is Veritas NetBackup 4.5. On the backup server, the `bpcllist` command revealed that only one class was defined for this server. An investigation of the exclude list, revealed one directory `/db_backup` that ought to be backed up with the DB backups class. This was immediately remedied. By taking the exclude list and doing an `ls` and then tossing out all the non-existent directories (sending STDERR to /dev/null), made this an easy task (`cat exclude_list.UNIX_OS | xargs -i{} ls -ld {} 2> /dev/null`). The `/home` directory should also be a part of a class, except for the fact that an `ls` shows that it is empty. All of this can be seen in Appendix N.

Regarding physical security, *softdemo* and the backup server are located in a C2 certified site. All doors are locked and require user verification prior to entry. Many video cameras exist, not only to monitor the entrances and exits, but nearly all the floor space of the data center is recorded. Escorts are required for those not on the authorized list. *Softdemo* is in a cabinet which can be locked at both the front and back doors. The backup server is not in a lockable cabinet, the back door of the cabinet is screwed shut, but can be opened with a screwdriver. The cabinet housing *softdemo* should be locked to prevent rogue consoles being applied to the server. The backup server should be relocated to a lockable cabinet. Also, the console is connected to a console server which also should be behind locked cabinet doors (both front and back). As a result of having serial consoles, there is no need to modify `/etc/default/kbd` to disable the L1-A break sequence. The weight of the cabinets would prevent anyone from entering from under the floor tiles, likewise, the holes with existing cables are far to narrow for someone to get their hand through.

Some of the servers have a DB25 to RJ45 connectors (making it simple to bypass the console server, if one has access to the back of the machine). This one does not. It is on a DB25-DB25 cable to the console server.

SANS Top 10 Unix vulnerabilities

"The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization"[21]. SANS publishes "The Twenty Most Critical Internet Security Vulnerabilities". Half of these are Unix related. This list was last revised October 8, 2003. The list can be found at http://www.sans.org/top20 [22]

U1 BIND Domain Name System

This vulnerability refers to CERT advisory CA-2002-19 [CERT advisories come from the CERT® Coordination Center based at Carnegie Mellon University. See http://www.cert.org.[23] The vendor supported information in the CERT refers to Sun Alert 46042[24] which is a document which refers to a buffer overflow in the DNS resolver library. Patch 109326-09 solves this problem. However, in reading the revisions for patch 109326, revision 14 is current. Revision 10 is the last revision that deals with the DNS clients. Revision 13 deals with a Negative Cache Poison Attack, but this is only relevant to DNS servers, which *softdemo* is not. *Softdemo* is running revision 10 which is sufficient for this server. It would be desirable, not essential, to patch the DNS resolver library even further than rev 10, but this will introduce other patch dependencies (libnsl patch 108993-27 which requires 8 other patches). If the Recommended Solaris 8 Bundle is applied this will be made current. As of this writing the last bundle, is dated April 26, 2004. For the current bundle, see http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=patch&doc=8_Recommended.README[25]
To determine the current patch revision, the following command was used:

```
$ showrev -p | awk '/^Patch: 109326/ {print $0}' | sort | tail -1
```

```
Patch: 109326-10 Obsoletes: 110514-01 Requires:  Incompatibles:
Packages: SUNWcsu, SUNWcsr, SUNWcslx, SUNWcsl, SUNWhea, SUNWarc,
SUNWarcx, SUNWcstl, SUNWcstlx
```

U2 Remote Procedure Calls (RPC)

The portmapper (Port 111) needs to be on for `ypbind` to work. However, `sadmind` should be disabled as this is not needed. `rstatd` is needed for monitoring. Ports here should be kept to a minimum. RPC exploits can bypass Intrusion Detection Systems[26], as a result, these RPC services should be blocked on the Partner Subnet at a minimum.

U3 Apache Web Server

There are many Web servers that are used for the internal demo applications and they are running Apache 1.3.27. The environments are such that they can bring up different web servers on different ports for the sake of their demos. See

Appendix M. Version 1.3.29 is current.[27] The security vulnerability for 1.3.28 is not relevant to our OS release, however mod_alias & mod_rewrite are vulnerable and the web server is configured with these modules. Both are vulnerable to buffer overflows. The Mitre Corporation documents these in the CVE lists:[28] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0542

The Web server may have interaction with Jakarta Tomcat 4.0.3 which is dated and has known security holes:

Denial of Service vulnerability:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0935
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0866
User spoofing:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0682
Unauthorized access:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1148
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1394

Whether there will be an online vulnerability or not, depends on whether the software module(s) GIAC Sales wishes to demonstrate will include the web server which utilizes Tomcat. However, since they may wish to do a demo other software to other clients, this could be an issue as this software port may be active. The Sales Department needs to detail all the different ports that they will have Apache running on and which will be using tomcat, so that we can filter accordingly. Conceivably these will be the ports that Apache is listening on, but not defined – i.e. 2 Listen port numbers will be set and the one that does not match the "Port" parameter, is likely to be the tomcat port. However, we do not know precisely what the users are doing.

U4 General UNIX Authentication Accounts with No Passwords or Weak Passwords

The NIS accounts are vulnerable. Part of this should be fixed with the netgroup restrictions in `/etc/passwd`. mentioned earlier. But, it is of note that by running an old version of Crack[29] many passwords for the users were found. "John the Ripper" would be a more contemporary password cracker than the Crack 5.0a version that was used.

Crack was previously compiled on Tru64 Unix 5.1 and this server is in the NIS domain. A copy of *softdemo*'s `/etc/passwd` and `/etc/shadow` were copied over to the auditor's home directory, this directory is also available on the Alpha server with Crack. The files were moved into a directory locally that is only readable by the auditor (and root). The encrypted passwords were extracted out of the copied `/etc/shadow` and replaced the place holder in copied `/etc/passwd`. (the accounts with "NP" in `/etc/shadow` were removed from both files). The file was then renamed `ypstuff`. This left the root account, 6 accounts needed for demos, 1 account needed for data transfer. A "`ypcat passwd >> ypstuff`" was also done. Crack was now run on ypstuff. See Appendix O.

A whopping 25% of passwords were cracked. These users were notified, but it is questionable as to whether they will change their password in a timely fashion. With this volume, we need to verify that management will backup written policy to lock *all* these accounts.

U5 Clear Text Services

With the minimal amount of use that is here (less than 20 users – 1/3 of which are SAs), we should be able to enforce a reduction of possibly all the clear text services like telnet except for ftp. The users should use SSH. There is another program that is being used on another host that needs to use ftp for data transfer. This account should be given a "fake shell" e.g. `/bin/true` with that shell being put in `/etc/shells`. This will limit the access to ftp. We should push the developers to change their automated transport mechanism. This is a hole and it needs to be watched.

U6 Sendmail

Sendmail is running on this box (with the "`-bd`" -- daemon -- flag), but there is no reason for it to be. The Sendmail daemon should be stopped and the startup file renamed in `/etc/rc2.d/S88sendmail` to `/etc/rc2.d/orig.S88sendmail`. The `rc-script-check.sh` (see Appendix J) should be installed. A root crontab file should be appended with the following information: "`5 * * * * /usr/lib/sendmail -q`". This, on 5 after the hour, will flush any mail that gets stuck in the mailqueue. Alternatively, the sendmail startup script could be changed to strip the "`-bd`" flag.

U7 Simple Network Management Protocol (SNMP)

SNMP was not running on this box, however, `/etc/rc3.d/S76snmpdx` exists. This file should be moved to `/etc/rc3.d/orig.S76snmpdx`, so that this does not start up in the future. The `rc-script-check.sh` (again Appendix J) should be installed.

U8 Secure Shell (SSH)

The SSH configs use "UseLogin yes" as opposed to "PermitRootLogin no"; the latter should be added. It is preferred to prevent root from logging in from other than the console. This is a Problem if `/etc/default/login` is not set to enforce this, which it currently is not.

There is also a problem with the configuration. One can not login with out generating keys and saving these in the proper locales of their home directories. So, if telnet is disabled, then only those who have configured SSH can login without the SAs' intervention.

Since the few interactive users have been known to use this server for CDE, some education needs to take place. They should be tunneling their X-traffic back to their PCs through SSH. Since they are using Hummingbird eXceed (which uses the rexec protocol), they will need to run something like puTTy

locally to establish the SSH tunnel.

U9 Misconfiguration of Enterprise Services NIS/NFS

There is a problem for NFS servers. This server does not serve NFS, but there are problems in the enterprise. As was previously mentioned, there are some world-mountable, read-write filesystems exported from some of the Enterprise's servers, that need to restrict what servers can mount the filesystems. Also, there needs to be further tightening on the exported filesystems which export to entire subnet ranges (i.e. Read only or no setuid exports).

U10 Open Secure Sockets Layer (SSL)

OpenSSL 0.9.7c is installed. Versions prior to 0.9.7a are vulnerable. However, this install requires `/opt/ssl/0.9.7c/lib` to be in one's LD_LIBRARY_PATH environment variable (e.g. If someone wants to run ssh). Without the lib, SSL type programs die. The lib should be linked or moved into something standard.

In addition, there are older versions of SSL that should be removed. "`/opt/openssl/bin/openssl version`" returns "`OpenSSL 0.9.6g 9 Aug 2002`". Also, tied to GIAC's software demos are 5 different installs of OpenSSL 0.9.6g (see Appendix M).

Outside the top 10.

Networking

TCPwrappers could be implemented in the `/etc/inetd.conf` To do this http://www.cert.org/security-improvement/implementations/i041.07.html[31] is a good instruction guide. However, this only addresses services which are defined in `/etc/inetd.conf`.

IP Filter[32], a host-based firewall, is being recommended instead to deal with the additional ports and due to the fact that the Networking Team is not prepared to implement strict firewall rules between this server and the partner subnet. TCPwrappers may be beneficial for additional logging and message banner activities.

IP Filter should be configured so that, any traffic that comes from the business partner's subnet is restricted to allowed ports. In this case, since the Sales Dept wants all ports open since they are unfamiliar with the inner workings of GIAC's software, it is recommended that we eliminate the known ports which might have issue. It is assumed that one could compile the software and do the necessary builds, so the configurations will be discussed: Ports to disable would be: 53 (DNS), 111 (the portmapper), 512-514 (rlogin, lpd, syslog), 2049 (rpc.nfsd), 32771-32779 (nfs ports). And for good behavior, at this point, we can block anything that is lower than 1024 which will catch some of the earlier stated ones. For a list of services & ports, see http://www.sans.org/top20/#ports[33]

In the IP Filter rulesets, anytime there is a rule with "quick", the rule takes place immediately. Otherwise, a flag is set as the rules are processed top-down. The last flag for a condition will be pass or block. For instance, "`block on hme1 from any to 200.140.150.69`"; followed by "`pass in on hme1 from 200.140.150.0/24 to 200.140.150.69`" would allow traffic from the 200.140.150.0 subnet. Also, rules such as "`pass in on lo0 from 127.0.0.1 to any`"; followed by "`block in on hme0 from 127.0.0.1 to any`" are designed to prevent misconfigured (malicious or otherwise) packets from hitting the server. In this case, 127.0.0.1 should only originate from the loopback interface (lo0) and not the ethernet interface, hme0. A recommended config file can be found in Appendix P.

Other issues: Complimentary servers

This server relies on other infrastructure servers. Those servers are mostly out of the context of this audit, but a brief overview is required.

The NIS master, console server, DNS master and slave, and Backup server: each of these needs to have rigorous security. By controlling any one of these, then *softdemo* could be compromised. Regarding physical security, each are located in the same C2-certified data center. The NIS master, the Backup server, the DNS master, and the DNS slave in addition to *softdemo*, are connected to the same serial console server.

The backup server should continue to be monitored for security. The backup architecture is outside the scope of the larger audit. The backup server is restricted by user authentication. Telnet should be restricted, but is not. SSH is installed, there is no reason that the System Admins and Backup Operators should not be using SSH-only.

The backup server is not in a lockable cabinet, the back door of the cabinet is screwed shut, but can be opened with a Phillips screwdriver. Also, the large Sun V880 server is too large for a single person to lift out, but its mounting drawer would allow someone to pull the unit mostly out of the cabinet from the front. Allowing someone access, though difficult, to the console connection in the rear of the unit. The backup server should be relocated to a front and rear lockable cabinet. The wiring to the current cabinet from the bottom is too difficult for someone to re-wire unless the rear panel to the cabinet is removed.

Being a backup server, this server can restore *softdemo's* data to another server if need be. The data that resides on this server is not necessarily of business critical importance, but would be important in the event of corporate espionage: competitors would see to whom we were trying to demo our software. Restores can only be performed by System Administrators (by use of the root password or sudo).

The backup server is on a separate NIS domain and has logins restricted to the

SAs & the backup operators by the use of netgroups.

Likewise, the NIS master for *softdemo* restricts logins to SAs only using netgroups. Changing the NIS maps requires the root password or sudo privileges – which is limited to the System Administrators. This server also should restrict logins to SSH (i.e. No telnet, no rlogin).

The console server is restricted to System Administrators by use of `/etc/passwd` & `/etc/shadow`. Logins can only be performed with SSH. This console server should be behind a locked cabinet door, both front and back. It is not. Someone with physical access could try to take control of the console server, then many servers are vulnerable (e.g. Someone could send a break to a Sun and drop it to the eprom, they could boot single user mode, and then take over the machine(s).)

