Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Security Assessment for ACME Services

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

GIAC Securing UNIX Practical Assignment

Prepared by Chris Hancock

October 26, 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Executive Summary

The purpose for this assessment is to detail the security risks associated with the operation of the ACME Service's (referred to as the "customer") Sun Solaris application server (referred to as the "server"). This document represents an evaluation for possible security violations. The audit of the customer's server was performed on October 24th and 25th, 2000.

A network host scan was identified during a routine log analysis. This network scan was originating from within the customers network. (The classic attack: exploit a machine and install tools on it to gain further knowledge of the network) Due to the time of the network host scan, 1:00 a.m. on October 15th, the decision was made to run a quick analysis of the suspect server. The analyst immediately ran the nmap security tool to find more information on this host. This scan revealed several major software holes on the server that could have been easily exploited. Next, the system administrator for that particular network was contacted and an onsite risk assessment was setup.

The server, which was scanning the network, was found to be a backup host for the customer's current production server. This backup system has since crashed for reasons unknown, but the suspicion is that the break down was intentional to possibly cover a system compromise. After verifying with the system administrator that network scans are not a part of this server's processes, information was gathered about the backup system.

The production server (the server under scrutiny here) was on the same network as the backup server. Both servers were configured similarly, which means the likelihood of an attack on the production server is very high.

Network data communications between the server and clients has been determined to be vulnerable. The protocols used to communicate have no encryption capability. Backups are being done, but no documentation of the procedure has been done. Although the system administrator has a plan for disaster recovery, the customer has no policies or written procedures in place for this type of an event. The customer could not produce any self-documented server information.

During the initial interview and onsite walkthrough, the following basic information was discovered:

- The hardware in use is a Sun Microsystems Enterprise 250 (UltraSPARC-II 400MHz). It is a single processor unit with 256 MB of RAM.
- The operating system is Solaris 2.6.
- The server's main purpose is to run IMS 2000.
    - IMS-2000 is a portfolio management, investment accounting and financial reporting system designed for large institutional investors.
    - The customer purchased the hardware and shipped it to the vendor for OS and application installation. This was purchased as essentially a "turn-key" solution.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The secondary services this server provides are telnet and NFS. These services are currently required for normal operations.
    - The telnet service is used for user login to the IMS application.
    - NFS is used to transfer files to the server from a Windows based workstation.
        - The user basically maps a drive letter under Windows to the NFS mounted volume on the server for drag and drop file transfers.

The following areas of vulnerability will be analyzed:

- Physical location
- File system
- Network services

The tools used to conduct this audit:

- NMAP Security Scanner (http://www.insecure.org/nmap/)
- Sun Solaris FingerPrint Database (http://sunsolve.sun.com/pub-cgi/show.pl?target=content/content7)
- Crack (ftp://coast.cs.purdue.edu/pub/tools/unix/crack/crack5.0.tar.gz) password file cracking tool.
- Sun Solaris Patchdiag tool (available only to Sun contract holders)

Finally, this assessment will offer a summary of recommendations on securing the server, and the approximate time that it will take to apply them.

Vulnerabilities

For each vulnerability, the following information will supplied:

- Threat level
- Possible outcomes
- Short suggestion on how to resolve the problem

The threat level indicates the possibility of un-authorized attempts to gain access to your network using buffer overflows or mis-configured/un-secured services.

The numbers 1-3 will indicate the threat level:

- **Low (1):** This vulnerability is low risk but still could be used to compromise the system. If the vulnerability is used, data on the server could be at risk. Although not high priority, this threat level might be used as a way to gather information in order to execute another more dangerous exploit.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **Medium (2):** This vulnerability is medium risk and probably would not take much time or knowledge to exploit. Data is probably at risk. This weakness should be taken care of as soon as possible.

- **High (3):** This vulnerability is high risk and usually means that the exploit could be immediate and the consequences could be disastrous. Data is definitely at risk because this is usually a well-known exploit. Someone with limited computer knowledge could probably accomplish this exploitation. This level could also indicate a misconfigured service, which allows access with no authentication. This threat level must be resolved immediately.

Operating System:

Threat level (3): Open NFS
The NFS shared volumes were found to be world read/write. This essentially means that anyone on the internet could have modified data on these mounted partitions. This is a commonly misconfigured service, which has very dangerous consequences. The partitions found were /home and /usr2. /home is used for user "home" directories. The volume /usr2 is where the IMS 2000 application and database files exist. The use of NFS is very insecure. Besides the fact that the authentication is extremely weak, the network traffic it creates is all in clear text. This makes NFS susceptible to packet sniffing.
Recommendation:
There are many exploits for the NFS service itself, so use of this service should be terminated, and an alternate means should be found to enable file transfer to/from the server. The suggestion here is SSH.

Threat level (3): Trojaned binaries
Due to the danger of the above NFS attack, the server may have been compromised. During the course of the exploit, the attacker could have replaced essential system binaries (ps or netstat for example). An attacker would do this to hide processes that they have executed with malicious intent or to try and cover the original exploit.
Recommendation:
An operating system re-install is required. It would be nearly impossible to verify the integrity of all installed binaries. A comparison could be done between the current files to the original OEM released files using Sun's Solaris Fingerprint Database, but the task could be overwelming.

Threat level (3): OS Patches
The current servers operating system, Solaris 2.6, is notorious for major flaws in its code. Numerous security related patches have been released to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

compensate for these flaws. Any server running Solaris 2.6 must be at the latest patch level. The output of Sun's PatchDiag tool reveals that this server is far from being at the latest revision. See Appendix A for the PatchDiag tool output.

Recommendation:
Install the latest recommended and security patches available from Sun. Then, keep the server up to date with the latest patch releases.

Threat level (2): TCP syn scanning
Since the server is not protected by a firewall, an attacker could scan the server's network ports looking for open services. This is a common information-gathering tactic.

Recommendation:
Any attacker wishing to gain knowledge of running services will probably scan for open ports as a first strike. Using a packet filtering router or stateful firewall will protect against these types of network reconnaissance. See appendix C for a TCP service listing provided by the NMAP network-scanning tool.

Threat level (1): File system attributes
The current servers operating system, Solaris 2.6, does not set properly "tuned" file modes for the system during the install. The default Solaris install sets un-secure file permissions. Again, This can give an attacker an edge when trying to exploit the server. Some exploits rely on this type of configuration in order to execute.

Recommendation:
Fix-modes is a shell script written by Casper Dik which makes extensive changes to the file and directory permissions on standard Solaris machines. Using the fix-modes script, file permissions may be modified in an effort to provide additional security. Setting the default root environment umask so that it does not include world access with 027 is also important. This keeps files created by root at least inaccessible by world. Also, be sure to set all daemons started by root with an acceptable umask value.

Configuration:

Threat level (3): Services running under inetd
This server's main role is IMS 2000 application based, with telnet based access. The /etc/inetd.conf is basically running all the default services (finger, time, etc). These services can be used as information gathering as well as exploited individually. These include RPC (Remote Procedure Call) weaknesses in rpc.ttdbserverd (tooltalk), rpc.cmsd (calendar manager) and rpc.statd, which allow immediate root compromise.

Recommendation:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The secure method is to disable the inetd process and shut down all the services it provides. 95 percent of these services are never even used. If any of the inetd services are absolutely necessary, then the recommendation is to use tcp_wrappers. Tcp_wrappers provides ip address based authentication, and is very customizable.

Threat level (2): SNMP
SNMP is the Simple Network Management Protocol with allows network monitoring and alarming based on pre-configured thresholds. It has always been dangerous to use because of the un-secure authentication scheme it uses (password on the network as clear text). This particular SNMP service is configured with the default community string password of "public". This is a well-known information gathering service and could guide a malicious person to a potential vulnerability.
Recommendation:
If this server is not currently being monitored with SNMP, then disable this service. If it needs SNMP then UC Davis has a good SNMP service that allows for ip-based access control.

Threat level (2): (r) command usage
The use of .rhosts and hosts.equiv on this system indicates host-based authentication which is easily spoofed and manipulated in order to gain un-authorized system access.
Recommendation:
The suggestion here is disable all use of the r-commands (rsh, rlogin and rexecd) in /etc/inetd.conf and use an alternative method of access. (SSH) It does not appear that this service is needed for normal operations of the server.