The DNS master is limited to 2 users (root being one). `telnet`, `rlogin`, etc. should be turned off. SSH is installed. Changes to the DNS server would allow someone to spoof Internet Protocol names. This could have an adverse affect on the NFS servers that serve files to *softdemo*. (e.g. If someone had root on the DNS server, then they could change some of the known hostnames which has a suid export, so that the DNS server was the one with the suid export. Then backdoors and trojan horses could be easily distributed to *softdemo*).

The security of these servers should not be trivialized. There should be careful attention to these servers.

Critical issues and recommendations

The approach to the server's security has been lax as it has resided solely on the inside, giving a false sense of security. Passwords are weak; too many ports are open. There are many issues to address, some will be quick and some will require some time. Gene Spafford writes: "Security is more than the apparent lack of obvious buffer overflows or the ease with which an experienced programmer can apply a patch. It includes fundamental issues of design, including (for instance) separation of privilege, user interfaces, minimalism of function, fail-safe defaults, and freedom from deadlock."[34] This statement applies to this server as well, as there are design issues in addition to patch obsolescence and les than "best practices" regarding the Operating System.

What follows is a list of action items. "Risk of Implementation" (sometimes, identified solely as "Risk") and "Value" are associated with most of the items. The CIS-scan report (Appendix I) identifies more. This should be re-run after the issues below are addressed. The top ten issues in order of urgency will be identified accordingly below.

Completed

- Spot check of integrity of binaries using MD5 checksums and verification against Sun's database.

- Installation of SRS NetConnect (this has been done). Risk of Implementation: Dependant upon Sun to not make our system data available. Value: Patch management is simplified and basic event monitoring is provided.
- Addition of this server to appropriate Veritas NetBackup class, correcting an oversight.

Recommended Immediate Changes by the SAs (non-intrusive)

- <1> Login restrictions should be added into `/etc/passwd` (`+::::::::/bin/false`) and a netgroup created which would list all needed users. Risk of implementation: Some users may get locked out until they are properly identified. Some labor lost. Value: "Best practices" implementation (BPI). There are far too many accounts that have access to this server. Less than 2% of the accounts need access to this server. In addition, there are far too many crackable passwords.
- <2> IP Filter installation and configuration. Risk of implementation: Overly strict policy could prevent those who need legitimate access. Less strict policy may give false sense of security. Value: This will be the best tool to prevent unauthorized traffic from the business partner subnet. This will be the greatest protection, if configured properly, to unauthorized connections to ports.
- <4> Network Device Driver reconfiguration and Networking script, `after-inet.sh`, should be installed. Risk of implementation: Concerns exist regarding `ip_strict_dst_multihoming`. It is possible that this is needed for the internally developed software for instance, using lo0 (127.0.0.1). Value: This will prevent many networking vulnerabilities (smurfing, syn floods, etc.) Networking vulnerabilities exist, especially in dual-homed servers. It is important the networking devices be configured properly to provide resilience to the server and to protect other devices on the network.
- <8> Services reduction in `inetd.conf`. Risk: minimal. It is likely that many of the services are not needed. Value: increases security with minimal impact. There are vulnerabilities in services like `sadmind`. Granted, these could be remediated with OS patches, but the basic rule applies: If you don't need it, turn it off.
- <9> Unnecessary startup files should be removed and `rc-script-check.sh` installed. Risk: some services might be needed. Value: increases security at minimal impact. i.e. If users need X-windows, they have alternatives and those users just need to be educated. There are too many services (like sendmail) that are running and this will reduce them to limit the opportunities for exploits while allowing to the system to run cleaner with fewer processes.
- <10> Set UID and Set GID files need restriction. CIS scanner identified many setuid & setgid files in `/var/sadm/pkg/mqm-upd03` These files should be tarred up and left in the directory. The permissions will be preserved in the tarball. Risk: none. Value: follows "best practices" by removing setuid/setgid files from the server. The files are owned by mqm which should limit vulnerability to this user account. However, it is an administrative account, so

if this is exploited, then tracking will be very difficult.

- Local file systems should be mounted ro (/usr) and nosuid (all partitions specified in /etc/vfstab except for / and /usr). Risk: Some legitimate set UID programs may not function properly. These will need to be discovered and either relocated to / or the partitions will need to be opened up to set UID. Value: BPI
- Enable *ufs* logging on the root partition. Risk: Performance will be impacted on the file system. Value: Speeds reboots.
- Touch `/etc/notrouter`. Risk: none. Value: this will prevent the server from functioning as a router
- `inetd.conf` should include TCP wrappers. Risk: minimal. Value: minimal, if IP Filter is installed. IP Filter should be installed, in which case, TCP wrappers only aid in logging and providing banner messages.
- `/etc/system` should include `noexec_user_stack`, `noexec_user_stack_log`, and `nfssrv` entries. Risk: none. Value: BPI – security.
- Remove unnecessary accounts, e.g. uucp, etc. Risk: none. Value: BPI – minimizes environment.
- `/etc/ftpusers` should include root and ftpsoftdemo. Risk: adds a bit of workload to SAs, if they, in less than "best practices" use root ftp to transfer data. Value: BPI
- `/etc/shells` should include reasonable shells (and not `/bin/false` which is recommended for the account restrictions). Risk: none. Value: BPI
- Give ftpsoftdemo user the shell of `/bin/true` and add `/bin/true` to `/etc/shells`. Risk: none Value: Reduces risk from known ftp-only user.
- Populate `cron.deny` & `at.deny` with accounts known not to need cron (e.g. ftpsoftdemo). Risk: some users may be locked out of `cron` or `at` until they complain. Value: BPI
- Physical Security – lock cabinet doors on Console server cabinet and *softdemo* cabinet. Risk: A person with access to the data center floor, could attach their own console to this server and take it over. Value: minimal. Security of the data center is very strict. surveillance cameras can track most of the floor and access to the data center is logged in detail.
- Remove `/opt/openssl` (this is the older SA installed version, not the current or the ones that support the demos). Risk: none. Value: Will simplify install and not confuse those who need OpenSSL and are distracted by this directory as opposed to the more current install.
- Turn off Clear Text Services like `telnet`, `rlogin`, etc (not ftp, unless prepared to do so). ssh should be encouraged. Risk: Users may have to survive a learning curve. Value: BPI

Recommended Changes Requiring Management approval (intrusive)

- <3> The latest Solaris 8 Recommended patch bundle should be installed. Risk of implementation: There could be incompatibilities with software running on the box. Value: Several security holes will be filled (root holes, denial of service vulnerabilities). Patch maintenance is the first step in setting up a

secure environment.

- <5> Apache Jakarta Tomcat should be patched or the GIAC software module should be removed. Risks: GIAC's home grown software may not run following the upgrade given that there is a new Java Server Page revision. Value: This software version has many holes that can be exploited (root holes, denial of service). The changes recommended below in the remediation section, do not necessarily make the box secure, nor do we know if it is compatible with the custom code.
- <6> OpenSSL should be upgraded. The same software module relies on an older version of SSL. Risk of implementation: Again, the GIAC software might not run if the SSL version is made current. Value: Depending on how the SSL modules are used, this may be a vulnerability that can be exploited. The transactions which require the OpenSSL module are not secure.
- <7> Apache HTTPd server should be upgraded or the Apache modules as risk should be removed. It is possible that the insecure modules can be removed with no upgrade. Risk: The upgrade is minimal (1.3.27 to 1.3.29), but there may be some incompatibility issues Value: Prevents exploits allowing execution of arbitrary code.
- Web servers and Oracle configs should be configured to refer to the host itself by "*localhost*" and not "*softdemo*" due to multiple network interface issues. Risk: requires reconfiguration of software. Currently Sales Dept is not fully aware of how all this software works. Value: Things may break when dual-homing of the server is attempted, regardless.
- Clear Text Services (ftp) for the ftpsoftdemo account needs to be reworked. Risk: Requires development changes. Value: BPI
- There should be a plan to move to convert to LDAP from NIS. This will take extensive effort. Risk: Legacy NIS clients will have problems. Value: More security can be implemented.

Recommended Changes Requiring Management approval (procurement required)

- Disks need to be added for redundancy. RAID software and disk drives will need to be procured. Risk: If a single drive fails, this server will remain down until the hardware is serviced under contract and the data is restored from tape.
- Add a 3rd network interface. This will allow backup data to flow over a dedicated wire. Risk: networks can be compromised and data stolen off the wire. Value: This will segment the traffic to a separate network that prevents access from others.
- New Cabinet for backup server with lockable front and back doors are needed. Risk: An individual in the data center could get access to the backup server. Value: Minimal. Detailed records of who has access to the data center floor are kept and many cameras are watching the floor. Many of those who have full time access, operate our tape library and thus already have physical access (and temporary possession) of our backup tapes.

Outside of this server

- NFS issues: NFSserv4 and NFSserv5 are exporting file systems to the entire

10.2.2.* subnet. This should be refined. NFSserv6 is exporting a file system to the world. This should be refined. Risks: Without tighter control of the environment, a vulnerability remains to plant files on NFS file systems. Value: BPI

- NIS issues: A handful of NIS automount maps are not defining the mounts as nosuid. Risks/Value: same as NFS directly above.
- Passwords. 25% of NIS passwords were crackable in a very short amount of time. This is not necessarily relevant to this server (if netgroup restrictions are utilized), but this needs to be addressed for the NIS domain. Risks: Users can disguise themselves in others' accounts and use their permissions. Value: BPI

Unknown Risks

- The quality of security of 3rd party and internally developed applications is unknown. Apache httpd, Apache Jakarta Tomcat, and OpenSSL have already been addressed. Oracle & Tuxedo have not. There is also doubt about the quality of the configurations in dealing with multiple network interfaces and hostnames. This issue surfaced in interviews with the user community and wasn't factored into this review as this is an issue for the application administrators. Risk: The software will have runtime errors or actually open security holes. Value: none. This is an issue of concern.

Final Recommendation

Even with the non-intrusive changes, this box is not secure enough to drop onto a subnet without a firewall. Actually, the firewall is not the issue, the issue is that there is still 3rd party software on this server (Apache TomCat & OpenSSL) which is vulnerable. If the corresponding custom developed software were removed, these (Tomcat & OpenSSL – the Sales Dept installs) could be removed as well. As a result, not all of the software would be capable of being demonstrated, but a majority would be available. The auditor finds this an acceptable situation; it is unknown if the Sales Dept. feels likewise.

Remediation of the top ten vulnerabilities

1. Login restrictions: Refer to the section on Identification and Protection of Sensitive Data – Accounts / User Authentication.
2. IP Filter: It is assumed that one can download and compile the software. After it is compiled and properly installed, use Appendix P. as a configuration file if hme1 is activated under the assumptions listed.
3. Solaris 8 Recommended Patch bundle application: Download latest Solaris 8 (not x86) bundle from http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access [35] and place in a reasonable location.
   ```
   unzip Recommended_8.zip;cd Recommended_8 ;
   sudo ./install_cluster
   ```
4. Networking Device Drivers and Network script to reconfigure the networking devices: Copy Appendix K to `/etc/init.d/after-inet.sh` Then as

root,

```
chmod 755 /etc/init.d/after-inet.sh ; cd /etc/rc2.d ;
ln -s ../init.d/after-inet.sh S70after-inet.sh  ;
/etc/init.d/after-inet.sh
```

5. Apache Jakarta Tomcat freshening: Updating tomcat is no guarantee that the custom software will work or that they are secure. The latest 4.*.* version is 4.1.30.

```
cd /export/home/af
mkdir tomcat
```

< Download this and place it into `/export/home/af/tomcat` >

```
cd /export/home/af/ENV2/d4b12/SOP1.5/3p
mv tomcat tomcat.old ; ln -s /export/home/af/tomcat tomcat
cd /export/home/af/ENV3/SOP1.5/3p
mv tomcat tomcat.old ; ln -s /export/home/af/tomcat tomcat
cd /export/home/af/ENV4/SOP1.5/3p
mv tomcat tomcat.old ; ln -s /export/home/af/tomcat tomcat
cd /export/home/af/ENV5/SOP1.5/3p
mv tomcat tomcat.old ; ln -s /export/home/af/tomcat tomcat
cd /export/home/af/ENV6/SOP1.5/3p
mv tomcat tomcat.old ; ln -s /export/home/af/tomcat tomcat
cd /export/home/af/ENV7/SOP1.5/3p
mv tomcat tomcat.old ; ln -s /export/home/af/tomcat tomcat
```

6. OpenSSL freshening: Updating OpenSSL is no guarantee that the custom software will work. The old files are tarred to prevent reference to the old SSL libraries. Two symbolic links are created, in the event that 0.9.6m needs be installed. If so, the `/export/home/af/openssl` link can be removed and the software dropped into this location.

```
cd /export/home/af ; ln -s /opt/ssl/0.9.7c openssl
cd /export/home/af/ENV3/SOP1.5/3p
tar -cvf openssl.old.tar openssl ; rm -r openssl
ln -s ../../../openssl openssl
cd /export/home/af/ENV4/SOP1.5/3p
tar -cvf openssl.old.tar openssl ; rm -r openssl
ln -s ../../../openssl openssl
cd /export/home/af/ENV5/SOP1.5/3p
tar -cvf openssl.old.tar openssl ; rm -r openssl
ln -s ../../../openssl openssl
cd /export/home/af/ENV6/SOP1.5/3p
tar -cvf openssl.old.tar openssl ; rm -r openssl
ln -s ../../../openssl openssl
cd /export/home/af/ENV7/SOP1.5/3p
```

```
tar -cvf openssl.old.tar openssl ; rm -r openssl
ln -s ../../../openssl openssl
```

7. Apache HTTPD freshening: Option 1: Remove `mod_alias` and `mod_rewrite` from each `httpd.conf`, if the change is compatable with our internally developed applications. Option 2 (Best): Rebuild Apache and rename the `conf` and `ht-docs` directories and restore the previous directories. However, this implies that the conf files need to be double checked each time Apache is upgraded to ensure that syntax is still valid and modules aren't depricated. Option 3 (Below): This method is the quickest, provided Option 1 does not work. This proposed method is dangerous as, this method will become nearly impossible to maintain in the future: Download latest Apache 1.3.29. `uncompress`, `untar`, compile. After a new `httpd` is compiled, then drop into place replacing the existing `httpd`.

```
cd /export/home/af/apache/bin ; mv httpd httpd.1.3.27
```

< copy new `httpd` into place here >

```
cd /export/home/af/ENV2/d4b12/SOP1.5/3p/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV3/SOP1.5/3p/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV4/SOP1.5/3p/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV5/SOP1.5/3p/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV5/SOP1.5/tools/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV6/SOP1.5/3p/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV6/SOP1.5/tools/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV7/SOP1.5/3p/apache/bin
mv httpd httpd.1.3.27
ln -s ../../../../../apache/bin/httpd httpd
cd /export/home/af/ENV7/SOP1.5/tools/apache/bin
mv httpd httpd.1.3.27
```

```
ln -s ../../../../../apache/bin/httpd httpd
```

8. Services reduction in `inetd.conf`: To remove `name`, `talk`, `comsatd`, `sadmind`, `amiserv`, `rpc.cmsd`, and `dtspcd` do the following as root:

```
cp -p /etc/inetd.conf /tmp/inetd.conf ;
egrep -v \
     'in.(tnamed|talkd|comsat)|sadmind|amiserv|rpc.cmsd|dtspcd' \
     /tmp/inetd.conf > /etc/inetd.conf
```

9. Unneccessary Startup Files minimization: Service Script to monitor changes of disabled default processes: do the following as root (stop the processes, rename the startup scripts/links, place script to monitor):

```
cd /etc/rc3.d ; S76snmpdx stop ; S15nfs.server stop
mv S76snmpdx     orig.S76snmpdx
mv S15nfs.server orig.S15nfs.server
cd /etc/rc2.d ; S99dtlogin stop ; S88sendmail stop ;
S85power stop ; S76nscd stop ; S72autoinstall stop ;
S71sysid.sys stop ; S30sysid.net stop
(echo S99dtlogin  ;echo S88sendmail    ;echo S85power ;
 echo S76nscd     ;echo S72autoinstall ;echo S71sysid.sys;
 echo S30sysid.net ) | xargs -i{} mv {} orig.\{\}
ln -s ../init.d/rc-script-check.sh S99rc-script-check.sh
echo "5 * * * * /usr/lib/sendmail -q" >> \
  /var/spool/cron/crontabs/root
touch           /etc/init.d/rc-script-check.sh
chmod 744       /etc/init.d/rc-script-check.sh
chown root:root /etc/init.d/rc-script-check.sh
```

< copy Appendix J into `rc-script-check.sh` >

10. Set UID and Set GID files need restriction. Securing mqm-owned files (do the following as root):

```
cd /var/sadm/pkg/mqm-upd03/save ;
tar -cvf opt-saved.tar opt/ ; rm -r opt
chown mqm opt-saved.tar
```

Notes

[1] MD5 06 Jul. 2000. URL: http://sunsolve.sun.com/md5/md5.tar.Z (01 May 2004)

[2] "Just the Facts". 06 Apr. 2001. URL: http://www.sunsite.ualberta.ca/Sun_Resources/Just_The_Facts/JTF.html (01 May 2004)

[3] "Netra™ t 1400 and 1405 Servers Just the Facts". 31 Oct. 2001. URL: http://lios.apana.org.au/~cdewick/sunshack/data/sh/2.0/infoserver.central/data/syshbk/Systems/Netra_t1400/documents/netrat1_1400_jtf.pdf (01 May 2004)

[4] "SunSolve Patch Support Portal". 2004. URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage (01 May 2004)

[5] "Sun Remote Services Net Connect". 2004. URL: http://www.sun.com/srs/netconnect (01 May 2004)

[6] "Sunsolve(tm)". 2004. URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=explorer/explorer (01 May 2004)

[7] URL: http://www.google.com (01 May 2004)

[8] "Solaris 8 Patch Report Update as of Apr/16/2004". 16 Apr 2004. URL: http://northstar-www.dartmouth.edu/public/OS/Sun/Solaris8/Patches/Patch-Report-2004-Apr16 (01 May 2004)

[9] "patch ID# 117000-05". 30 Apr. 2004. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?type=0&doc=fpatches%2F117000&display=plain (01 May 2004)

[10] "patch ID# 114146-01". 09 Dec. 2002. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?type=0&doc=fpatches%2F114146&display=plain (01 May 2004)

[11] Pomeranz, Hal. SANS Security Essentials VI: Unix Security, 2002, Reading: 2002, pg. 1-7

[12] Noordergraph, Alex and Watson, Keith. "Sun™ Operating Environment Network Settings for Security". Sun BluePrints™ Online 1999. Dec. 1999. URL: http://www.sun.com/solutions/blueprints/1299/network.pdf (01 May 2004)

[13] "resolv.conf(4)", Trusted Solaris 8 Reference Manual, 09 Sep. 1997. URL: http://docs.sun.com/db/doc/835-8005/6ruu381rk?q=+resolv.conf&a=view (01 May 2004)

[14] Pomeranz, Hal. SANS Unix Practicum, 2003, Reading: 2003, pg.3-4

[15] Pomeranz, Reading: 2003 pg. 3-5

[16] Moffet, Darren. "Re: five questionable processes on fw". 30 Jan. 2001, URL: http://archives.neohapsis.com/archives/sf/sun/2001-q1/0046.html (01 May 2004)

[17] Instenes, Shawn. "Protecting Insecure Programs". 28 May 2003. URL: http://www.giac.org/practical/gsec/Shawn_Instenes_GSEC.pdf (01 May 2004)

[18] "Kernel Parameters". Solaris 10 Administrator Collection. URL: http://docs.sun.com/db/doc/817-0404/6mg74vsat?a=view (01 May 2004)

[19] "The Jakarta Site – Apache Tomcat". 2004. URL: http://jakarta.apache.org/tomcat/index.html (01 May 2004)

[20] "Open SSL: The Open Source toolkit for SSL/TLS". 2002. URL: http://www.openssl.org (01 May 2004)

[21] "About the SANS Institute". 2004. URL: http://www.sans.org/aboutsans.php (01 May 2004)

[22] "SANS Top 20 Vulnerabilities – The Expert Consensus ". 2004. URL: http://www.sans.org/top20 (01 May 2004)

[23] "Cert Coordination Center" 18 May. 2004. URL: http://www.cert.org (18 May 2004)

[24] "#46042, Free Sun Alert Notifications". 22 Aug. 2002. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/46042 (01 May 2004)

[25] "8_Recommended.README". 17 May. 2004. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=patch&doc=8_Recommended.README (18 May 2004)

[26] Taylor, Joseph (Randy). "Intrustion Detection FAQ IDS Evasion and Denial of Service Using RPC Design Flaws". URL: http://www.sans.org/resources/idfaq/rpc_evas.php (01 May 2004)

[27] "Change Log for 1.3.31" URL: http://www.apache.org/dist/httpd/CHANGES_1.3 (01 May 2004)

[28] "Common Vulnerabilities & Exposures". 13 May. 2004. URL: http://cve.mitre.org (18 May 2004)

[29] Muffett, Alec. "Crack Password Cracker FAQ". 21 Feb. 2003. URL: http://www.crypticide.com/users/alecm/security/c50-faq.html (01 May 2004)

[30] Tatham, Simon. "PuTTY: a free telnet/SSH client". 21 Apr. 2004. URL: http://www.chiark.greenend.org.uk/~sgtatham/putty/ (01 May 2004)

[31] "Installing, configuring, and using tcp wrapper to log unauthorized connection attempts on systems running Solaris 2.x ". 01 Mar. 2001. URL: http://www.cert.org/security-improvement/implementations/i041.07.html (01 May 2004)

[32] Reed, Darren. "IP Filter – TCP/IP Firewall/NAT software". URL: http://coombs.anu.edu.au/~avalon/ip-filter.html or http://www.ipfilter.org (01 May 2004)

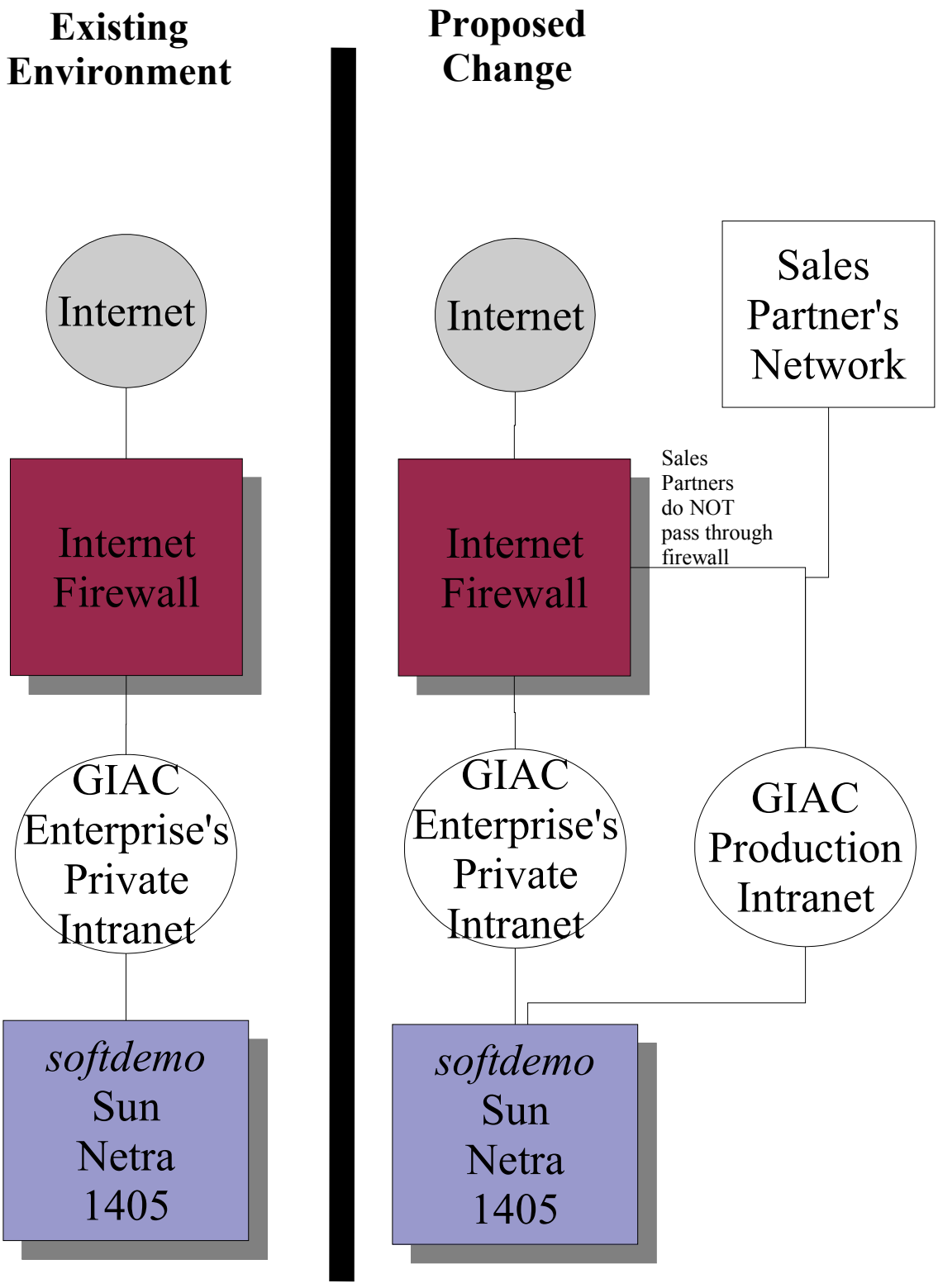
[33] "SANS Top 20 Vulnerabilities – The Expert Consensus ". 2004. URL: http://www.sans.org/top20/#ports (01 May 2004)

[34] The SANS Institute. SANS NewsBites. 21 Apr. 2004. Vol. 6, Num 16

[35] "SunSolve Patch Access". 2004 URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access (17 May 2004)

Appendices

Appendix A: Diagram of Proposed Network Changes



Appendix B: Example of Sun's MD5 fingerprint check

With the information from the output (everything prefaced by “MD5” below, is pasted in Sun's fingerprints.pl web page's dialog box described in the next appendix).