Threat level (2): Antivirus
The use the system as a NFS service mounted to a Windows drive mapping may allow a virus to spread from workstation to workstation.
Recommendation:
Again, the use of NFS is discouraged. If it cannot be disabled, an anti-virus software package must be installed. Also, the anti-virus software must be kept up to date with the latest virus definition files available from the vendor.

Threat level (2): /etc/rc startup scripts
Upon boot up, all services are started via the /etc/rc*.d directories. Most of these processes are not needed during normal server operations and can be disabled. This can give an attacker an edge when trying to exploit the server, especially if the attacker is local (on the console with user level access).
Recommendation:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The suggestion here is disable all non-essential startup scripts from /etc/rc2.d and /etc/rc3.d. Also, the system should never be in run states other than turned off, single-user, or full multi-user mode, so the recommendation is also to remove the /etc/rc0.d, /etc/rc1.d and /etc/rc3.d directories. See Appendix B for a current /etc/rc2.d and /etc/rc3.d directory listing.

Extra file system security:

- Install and monitor the tripwire software package(or use Sun's Solaris Fingerprint Database). These tools can be configured to log any file changes.
- Consider enabling Sun's built-in system accounting package and track system usage.
- Mount the /usr partition using the read-only option in /etc/vfstab.
- Monitor all essential log files for anomalous messages.
- Regularly check vendor web sites for updated patches and subscribe to any applicable mailing lists to stay informed.
- Configuring an admin group such as that found on most BSD derived systems can control execution of the su command.
    - /usr/sbin/groupadd -g 13 admin
    - /usr/bin/chgrp admin /usr/bin/su /sbin/su.static
    - /usr/bin/chmod 4550 /usr/bin/su /sbin/su.static

  Add users to the group "wheel" to allow su command execution.

Extra network service security:

- Install and use SSH for secure network access and file transfers.
- Use tcp_wrappers for ip-based authentication for services.
- Periodically run vulnerability scanners against the server in order to verify minimal services are running and there are no "new" vulnerabilities (Solaris 2.6 patches have been known to re-enable services that you have disabled).
- Edit the /etc/rc2.d/S74syslog file in order to prevent remote hosts to log locally, thus preventing a denial of service attack. Change the line containing:

  /usr/sbin/syslogd >/dev/msglog 2>&1 &

  to

  /usr/sbin/syslogd -t >/dev/msglog 2>&1 &

  By adding the -t option you can disable the syslogd logging of remote messages. (Solaris 8)
- Disable all "version" banners from any running services including sendmail, telnet and ftp.
    - Create a /etc/default/telnet file with banner="" as the only text.
    - Create a /etc/default/telnet file with banner="" as the only text.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

    - Modify the sendmail.cf file with the following line:
      O SmtpGreetingMessage=$j Sendmail $v/$Z; $b
- If FTP services are absolutely required, control access to the ftp daemon using the /etc/ftpusers file. Execute the following commands to create a fully populated /etc/ftpusers file. Remove users from this file to allow ftp access, never remove root from this file.
    - cat /etc/passwd | cut -f1 -d: > /etc/ftpusers
    - chown root /etc/ftpusers
    - chmod 600 /etc/ftpusers
- Create an /etc/issue file to display the following warning banner:
    - WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.
    - Copy the /etc/issue file to /etc/motd to also display this banner after the user is authenticated.

Installed Third Party Software Risks

The customer only intended to run the IMS 2000 portfolio management software package, but a few other software packages were found to be running also.

The IMS 2000 software has no known risks. The only drawback may be that it only supports Solaris 2.6, which is an aging operating system. The vendor has informed the security analyst that a Solaris 7 implementation has been dropped in favor of Solaris 8, which should be out by Q2, 2001.

HP JetAdmin has been installed for network printing to HP LaserJet printers. In the past, this software has been vulnerable to local attacks, which resulted in super-user account exploits. This was because the HP JetAdmin requires user root in order to modify printer configurations. Verify that the server absolutely needs to have a printing solution and that all other server-based printing options have been exhausted. The recommendation here is to discontinue using the server for printing services.