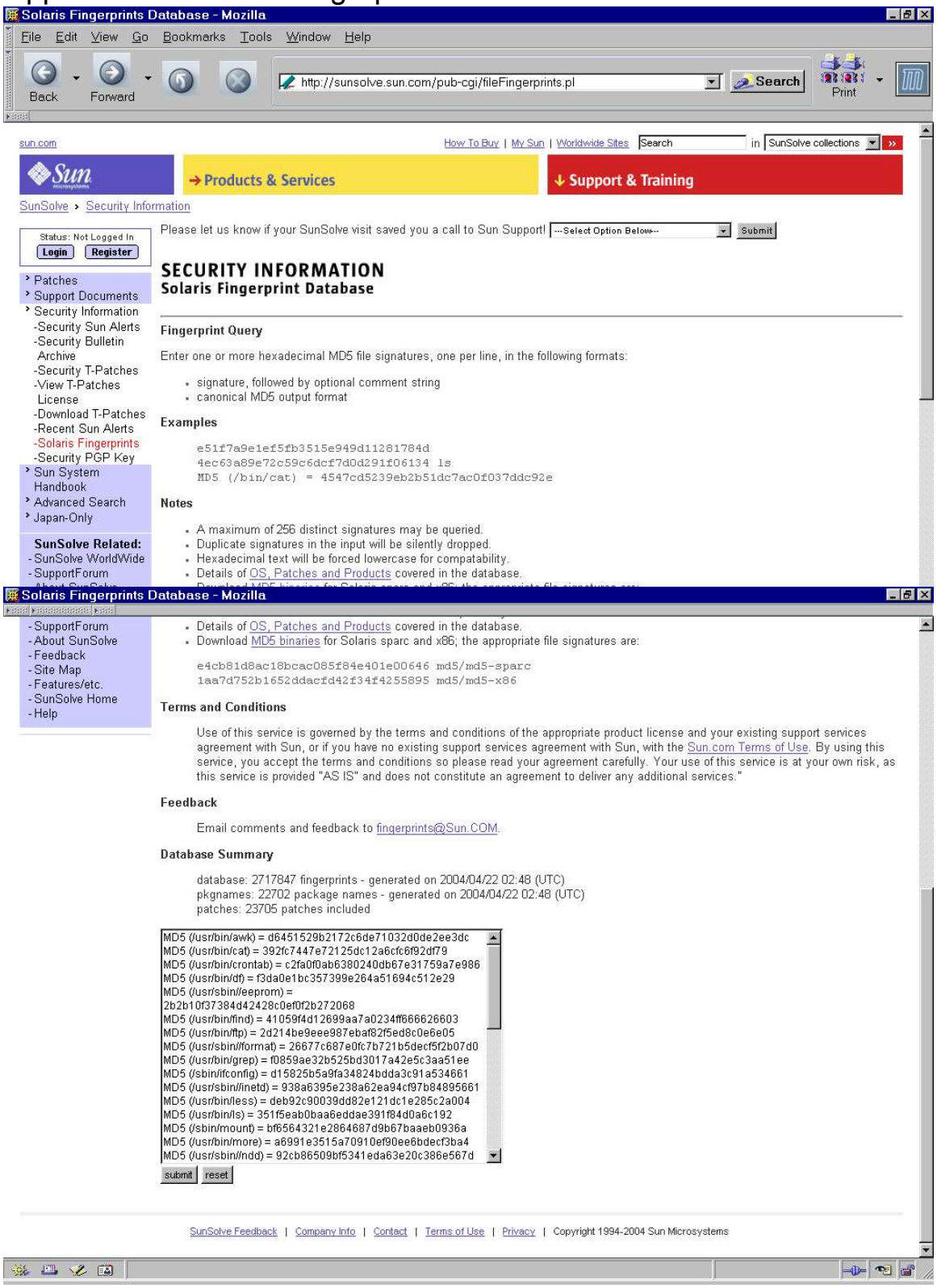
```
$ cat << EOF | xargs md5-sparc
> /usr/bin/awk
> /usr/bin/cat
> /usr/bin/crontab
> /usr/bin/df
> /usr/sbin/eeprom
> /usr/bin/find
> /usr/bin/ftp
> /usr/sbin/format
> /usr/bin/grep
> /sbin/ifconfig
> /usr/sbin/inetd
> /usr/bin/less
> /usr/bin/ls
> /sbin/mount
> /usr/bin/more
> /usr/sbin/ndd
> /usr/bin/netstat
> /usr/sbin/nslookup
> /usr/platform/sun4u/sbin/prtdiag
> /usr/bin/rlogin
> /usr/sbin/showmount
> /usr/bin/showrev
> /usr/bin/telnet
> /usr/bin/uname
> /usr/bin/xargs
> /usr/bin/ypcat
> /usr/bin/ypwhich
> /usr/bin/egrep
> /usr/sbin/in.telnetd
> /usr/sbin/in.rlogind
> /usr/sbin/in.rexecd
> /usr/sbin/in.rshd
```

> **/usr/sbin/in.ftpd**

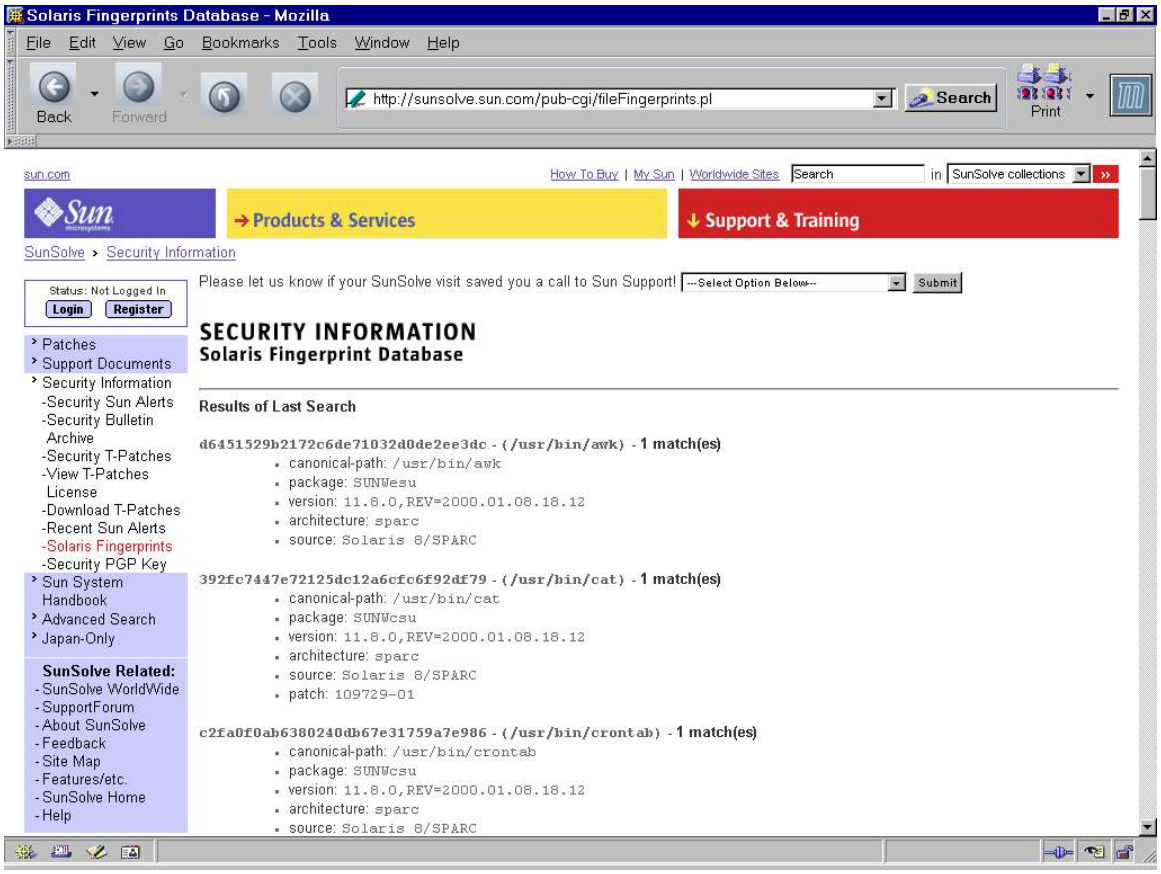
> **EOF**

```
MD5 (/usr/bin/awk) = d6451529b2172c6de71032d0de2ee3dc
MD5 (/usr/bin/cat) = 392fc7447e72125dc12a6cfc6f92df79
MD5 (/usr/bin/crontab) = c2fa0f0ab6380240db67e31759a7e986
MD5 (/usr/bin/df) = f3da0e1bc357399e264a51694c512e29
MD5 (/usr/sbin/eeprom) = 2b2b10f37384d42428c0ef0f2b272068
MD5 (/usr/bin/find) = 41059f4d12699aa7a0234ff666626603
MD5 (/usr/bin/ftp) = 2d214be9eee987ebaf82f5ed8c0e6e05
MD5 (/usr/sbin/format) = 26677c687e0fc7b721b5decf5f2b07d0
MD5 (/usr/bin/grep) = f0859ae32b525bd3017a42e5c3aa51ee
MD5 (/sbin/ifconfig) = d15825b5a9fa34824bdda3c91a534661
MD5 (/usr/sbin/inetd) = 938a6395e238a62ea94cf97b84895661
MD5 (/usr/bin/less) = deb92c90039dd82e121dc1e285c2a004
MD5 (/usr/bin/ls) = 351f5eab0baa6eddae391f84d0a6c192
MD5 (/sbin/mount) = bf6564321e2864687d9b67baaeb0936a
MD5 (/usr/bin/more) = a6991e3515a70910ef90ee6bdecf3ba4
MD5 (/usr/sbin/ndd) = 92cb86509bf5341eda63e20c386e567d
MD5 (/usr/bin/netstat) = 271daa9c1c246057b9a1929be919768c
MD5 (/usr/sbin/nslookup) = 66ac7c8125e831d77c7c65149c5f5810
MD5 (/usr/platform/sun4u/sbin/prtdiag) =
5e8fe2bed04ee5b2db18c5597cceb0ca
MD5 (/usr/bin/rlogin) = b76b06124a83abcab75707c55d4a3ec4
MD5 (/usr/sbin/showmount) = 8c0b2cfa875a540b750fac49f35b31df
MD5 (/usr/bin/showrev) = 65c1b4a19abe1950a044a3c8b4583fd1
MD5 (/usr/bin/telnet) = ca14dbb0272fe11cd4db7074b25c7268
MD5 (/usr/bin/uname) = 6c11382fa110495c1e825b2f14485672
MD5 (/usr/bin/xargs) = 42cace2419af3b639666c4103e401b21
MD5 (/usr/bin/ypcat) = 152d7a056da4c95029109c371593a1a0
MD5 (/usr/bin/ypwhich) = 5b2dcbdcfc8067b0da048fd92ca1be6d
MD5 (/usr/bin/egrep) = af5b7363657bbad817f09af0e2a61fe9
MD5 (/usr/sbin/in.telnetd) = 62bbe70a4dbaa8306cb885ef9ac053c3
MD5 (/usr/sbin/in.rlogind) = 46c1c2ba01e36c8264a3d25c4097bc98
MD5 (/usr/sbin/in.rexecd) = a87cbac9afcc06de574f563fe628d2f1
MD5 (/usr/sbin/in.rshd) = c2d9bbc6eef5f52ad5422ba8c984ff9b
MD5 (/usr/sbin/in.ftpd) = e4e86332f13406ce9e8bf307126e4238
```

Appendix C: Solaris Fingerprint Database Website



Appendix D: Solaris Fingerprint Database Website Output



Appendix E: Unix utilities' output

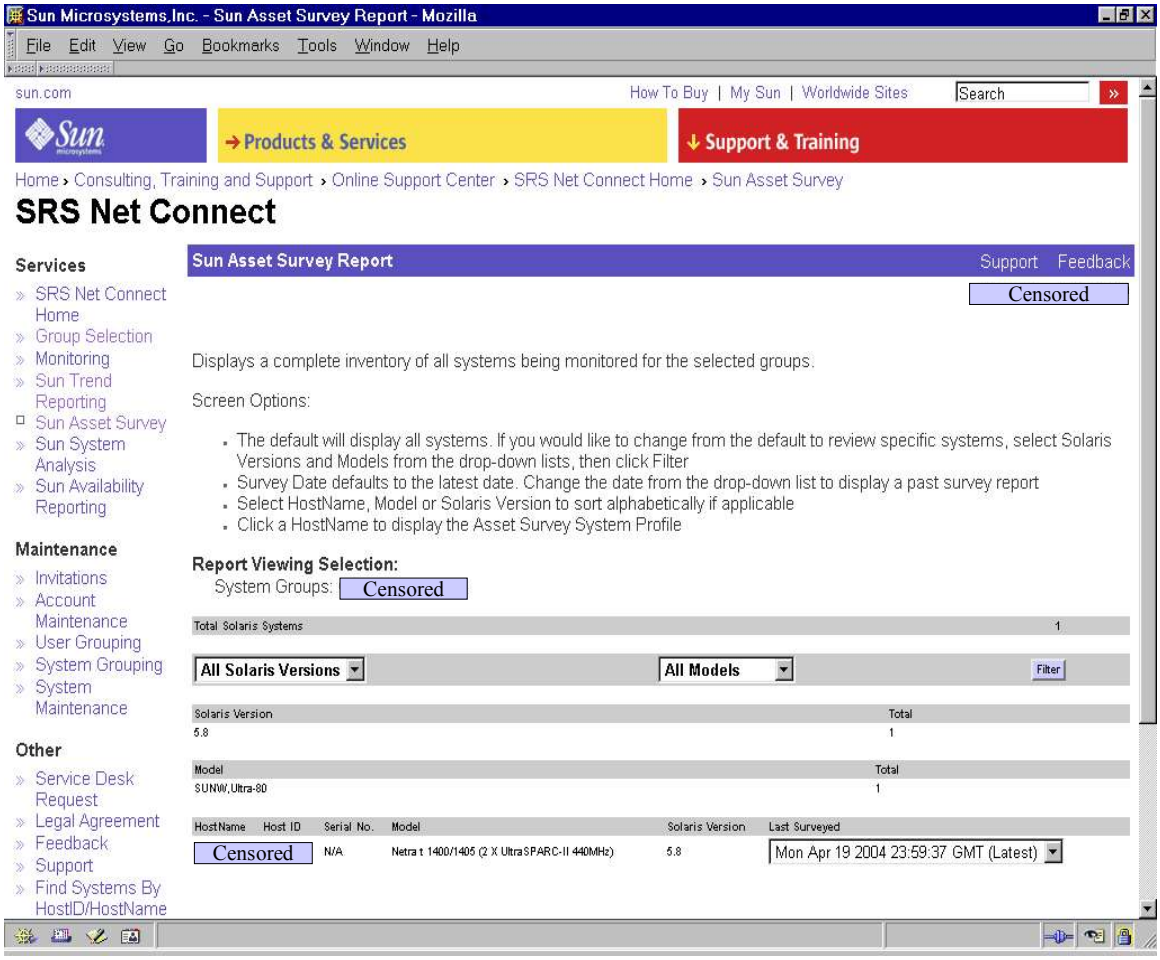
```
$ uname -X
System = SunOS
Node = softdemo
Release = 5.8
KernelID = Generic_108528-26
Machine = sun4u
BusType = <unknown>
Serial = <unknown>
Users = <unknown>
OEM# = 0
Origin# = 1
NumCPU = 2


$ /usr/platform/sun4u/sbin/prtdiag
System Configuration:  Sun Microsystems  sun4u Netra t 1400/1405 (2 X
UltraSPARC-II 440MHz)
System clock frequency: 110 MHz
Memory size: 4096 Megabytes


========================= CPUs =========================


                   Run   Ecache   CPU    CPU
Brd  CPU   Module   MHz     MB    Impl.   Mask
---  ---  -------  -----  ------  ------  ----
 0     1      1      440     4.0   US-II    10.0
 0     2      2      440     4.0   US-II    10.0


========================= IO Cards =========================


     Bus   Freq
Brd  Type  MHz   Slot        Name                                Model
---  ----  ----  ----------  ---------------------------------
----------------------
 0   PCI    33     On-Board  network-SUNW,hme
 0   PCI    33     On-Board  scsi-glm/disk (block)
Symbios,53C875
 0   PCI    33     On-Board  scsi-glm/disk (block)
Symbios,53C875
 0   PCI    33   pcib slot 2  SUNW,hme-pci108e,1001
SUNW,qsi-cheerio
 0   PCI    33   pcia slot 1  TSI,gfxp                           GFXP


No failures found in System
===========================


$ df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c0t0d0s0    3009327   53147 2895994     2%    /
/dev/dsk/c0t0d0s3    1987399 1501247  426531    78%    /usr
/proc                      0       0       0     0%    /proc
```

```
fd                         0       0       0     0%    /dev/fd
mnttab                     0       0       0     0%    /etc/mnttab
/dev/dsk/c0t0d0s4     962571  593639  311178    66%    /var
swap                 3065192      24 3065168     1%    /var/run
swap                 3065256      88 3065168     1%    /tmp
/dev/dsk/c0t0d0s5    2508555 2111625  346759    86%    /opt
/dev/dsk/c0t1d0s3    2056211 1278438  716087    65%    /db_backup
/dev/dsk/c0t2d0s0   10325760 8439971 1782532    83%    /vol01
/dev/dsk/c0t1d0s4    2056211       9 1994516     1%    /data
/dev/dsk/c0t1d0s5    2056211       9 1994516     1%    /billing
/dev/dsk/c0t1d0s6    2056211       9 1994516     1%    /billtmp
/dev/dsk/c0t3d0s0   17408538 13429616 3804837    78%    /export/home
/dev/dsk/c0t2d0s3    2056211     104 1994421     1%    /var/mqm
/dev/dsk/c0t1d0s0    4131866 2893847 1196701    71%    /opt/app/oracle
/dev/dsk/c0t2d0s4    2056211       9 1994516     1%    /var/mqm/log


$ su
Password:
# /usr/sbin/format
Searching for disks...done



AVAILABLE DISK SELECTIONS:
       0. c0t0d0 <SUN18G cyl 7506 alt 2 hd 19 sec 248>  rootdisk
          /pci@1f,4000/scsi@3/sd@0,0
       1. c0t1d0 <SUN18G cyl 7506 alt 2 hd 19 sec 248>  data
          /pci@1f,4000/scsi@3/sd@1,0
       2. c0t2d0 <SUN18G cyl 7506 alt 2 hd 19 sec 248>  billing1
          /pci@1f,4000/scsi@3/sd@2,0
       3. c0t3d0 <SUN18G cyl 7506 alt 2 hd 19 sec 248>  billing2
          /pci@1f,4000/scsi@3/sd@3,0
Specify disk (enter its number): 0
selecting c0t0d0: rootdisk
[disk formatted]
Warning: Current Disk has mounted partitions.



FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
        save       - save new disk/partition definitions
        inquiry    - show vendor, product and revision
        volname    - set 8-character volume name
        !<cmd>     - execute <cmd>, then return
        quit
format> quit
```

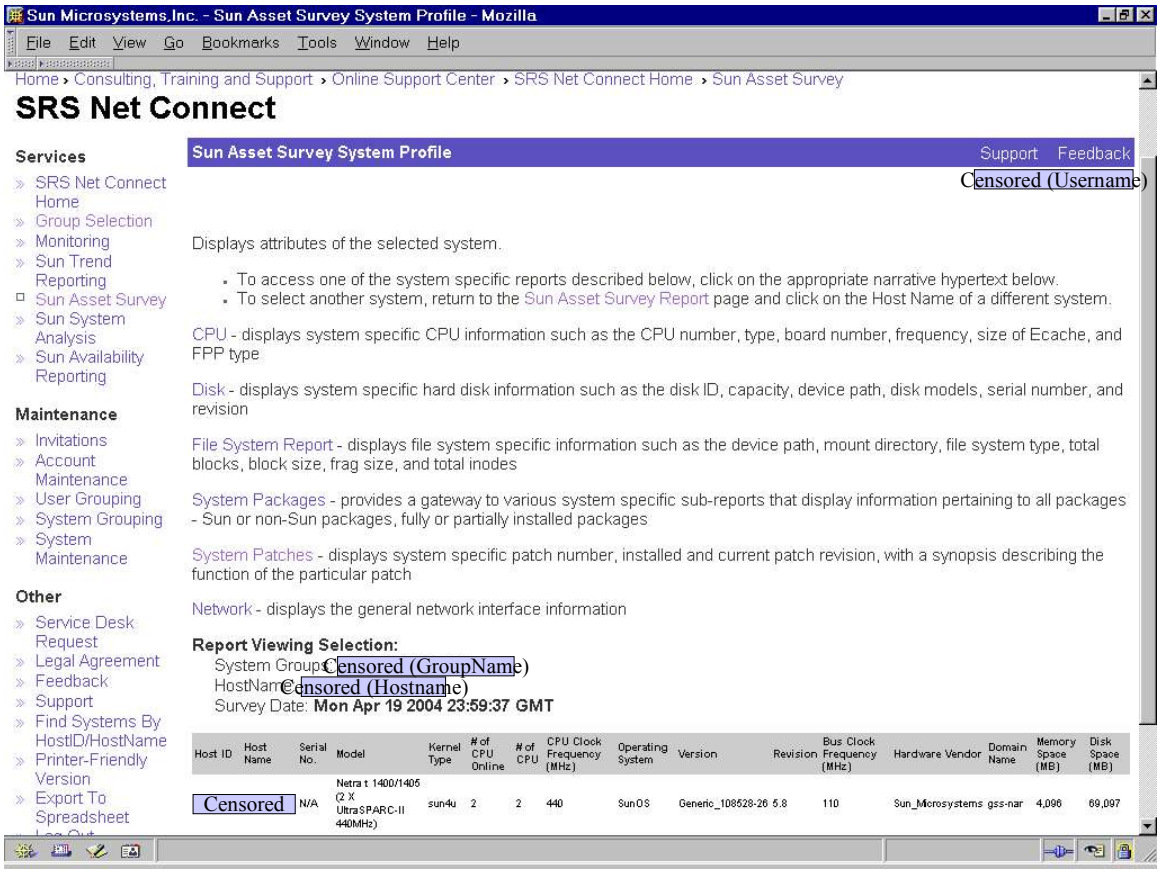
Appendix F: Sun SRS NetConnect

Screen shots from Sun's SRS NetConnect Page. This is after the company, account, and server has been setup. Login and precise server name have been blocked out.

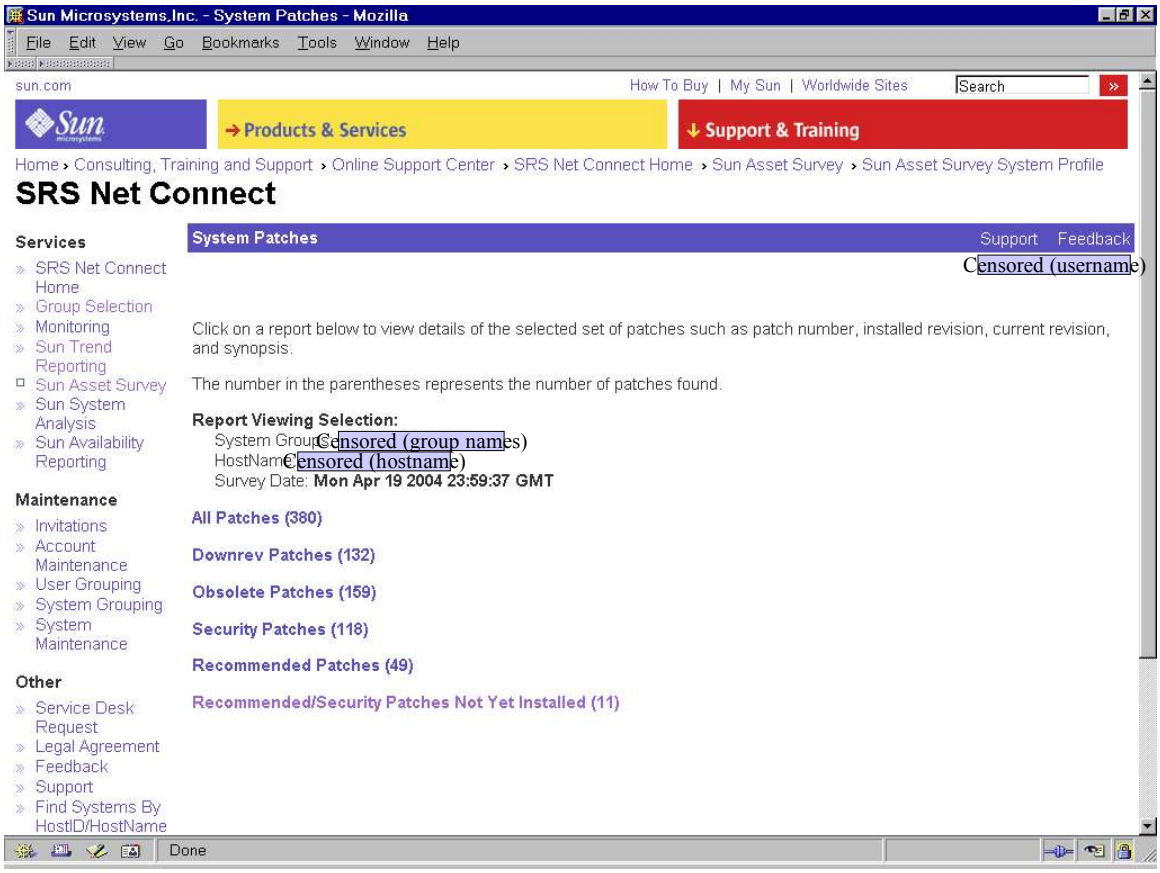
This is the 1st page after selecting the specific host in the hostgroup for the Asset Survey Report.