The server console runs the Common Desktop Environment (CDE) graphical user interface. There are numerous CDE vulnerabilities associated with this package. It has been determined that the CDE is not required for normal operations and should be disabled. The bonus here is the fact that CDE requires RPC services in order to execute. If CDE is disabled, then the RPC services can be disabled as well. This will eliminate even more services from the danger of being exploited.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sendmail 8.6 has known vulnerabilities and can be easily exploited. This could lead to un-authorized root level system access. If this server is not receiving mail from an outside host, this should be disabled. The recommendation is to create a ch-rooted environment for Sendmail using smrsh or install a different mail package, both of which are less likely to allow system compromise. Sendmail normally runs as root, which if successfully exploited, could allow a malicious person to raise their privilege level. Some alternatives to Sendmail include:

- Qmail
- Postfix
- Exim

This audit revealed that the Sendmail service on the server is open to Spam-Relay and should be disabled immediately.

Administrative Practices

QED is the third-party vendor, which developed the IMS 2000 application. This vendor sold the entire hardware/software solution as a turn-key Portfolio Management system. QED installs OS and application patches basically as they deem necessary. There is absolutely no pro-active patch update routine.

The customer does only basic administration on the server and has almost no experience with Solaris.

None of the logs are regularly inspected for anomalous or critical messages. This must be done in order to ensure minimum downtime. If the logs files are not regularly maintained, the customer might not be aware of the following events:

- Hardware errors that might predict a failure.
- Software errors, which could lead to data-corruption or worse.
- Buffer overflow attempts or exploits.
- Monitor who is accessing the system and for what purpose.
- Detection of other anomalous events.

Some suggestions are to limit and monitor what QED does on the server. Also, the customer must take all server administration responsibilities. QED does not have the customer's best interest in mind when it comes to server administration. QED's only concern is that the IMS 2000 application is in proper working order. A system change log is also highly recommended; due to the fact that more than one user has access to make system modifications. In order to securely log the server, a separate host should be setup to allow remote syslogs. This would provide log file protection against a nasty attacker running a root-kit after a successful exploitation.

Security Patches up to date

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Verification of the server's patch status was done using SUNS PatchDiag tool. This audit confirmed that the server's recommended and security patches are not up to date. See Appendix A for information on PatchDiag's output.

Install the latest recommended and security patches available from Sun. Then, keep the server up to date with the latest patch releases.

Sensitive data stored encrypted

The IMS 2000 application database has been determined (by the customer) to contain non-sensitive information.

Authentication information is the only other "privileged" data, which could be used to exploit the system. The /etc/shadow file is an access-restricted ASCII system file that stores users' encrypted passwords and related information. The use of encrypted shadow files is the default when Solaris is installed. The drawback is that the file may still be "cracked". One such tool that could be used to accomplish this is Crack. Crack is a security tool used to verify secure passwords. The /etc/shadow file has been audited using Crack with positive results. 4 out of 20 accounts were cracked in less than one hour, including the super-user account, which would control of the system.

In general, a good password will have a mix of lower and upper-case characters, numbers, and special characters, should be at least 6 characters long and should never appear in any dictionary (all languages apply). All user account passwords should be changed and conform to the guidelines set above.

Un-encrypted Network Communications

The protocols used to connect to the server are NFS, Telnet and FTP. The customer also connects to the X11 server for X11 sessions. All of these protocols produce network data that is susceptible to network "sniffing". This network data is transmitted in "clear text" which would allow a malicious person to capture authentication or other sensitive information. The third-party software vendor is allowed to access the server across the internet using telnet. The security analyst even found evidence of the vendor using telnet from their home ISP dialup account to access the server. The other protocol determined to be in use over the internet is ftp, which is equally susceptible to user/password "sniffing".

The installation and use of the SSH software package is highly recommended for secure communications. Discontinue use of (and disable) other services once SSH has been installed and tested.