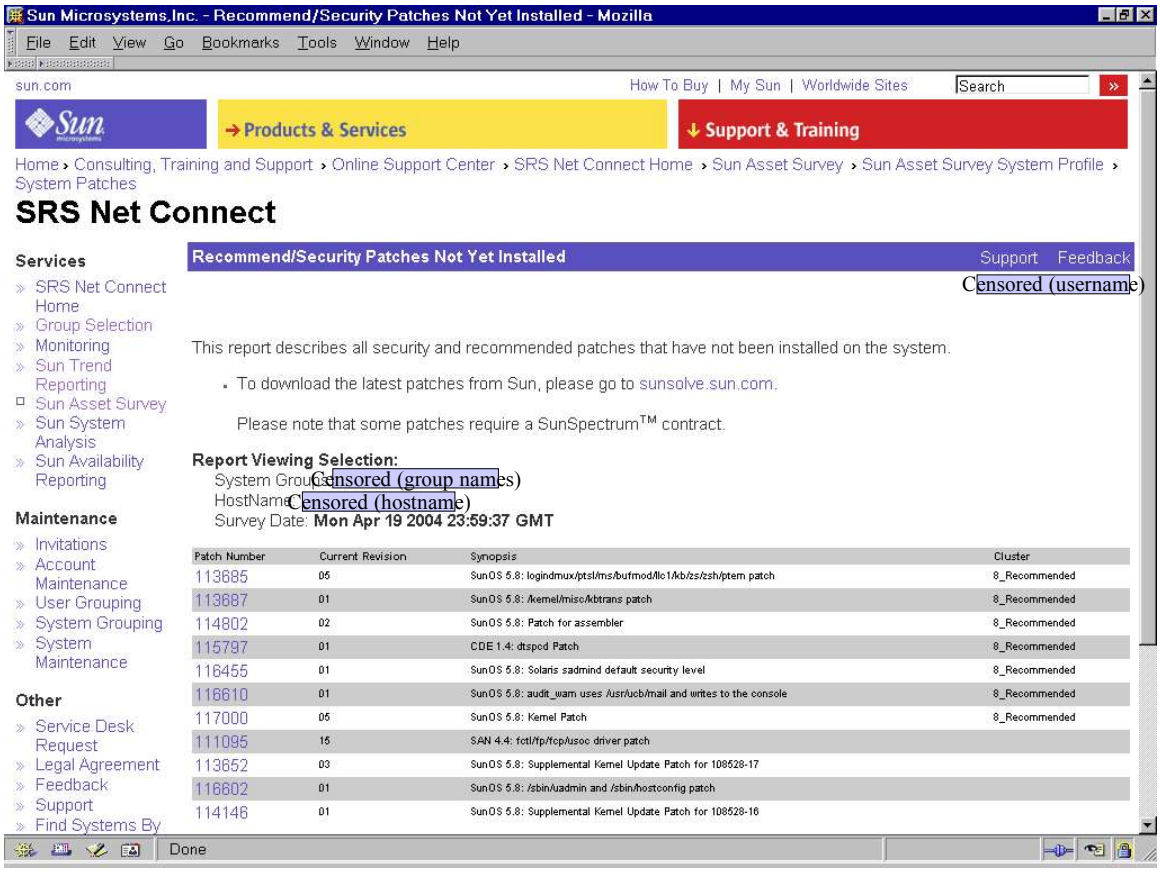
This is the 2nd page (after clicking on the hostname).



This is the 3rd page (selecting **System Patches**).



This is the 4th page (selecting **Recommended/Security patches not yet installed**).



Appendix G: Networking

Section 1: Interfaces (sudo for the purposes of doing this as root, `ifconfig` as a normal users does not displace the MAC address).

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
2
        inet 10.2.2.69 netmask ffffff00 broadcast 10.2.2.255
        ether 8:0:20:d1:d5:79
# netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
10.8.32.0            10.2.2.69            U         1   5269  hme0
224.0.0.0            10.2.2.69            U         1      0  hme0
default              10.2.2.1               UG        1  12914
127.0.0.1            127.0.0.1             UH       93 891639  lo0

# ls -ld /etc/notrouter /etc/defaultrouter
/etc/notrouter: No such file or directory
-rw-r--r--   1 root     other         14 Apr 16 16:27 /etc/defaultrouter
```

Section 2: Network driver settings

```
# ndd -get /dev/tcp tcp_conn_req_max_q0
1024
# ndd -get /dev/tcp tcp_ip_abort_cinterval
180000
# ndd -get /dev/ip ip_respond_to_timestamp
1
# ndd -get /dev/ip ip_respond_to_timestamp_broadcast
1
# ndd -get /dev/ip ip_respond_to_address_mask_broadcast
0
# ndd -get /dev/ip ip_forward_directed_broadcasts
1
# ndd -get /dev/arp arp_cleanup_interval
300000
# ndd -get /dev/ip ip_ire_arp_interval
1200000
# ndd -get /dev/ip ip_ignore_redirect
```

```
0
# ndd -get /dev/ip ip_send_redirects
1
# ndd -get /dev/ip ip_forward_src_routed
1
# ndd -get /dev/ip ip_forwarding
0
# ndd -get /dev/ip ip_strict_dst_multihoming
0
# ndd -get /dev/tcp tcp_strong_iss
1
# cat /etc/default/inetinit
# @(#)inetinit.dfl 1.2 97/05/08
#
# TCP_STRONG_ISS sets the TCP initial sequence number generation
parameters.
# Set TCP_STRONG_ISS to be:
#       0 = Old-fashioned sequential initial sequence number generation.
#       1 = Improved sequential generation, with random variance in
increment.
#       2 = RFC 1948 sequence number generation, unique-per-connection-
ID.
#
TCP_STRONG_ISS=1
# ndd -get /dev/tcp tcp_sack_permitted
2
```

Section 3: DNS

```
# egrep -v "^#" /etc/nsswitch.conf | grep dns
hosts:      files dns

# cat /etc/resolv.conf
domain giac.com
search giac.com
nameserver 10.2.2.52
nameserver 10.2.2.56
nameserver 10.2.2.91
nameserver 10.2.2.52
```

Section 4: RPC information

```
$ rpcinfo -p
   program vers proto   port  service
    100000    4   tcp    111  rpcbind
```

```
    100000    3   tcp    111  rpcbind
    100000    2   tcp    111  rpcbind
    100000    4   udp    111  rpcbind
    100000    3   udp    111  rpcbind
    100000    2   udp    111  rpcbind
    100007    3   udp  32774  ypbind
    100007    2   udp  32774  ypbind
    100007    1   udp  32774  ypbind
    100007    3   tcp  32771  ypbind
    100007    2   tcp  32771  ypbind
    100007    1   tcp  32771  ypbind
    100232   10   udp  32776  sadmind
    100001    2   udp  32777  rstatd
    100001    3   udp  32777  rstatd
    100001    4   udp  32777  rstatd
    100068    2   udp  32778
    100068    3   udp  32778
    100068    4   udp  32778
    100068    5   udp  32778
    100024    1   udp  32779  status
    100024    1   tcp  32772  status
    100133    1   udp  32779
    100133    1   tcp  32772
    100021    1   udp   4045  nlockmgr
    100021    2   udp   4045  nlockmgr
    100021    3   udp   4045  nlockmgr
    100021    4   udp   4045  nlockmgr
    100021    1   tcp   4045  nlockmgr
    100021    2   tcp   4045  nlockmgr
    100021    3   tcp   4045  nlockmgr
    100021    4   tcp   4045  nlockmgr
    300598    1   udp  32820
    300598    1   tcp  32795
 805306368    1   udp  32820
 805306368    1   tcp  32795
    100249    1   udp  32821
    100249    1   tcp  32796
```

Section 5: NIS maps

```
% egrep '^[^#]+nis( |$)' /etc/nsswitch.conf
passwd_compat: nis
```

```
group:      files nis
printers.conf:  files nis
printers:       user files nis
netgroup:   files nis
automount:  nis files
```

Section 6: NIS servers

```
# cat /var/yp/binding/nar/ypservers
nismaster.giac.com


# cat /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
10.2.2.69      softdemo
10.2.2.56      nismaster.giac.com nismaster
10.2.2.91      nisslave1.giac.com      nisslave1 loghost
200.140.150.69  new-softdemo
200.35.40.94 bus-part
```

Section 7: NFS server does not exist

```
$ egrep -v '^#|^$' /etc/dfs/dfstab
$ showmount -e
showmount: softdemo: RPC: Program not registered
$
```

Section 8: inetd.conf

```
$ egrep -v '^#' /etc/inetd.conf
ftp     stream  tcp6    nowait  root    /usr/sbin/in.ftpd       in.ftpd
telnet  stream  tcp6    nowait  root    /usr/sbin/in.telnetd
in.telnetd
name    dgram   udp     wait    root    /usr/sbin/in.tnamed
in.tnamed
shell   stream  tcp     nowait  root    /usr/sbin/in.rshd       in.rshd
shell   stream  tcp6    nowait  root    /usr/sbin/in.rshd       in.rshd
login   stream  tcp6    nowait  root    /usr/sbin/in.rlogind
in.rlogind
exec    stream  tcp     nowait  root    /usr/sbin/in.rexecd
in.rexecd
exec    stream  tcp6    nowait  root    /usr/sbin/in.rexecd
in.rexecd
comsat  dgram   udp     wait    root    /usr/sbin/in.comsat
in.comsat
talk    dgram   udp     wait    root    /usr/sbin/in.talkd      in.talkd
100232/10       tli     rpc/udp wait root /usr/sbin/sadmind     sadmind
rstatd/2-4      tli   rpc/datagram_v wait root /
usr/lib/netsvc/rstat/rpc.rstatd rpc.rstatd
fs              stream  tcp     wait nobody /usr/openwin/lib/fs.auto
fs
100234/1        tli     rpc/ticotsord   wait    root    /
usr/lib/gss/gssd gssd
100146/1        tli     rpc/ticotsord   wait    root    /
usr/lib/security/amiserv       amiserv
100147/1        tli     rpc/ticotsord   wait    root    /
usr/lib/security/amiserv       amiserv
dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
```

```
100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
bpcd    stream  tcp     nowait  root    /usr/openv/netbackup/bin/bpcd
bpcd
vnetd   stream  tcp     nowait  root    /usr/openv/bin/vnetd vnetd
vopied  stream  tcp     nowait  root    /usr/openv/netbackup/bin/vopied
vopied
bpjava-msvc     stream  tcp     nowait  root    /
usr/openv/netbackup/bin/bpjava-msvc bpjava-msvc -transient
$
```

Section 9: FTP files

```
$ ls -ld /etc/shells /etc/ftpusers
/etc/shells: No such file or directory
-rw-r--r--   1 root     sys           64 Dec  8 09:33 /etc/ftpusers
$ egrep root /etc/ftpusers
$
```

Appendix H: File Systems

Section 1: Search /etc/vfstab & auto.master NIS map.

```
$ grep suid /etc/vfstab
$ grep logging /etc/vfstab
$ grep auto /etc/nsswitch.conf
automount:  nis files
$ ypcat -k auto.master
/auto/p1 auto_p1         -timeo=20,intr,retrans=4,nosuid,hard
/users auto.home        -rw,soft,bg,nobrowse
/share auto_share       -timeo=20,intr,retrans=4,suid,hard
/proj auto_proj -timeo=20,intr,retrans=4,nosuid,hard
/vws auto.views      -rw,hard,bg,nfsv3
/net -hosts             -nosuid,nobrowse
/app auto_app   -timeo=20,intr,retrans=4,suid,hard
/- auto_direct  -timeo=20,intr,retrans=4,nosuid,hard
```

Section 2: No Set UID indirect NIS maps

```
$ ypcat -k auto.master | grep nosuid
/auto/p1 auto_p1         -timeo=20,intr,retrans=4,nosuid,hard
/proj auto_proj -timeo=20,intr,retrans=4,nosuid,hard
/net -hosts             -nosuid,nobrowse
/- auto_direct  -timeo=20,intr,retrans=4,nosuid,hard
```

Section 3: Set UID indirect NIS maps and export permissions from the NFS servers.

```
$ ypcat -k auto.master | grep -v nosuid | grep suid
/share auto_share       -timeo=20,intr,retrans=4,suid,hard
/app auto_app   -timeo=20,intr,retrans=4,suid,hard
$ ypcat -k auto.share
SUNWspro_6.0u2 nfsserv1:/install/SUNWS/SUNWspro_6.0u2/SUNWspro
SUNWspro_6.0u1 nfsserv1:/install/SUNWS/SUNWspro_6.0u1/SUNWspro
SUNWspro_6.0 nfsserv1:/install/SUNWS/SUNWspro_6.0/SUNWspro
SUNWspro_5.0 nfsserv1:/install/SUNWS/SUNWspro_5.0/SUNWspro
SUNWspro_4.0 nfsserv1:/install/SUNWS/SUNWspro_4.0/SUNWspro
SUNWspro nfsserv1:/install/SUNWS/SUNWspro_4.0/SUNWspro
X11R6 nfsserv3:/export/home/usr/local/${OSNAME}/share/&
X11R5 nfsserv3:/export/home/usr/local/${OSNAME}/share/&
amt nfsserv2:/export/opt1/&
```

```
adm nfsserv3:/export/home/usr/local/${OSNAME}/share/adm
X11 nfsserv3:/export/home/usr/local/${OSNAME}/share/X11R6
$ ypcat -k auto.app
SUNWexplo nfsserv3:/export/a1000/app/${OSNAME}/SUNWexplo
freetype nfsserv3:/export/a1000/app/freetype/${OSNAME}/${OSREL}
texinfo nfsserv3:/export/a1000/app/${OSNAME}/${OSREL}/texinfo
python nfsserv3:/export/a1000/app/python/${OSNAME}/${OSREL}
icare nfsserv3:/export/a1000/app/${OSNAME}/${OSREL}/icare
frame nfsserv3:/export/home/frame5.5
zlib nfsserv3:/export/a1000/app/zlib/${OSNAME}/${OSREL}
sudo nfsserv3:/export/a1000/app/sudo
nrpe nfsserv3:/export/a1000/app/nrpe/${OSNAME}/${OSREL}
java nfsserv3:/export/a1000/app/java
xpm nfsserv3:/export/a1000/app/xpm/${OSNAME}/${OSREL}
ssl nfsserv3:/export/a1000/app/ssl/${OSNAME}/${OSREL}
jmm -rw  nfsserv2:/export/opt1/jmm
gd nfsserv3:/export/a1000/app/gd/${OSNAME}/${OSREL}
frame5.5.6 -rw     nfsserv3:/export/home/frame5.5.6
netscape nfsserv3:/export/a1000/app/netscape
frame5.5 -rw     nfsserv3:/export/home/frame5.5
rrdtool nfsserv3:/export/a1000/app/rrdtool/${OSNAME}/${OSREL}
acrobat nfsserv3:/export/home/Acrobat3
xemacs nfsserv3:/export/a1000/app/${OSNAME}/${OSREL}/xemacs
purify nfsserv3:/export/a1000/app/Rational/${OSNAME}
rsync nfsserv3:/export/a1000/app/rsync
jpeg nfsserv3:/export/a1000/app/jpeg/${OSNAME}/${OSREL}
ssh nfsserv3:/export/a1000/app/ssh/${OSNAME}/${OSREL}
png nfsserv3:/export/a1000/app/libpng/${OSNAME}/${OSREL}
gsi -rw  nfsserv2:/export/opt1/gsi
$
$ showmount -e nfsserv1
export list for nfsserv1:
/install   snj_all
/export/p1 snj_all
/export/p2 snj_all
$
$ showmount -e nfsserv2
export list for nfsserv2:
/opt      snj_all
```

```
/var/mail snj_all
/export   snj_all
$
$ showmount -e nfsserv3
export list for nfsserv3:
/export/sena       snj_all
/export/a1000/proj snj_all
/export/a1000/gss  snj_all
/export/a1000/app  snj_all
/export/home       snj_all
$

$ ypcat -k netgroup | grep softdemo
```

Section 4: Indirect Maps not defined suid or nosuid.

```
$  ypcat -k auto.master | awk ' ! /suid/ {print $2}' | xargs ypcat -k
release -rw,soft,bg,largefiles  nfsserv4:/vol/vol0/release
test -rw,soft,bg              nfsserv5:/vegas/test
vegas -rw,hard,bg,nosuid       nfsserv6:/vegas/home
ti -rw,hard,bg,suid    nfsserv6:/vol/vol0/ti
sd -rw,hard,bg         nfsserv6:/vol/vol0/sd-home
$
$ showmount -e nfsserv4 | egrep 'release[^-/a-zA-Z]'
/vol/vol0/release         backup-filer.giac.com,wdc_unix_hosts,sfcr-
dev1.giac.com,10.2.2/24,london-hosts,river.giac.com,camb-tss-
hosts,camb-con-hosts,cala-unix-hosts,singapore-unix-hosts,api-
dev1.giac.com
$ showmount -e nfsserv5 | egrep 'test[^-a-zA-Z]'
/home/test            @10.2.2/24,all-nevada-unix-hosts
$ showmount -e nfsserv6 | egrep 'home[^-/a-zA-Z]'
export list for nfsserv6:
/vol/vol0/sd-home               con-hosts,backup-
filer.giac.com,frodo.giac.com
/vol/vol0/vegas/home            10.2.2/24,all-nevada-unix-hosts
/vol/vol0/vegas-home            backup-filer.giac.com,10.2.2/24,tig-
pc,all-colorado-unix-hosts,disk-access-ws
/vol/vol0/dev-home               (everyone)
$ showmount -e nfsserv6 | egrep 'ti[^-/a-zA-Z]'
/vol/vol0/ti                    all-nevada-unix-hosts,tig-
pc,aragorn.giac.com,10.2.2/24,nfsserv1.giac.com,gandalf.giac.com
```

Appendix I: CIS-scan output

$ **grep -i Neg /opt/CIS/cis-ruler-log.20040507-23:13:53.2102 | tail -1**
Negative: 6.8 Non-standard SGID program /var/sadm/pkg/mqm-upd03/save/opt/mqm/bin/setmqcap

$ **sudo cat /opt/CIS/cis-ruler-log.20040507-23:13:53.2102 | grep -i Neg | grep SGID | wc -l**

50

$ **sudo cat /opt/CIS/cis-ruler-log.20040507-23:13:53.2102 | grep -i Neg | egrep 'S[GU]ID' | wc -l**

111

$ **sudo cat /opt/CIS/cis-ruler-log.20040507-23:13:53.2102 | grep -i Neg | egrep -v 'S[GU]ID|world-writable|.(7|3) User'**

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

Negative: 1.2 tcp6-protocol service ftp in inetd.conf is not wrapped.

Negative: 1.2 tcp6-protocol service telnet in inetd.conf is not wrapped.

Negative: 1.2 udp-protocol service name in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service shell in inetd.conf is not wrapped.

Negative: 1.2 tcp6-protocol service shell in inetd.conf is not wrapped.

Negative: 1.2 tcp6-protocol service login in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service exec in inetd.conf is not wrapped.

Negative: 1.2 tcp6-protocol service exec in inetd.conf is not wrapped.

Negative: 1.2 udp-protocol service comsat in inetd.conf is not wrapped.

Negative: 1.2 udp-protocol service talk in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service fs in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service dtspc in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service bpcd in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service vnetd in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service vopied in inetd.conf is not wrapped.

Negative: 1.2 tcp-protocol service bpjava-msvc in inetd.conf is not wrapped.

Negative: 2.1 inetd listens on port fs -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port dtspc -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port exec -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port comsat -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port talk -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port name -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port 100068/2-5 -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port 100146/1 -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port 100147/1 -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port 100232/10 -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.1 inetd listens on port rstatd/2-4 -- this port's line should be commented out or deleted in inetd.conf.

Negative: 2.2 telnet not deactivated.

Negative: 2.3 ftp not deactivated.

Negative: 2.4 rsh (shell) should be deactivated.

Negative: 2.4 rlogin (rlogin) should be deactivated.

Negative: 2.8 CDE-related daemon fs.auto (port fs) not deactivated in inetd.conf.

Negative: 2.10 kerberos net daemon gssd not deactivated in inetd.conf.

Negative: 3.1 Serial login prompt not disabled.

Negative: 3.3 inetd is still active.

Negative: 3.4 System is running syslogd without the -t switch, accepting remote logging.

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

Negative: 3.6 in.rarpd program has not been disabled in /etc/rc3.d/S15nfs.server.

Negative: 3.6 rpc.bootparamd program has not been disabled in /etc/rc3.d/S15nfs.server.

Negative: 3.6 in.rarpd program has not been disabled in /etc/rc3.d/S15nfs.server.

Negative: 3.6 rpc.bootparamd program has not been disabled in /etc/rc3.d/S15nfs.server.

Negative: 3.7 llc2 not deactivated.

Negative: 3.7 uucp not deactivated.

Negative: 3.7 slpd not deactivated.

Negative: 3.7 PRESERVE not deactivated.

Negative: 3.7 bdconfig not deactivated.

Negative: 3.7 wbem not deactivated.

Negative: 3.7 ncalogd not deactivated.

Negative: 3.7 ncad not deactivated.

Negative: 3.7 mipagent not deactivated.

Negative: 3.7 autoinstall not deactivated.

Negative: 3.7 asppp not deactivated.

Negative: 3.7 cachefs.daemon not deactivated.

Negative: 3.7 cacheos.finish not deactivated.

Negative: 3.7 power not deactivated.

Negative: 3.7 dmi not deactivated.

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

Negative: 3.10 NFS script nfs.client not deactivated.

Negative: 3.10 NFS script autofs not deactivated.

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

Negative: 3.14 LDAP cache manager not deactivated.

Negative: 3.15 lp not deactivated.

Negative: 3.15 spc not deactivated.

Negative: 3.16 volume manager not deactivated.

Negative: 3.17 Graphical login-related script dtlogin not deactivated.

Negative: 4.1 Coredumps aren't deactivated.

Negative: 4.2 Stack is not set non-executable

Negative: 4.2 Non-executable stack violation logging is not active.

Negative: 4.3 NFS clients aren't restricted to privileged ports.

Negative: 4.4 Source routing (ip_forward_src_routed) should be deactivated

Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be deactivated

Negative: 4.4 Forwarding of directed broadcasts (ip_forward_directed_broadcasts) isn't disabled.

Negative: 4.4 tcp_conn_req_max_q0 should be at least 4096 to avoid TCP flood problems.

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

Negative: 4.4 ip_respond_to_timestamp isn't 0.

Negative: 4.4 ip_respond_to_timestamp_broadcast should be 0.

Negative: 4.4 ip_ignore_redirect isn't set to 1.

Negative: 4.4 ip6_ignore_redirect isn't set to 1.

Negative: 4.4 ARP timer (arp_cleanup_interval) should be at most 60,000.

Negative: 4.4 ARP timer (ip_ire_arp_interval) should be at most 60,000

Negative: 4.5 ip_strict_dst_multihoming isn't activated.

Negative: 4.5 ip6_strict_dst_multihoming isn't activated.

Negative: 4.5 ip_send_redirects isn't set to 0.

Negative: 4.6 TCP sequence numbers not strong enough.

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

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

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

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

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

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

Negative: 5.5 Couldn't find an active sadc line in /etc/rc2.d/S21perf to verify system acctg.

Negative: 5.5 No sa1 line in /var/spool/cron/crontabs/sys -- no system accounting.

Negative: 5.5 No sa2 line in /var/spool/cron/crontabs/sys -- no system accounting.

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

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

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

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

Negative: 7.1 /etc/pam.conf appears to support rhost auth.

Negative: 7.2 File //.rhosts exists, is non-zero size, isn't linked to /dev/null, and doesn't contain only the - character.

Negative: 7.4 /etc/shells does not exist.

Negative: 7.5 /etc/dt/config/Xaccess doesn't exist, thus permits remote X-terminal login.

Negative: 7.7 /etc/dt/config/ doesn't exist, so GUI screenlocker can't be configured.

Negative: 7.8 Couldn't open cron.allow

Negative: 7.8 Couldn't open at.allow

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

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

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

Negative: 7.10 EEPROM banner isn't on.

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

Negative: 7.10 Couldn't open /etc/default/telnetd to test for BANNER line.

Negative: 7.10 Couldn't open /etc/default/ftpd to test for BANNER line.

Negative: 7.10 /etc/dt/config/ doesn't exist, so GUI welcome message couldn't have been changed.

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

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

Negative: 7.13 EEPROM isn't password-protected.

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

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

Negative: 8.1 nobody4 has a valid shell of /bin/sh. Remember, an empty

shell field in /etc/passwd signifies /bin/sh.

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

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

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

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

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

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

Negative: 8.2 User oracle has no password in /etc/shadow!

Negative: 8.2 User +@SA-ADMINS has no password in /etc/shadow!

Negative: 8.2 User +@SECURITY has no password in /etc/shadow!

Negative: 8.2 User +@DEVDBA has no password in /etc/shadow!

Negative: 8.2 User +@MKTNAR has no password in /etc/shadow!

Negative: 8.2 User + has no password in /etc/shadow!

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

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

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

Negative: 8.4 /etc/passwd contained +: in it!

Negative: 8.4 /etc/shadow contained +: in it!

Negative: 8.5 A non-root UID 0 account (named +@SA-ADMINS) was found.

Negative: 8.5 A non-root UID 0 account (named +@SECURITY) was found.

Negative: 8.5 A non-root UID 0 account (named +@DEVDBA) was found.

Negative: 8.5 A non-root UID 0 account (named +@MKTNAR) was found.

Negative: 8.5 A non-root UID 0 account (named +) was found.

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

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

Negative: 8.8 User srsnetc has world/group-writable dot-files (.*) in his/her home directory.

Negative: 8.10 Current umask setting in file /etc/default/login is 000 -- it should be stronger to block world-read/write/execute.

Negative: 8.10 Current umask setting in file /etc/default/login is 000 -- it should be stronger to block group-read/write/execute.

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

Negative: 8.10 Current umask setting in file /etc/profile is 022 -- it should be stronger to block world-read/write/execute.

Negative: 8.10 Current umask setting in file /etc/profile is 022 -- it

should be stronger to block group-read/write/execute.

Negative: 8.10 Current umask setting in file /etc/.login is 000 -- it should be stronger to block world-read/write/execute.

Negative: 8.10 Current umask setting in file /etc/.login is 000 -- it should be stronger to block group-read/write/execute.

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

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

$

Appendix J: rc-script-check.sh

```
#!/bin/sh

#
# rc-script-check.sh
# v1.0
# James Surlow
# 05/05/04
#
# This script is used to check to see if any patches placed any
# files back into the startup scripts.
#
# It is assumed to be placed in /etc/init.d on Solaris boxes
# It is assumed that one would symlink with
#   /etc/rc3.d/S99rc-script-check.sh
#
# This script assumes:
# 1) that files are renamed to be $SEARCH.<filename>
#      e.g. if standard used is "orig.<filename>
#               S88sendmail becomes orig.S88sendmail
# 2) mail can still flow to root
#
MAILTO=root
SEARCH=orig

ECHO=/bin/echo
HOSTNAME=/bin/hostname
LS=/bin/ls
MAIL=/bin/mail
SED=/bin/sed
WC=/bin/wc
XARGS=/bin/xargs

RC=`$LS /etc/rc?.d/$SEARCH* | $SED "s/$SEARCH\.//" | $XARGS ls`

if [ 0 -ne `$ECHO $RC | $WC -l`  ]; then
        ( $ECHO "The following files were found on `$HOSTNAME`:"; $ECHO
$RC; ) \
             | $MAIL $MAILTO
fi

# end of file
```

Appendix K: after-inet.sh

```
#!/bin/sh
#
# after-inet.sh
# v1.0
# James Surlow
# 05/12/04
#
# This script is used to set network device drives to more
# appropriate values than the defaults.
#
# It is assumed to be placed in /etc/init.d on Solaris boxes
# It is assumed that one would symlink with
#    /etc/rc2.d/S70after-inet.sh
#
#######
# SYN flood protection
#   Increase number of connections from 1024
#   Decrease amount of abort interval from 180000
#                              milliseconds (3 min)
#
ndd -set /dev/tcp tcp_conn_req_max_q0 8192
ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
#
#######
# SMURF protection
#   Turn off response to timestamp requests
#   Turn off response to timestamp broadcast requests
#   Turn off response to address_mask broadcast requests
#   Do not forward broadcasts
#
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
#
#######
# ARP timeout tuning
#   Turn down arp cache to 1 minute
#
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip ip_ire_arp_interval   60000
#
#######
# IP redirect: disable
#   Redirects should be sent by the router, ignore others
#   Do not send any redirects
#
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 0
#######
# Disable Source routing
#
ndd -set /dev/ip ip_forward_src_routed 0
#
#######
# Disable IP Forwarding
```

```
#   Do not IP forward
#   Do not forward packets on the same host to different
#      interfaces
#
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 1
#######
# TCP sequence numbers - best algorithm
#
ndd -set /dev/tcp tcp_strong_iss 2
#
# end of file
```

Appendix L: inetd.conf in rc scripts

```
$ grep inetd /etc/rc2.d/*
/etc/rc2.d/S72inetsvc:  /usr/bin/pkill -x -u 0 'in.named|inetd'
/etc/rc2.d/S72inetsvc:# Run inetd in "standalone" mode (-s flag) so
that it doesn't have
/etc/rc2.d/S72inetsvc:# to submit to the will of SAF.  Why did we ever
let them change inetd?
/etc/rc2.d/S72inetsvc:/usr/sbin/inetd -s &
/etc/rc2.d/S73cachefs.daemon:inetconf=/etc/inet/inetd.conf
```

Appendix M: Apache servers (HTTP & Tomcat & GIAC Sales OpenSSL)

```
$ sudo find /export/home  -name httpd.conf -print -exec egrep '^Port|
^Listen|mod_(alias|rewrite)' {} \;
/export/home/af/scripts/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 22000
Listen 22000
Listen 22001
<IfModule mod_alias.c>
/export/home/af/ENV2/d4b12/SOP1.5/cc/gui/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 8080
<IfModule mod_alias.c>
/export/home/af/ENV2/d4b12/SOP1.5/3p/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 32000
Listen 32000
Listen 32001
<IfModule mod_alias.c>
/export/home/af/ENV3/SOP1.5/cc/gui/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 8080
<IfModule mod_alias.c>
/export/home/af/ENV3/SOP1.5/3p/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 33000
Listen 33000
Listen 33001
<IfModule mod_alias.c>
/export/home/af/ENV4/SOP1.5/3p/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 24000
Listen 24000
Listen 24001
<IfModule mod_alias.c>
/export/home/af/ENV4/SOP1.5/cc/gui/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
```

```
Port 8080
<IfModule mod_alias.c>
/export/home/af/ENV5/SOP1.5/3p/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 80
Listen 8080
Listen 8443
<IfModule mod_alias.c>
/export/home/af/ENV5/SOP1.5/tools/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 25000
Listen 25000
Listen 25001
<IfModule mod_alias.c>
/export/home/af/ENV6/SOP1.5/3p/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 80
Listen 8080
Listen 8443
<IfModule mod_alias.c>
/export/home/af/ENV6/SOP1.5/tools/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 36000
Listen 36000
Listen 36001
<IfModule mod_alias.c>
/export/home/af/ENV7/SOP1.5/install_backup/ccgui-04062004-
110944/apache_conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 37000
Listen 37000
Listen 37001
<IfModule mod_alias.c>
/export/home/af/ENV7/SOP1.5/3p/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 80
Listen 8080
Listen 8443
<IfModule mod_alias.c>
/export/home/af/ENV7/SOP1.5/tools/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
```

```
AddModule mod_rewrite.c
Port 37000
Listen 37000
Listen 37001
<IfModule mod_alias.c>
/export/home/af/apache/conf/httpd.conf
LoadModule alias_module       libexec/mod_alias.so
LoadModule rewrite_module     libexec/mod_rewrite.so
AddModule mod_alias.c
AddModule mod_rewrite.c
Port 22000
Listen 22000
Listen 22001
<IfModule mod_alias.c>
$
```

```
$ sudo find /export/home/af -name httpd -print -exec {} -v \;
Password:
/export/home/af/ENV2/d4b12/SOP1.5/3p/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV3/SOP1.5/3p/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV4/SOP1.5/3p/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV5/SOP1.5/3p/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV5/SOP1.5/tools/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV6/SOP1.5/3p/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV6/SOP1.5/tools/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV7/SOP1.5/3p/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/ENV7/SOP1.5/tools/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
/export/home/af/apache/bin/httpd
Server version: Apache/1.3.27 (Unix)
Server built:   Feb 11 2003 11:56:49
$
```

```
# pwd
/export/home/af
```

```
# find . -name tomcat -print 2> /dev/null | xargs -iX find X -name
VERSION -print -exec cat {} \;
./ENV2/d4b12/SOP1.5/3p/tomcat/VERSION
4.0.3
./ENV3/SOP1.5/3p/tomcat/VERSION
4.0.3
```

```
./ENV4/SOP1.5/3p/tomcat/VERSION
4.0.3
./ENV5/SOP1.5/3p/tomcat/VERSION
4.0.3
./ENV6/SOP1.5/3p/tomcat/VERSION
4.0.3
./ENV7/SOP1.5/3p/tomcat/VERSION
4.0.3

# find . -name openssl -type f -print 2> /dev/null -exec {} version \;
./ENV3/SOP1.5/3p/openssl/bin/openssl
OpenSSL 0.9.6g 9 Aug 2002
./ENV4/SOP1.5/3p/openssl/bin/openssl
OpenSSL 0.9.6g 9 Aug 2002
./ENV5/SOP1.5/3p/openssl/bin/openssl
OpenSSL 0.9.6g 9 Aug 2002
./ENV6/SOP1.5/3p/openssl/bin/openssl
OpenSSL 0.9.6g 9 Aug 2002
./ENV7/SOP1.5/3p/openssl/bin/openssl
OpenSSL 0.9.6g 9 Aug 2002
```

Appendix N: Veritas NetBackup

From the backup server:

```
#/usr/openv/netbackup/bin/admincmd/bpcllist -byclient softdemo | egrep
'CLASS|softdemo'
CLASS UNIX_OS *NULL* 0 0 0 *NULL*
CLIENT softdemo Solaris Solaris8 0 0 0 0 *NULL*
```

On *softdemo*:

```
$ cat exclude_list.UNIX_OS | xargs -i{} ls -ld {} 2>      /dev/null
dr-xr-xr-x 815 root     root      480032 May  7 13:21 /proc/
drwxrwxrwt  13 root     sys         1693 May  7 13:21 /tmp/
drwxr-xr-x   2 root     nobody       512 Sep  3  2003 /cdrom/
dr-xr-xr-x   2 root     root         512 Sep  3  2003 /home/
drwxr-xr-x   2 root     root         512 Sep  3  2003 /vol/
dr-xr-xr-x   2 root     root         512 Sep  3  2003 /xfn/
dr-xr-xr-x   1 root     root           1 Apr 16 17:20 /net/
drwxr-xr-x   2 root     sys          512 Sep  3  2003 /mnt/
drwxr-xr-x   5 oracle   dba          512 Jan 28 15:19 /db_backup/
dr-xr-xr-x   2 root     root         512 Sep  3  2003 /export/restore
```

From the backup server (after omission was handled):

```
#/usr/openv/netbackup/bin/admincmd/bpcllist -byclient softdemo | egrep
'CLASS|softdemo'

CLASS DB_BACKUP *NULL* 0 0 0 *NULL*
CLIENT softdemo Solaris Solaris8 0 0 0 0 *NULL*
CLASS UNIX_OS *NULL* 0 0 0 *NULL*
CLIENT softdemo Solaris Solaris8 0 0 0 0 *NULL*
```

Appendix O: Crack

```
% ./Crack ypstuff
Crack 5.0a: The Password Cracker.
(c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996
System: OSF1 crakrjak.giac.com V5.1 732 alpha
Home: /home/crack50a
Invoked: ./Crack ypstuff
Stamp: osf1-v5-alpha

Crack: making utilities in run/bin/osf1-v5-alpha
find . -name "*~" -print | xargs -n50 rm -f
( cd src; for dir in * ; do ( cd $dir ; make clean ) ; done )
rm -f dawglib.o debug.o rules.o stringlib.o *~
/bin/rm -f *.o tags core rpw destest des speed libdes.a .nfs* *.old
*.bak destest rpw des speed
rm -f *.o *~
`../../run/bin/osf1-v5-alpha/libc5.a' is up to date.
all made in util
Crack: The dictionaries seem up to date...
Crack: Sorting out and merging feedback, please be patient...
Crack: Merging password files...
Crack: Creating gecos-derived dictionaries
mkgecosd: making non-permuted words dictionary
mkgecosd: making permuted words dictionary
Crack: launching: cracker -kill run/Kcrakrjak.giac.com.21288
Done

$ ./Reporter | egrep 'Guessed' | wc -l
344

$ wc -l ypstuff
   1367 ypstuff
```

Appendix P: IP Filter configuration file

```
# Configuration file for IP Filter
# /etc/opt/ipf/ipf.conf
#
# James Surlow
# May 15, 2004
# rev 1.0
#
# private internal network has IP numbers of the form:
#    10.x.y.z
# our IP on the internal network:          10.2.2.69
# our IP on the business partner network:  200.140.150.69
# the source IP from our business partner: 200.35.40.94
# internal network         will use hme0
# business partner network will use hme1
#
#
# allow packets from 10.x.y.z
#
pass in  from 10.0.0.0/8 to any
#
#
# allow packets from loopback
# block and log any packets from 127.0.0.1 that do not
#   originate on the loopback.
#
pass  in     on lo0  from 127.0.0.1 to any
block in log on hme0 from 127.0.0.1 to any
block in log on hme1 from 127.0.0.1 to any
#
#
# allow known IP in bound.
block in log on hme1 from any              to 200.140.150.69
pass  in     on hme1 from 10.0.0.0/8       to 200.140.150.69
pass  in log on hme1 from 200.140.150.0/24 to 200.140.150.69
#
# block ports 53 (DNS), 111 (portmapper),
#         512-515 (syslog, print, rs-services),
#         2049 (rpc.nfsd), 6000-6009 (X)
# and exit immediately
block in log quick on hme1 from proto tcp/udp from 200.35.40.94 to
200.140.150.69/32 port = 53
block in log quick on hme1 from proto tcp/udp from 200.35.40.94 to
200.140.150.69/32 port = 111
```

```
block in log quick on hme1 from proto tcp/udp from 200.35.40.94 to
200.140.150.69/32 port 511 >< 515

block in log quick on hme1 from proto tcp/udp from 200.35.40.94 to
200.140.150.69/32 port = 2049

block in log quick on hme1 from proto tcp/udp from 200.35.40.94 to
200.140.150.69/32 port 5999 >< 6010

# block NFS ports 32771-32779 and exit immediately

block in log quick on hme1 from proto tcp/udp from 200.35.40.94 to
200.140.150.69/32 port 32770 >< 32780

#

#

# pass in other ports above 1024 from business partner
pass  in log on hme1 proto tcp/udp from 200.35.40.94     to
200.140.150.69/32 port > 1024

#

# pings and other ICMP are okay
pass  in log on hme1 proto icmp from any to any keep state

#

# no limits on outbound.
pass  out from any to any
```