SSH has numerous benefits, including:

- Protects all passwords and data (no authentication information sent in "clear text" to prevent the capture of passwords.)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Full replacement for telnet, rlogin, rsh, rcp, and ftp.
- Supports tcp_wrapper functionality that allows ip-address based authentication as well.
- Multiple strong authentication methods that prevent such security threats as spoofing identity.
- Authentication of both ends of connection, the server and the client are authenticated to prevent identity spoofing.
- Automatic authentication using agents to enable strong authentication to multiple systems with a single sign-on.
- Transparent and automatic tunneling of X11 sessions.
- Encryption and compression of data for security and speed.
- Multiple built-in authentication methods.
- Multiple ciphers for encryption, including e.g. 3DES, Blowfish and Twofish.

SSH creates a secure connection, which encrypts the data from client to server. SSH can take the place of all the above protocols except NFS. SSH uses SFTP, which could be used as a replacement for NFS. This would add a little more user interaction/authentication with the system. The reward is secure file transfers with authenticated users, something that this server's current NFS implementation cannot provide.

Antivirus Software is updated

The server currently has no virus scanning software since Windows-based users are mounting NFS-Shares as drive letters; the chance for a virus to be put on the system is high. Without running an anti-virus scanner on the server, the security analyst found traces of virus activity. The following is a listing from the servers /home directory:

-rwxrwxrwx 1 connie sysadmin 39936 Jun 20 13:03 life_stages.txt.shs*

This indicates that a well-known Windows/outlook virus was somehow able to infest the UNIX file system. This was most likely infected from the use of NFS.

As a general rule, if users are uploading files from Windows workstations, a virus scanning application must be installed and scheduled to run regularly. It also must be kept up to date with the latest virus signatures available from the vendor.

Access is Restricted to Authorized Users

Access to the server can be broken down into two categories:

Physical:

The physical location of the server is a communications closet offset from the system administrator's office. The communications closet

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

is basically a small storage area. The door is locked when not is use. Due to the closet space limitations, the server console sits on a desk facing the doorway. The chances of a malicious person "shoulder surfing" could pose a security risk by obtaining usernames/passwords. Also, if a malicious person were able to enter the data communications closet, it would almost be trivial for them to cause damage to the system due to the fact that the servers are not physically secured in lockable storage racks.

Access to the communications closet should only be allowed to key administrative personnel (systems administrator and the backup person). The customer should consider purchasing lockable equipment racks and securing all servers and associated peripherals.

Network:

The network has no firewall or intrusion detection system (IDS). Any malicious person connected to the internet could attempt to access or exploit the server. Upon initial walkthrough of the communications closet, the security analyst noted 6 analog modems connected to various Windows, LINUX and Solaris servers.

The recommendation here is to install a firewall and IDS system and monitor the logs each produces. This can indicate hacking/scanning trends and allow the administrator to harden systems accordingly. Only allowing access for the systems and users that need it, drastically cuts the potential vulnerabilities of the systems inside the network. This does not imply that the firewall will solve all security problems; a secure network utilizes a firewall, which protects hardened servers. Also, an audit of the modems in use needs to be done to validate the need for each. If it is not being utilized for anything, then the recommendation is to disconnect it.

Backup Policies and Disaster Preparedness

As mentioned in the executive summary, no policies of any kind exist. In order to ensure minimum server downtime, policies must be in place to protect the IMS 2000 application investment.

Current Practices:

The system is fully backed up to a 4mm DAT tape every weekday night with a job scheduled with cron. Tapes are rotated for 5 weeks and then get re-used. A tape is produced at the end of every month. This monthly tape is stored separately from the regular rotation of backup tapes and is only ever written to once. The software used to backup/restore is ufsdump/ufsrestore.

The system boot disk is not mirrored. The application data on the server is somewhat protected by software RAID-5. This is done using Solstice Disk Suite (SDS) version 4.2 utilizing three separate disks.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A standby-server is online and is used generally for application/database testing. It would be used in the event of a catastrophe.

The customer did not purchase a service contract with SUN, so only the basic warranty applies, which is inadequate because repairs and hardware replacements are not expedited.

Potential hazards:

Since the customer has no policies or documented procedures for backing up or restoring the server, it is very likely that a hardware failure could result in extended downtime.

There are also no policies/procedures for disaster recovery, which could hamper the transition time from the production server to the standby server. Also, without a security policy, no procedures are set into place for security related incidents, including a server compromise.

Since the customer only has one system administrator, backups go unchecked during vacation or sickness. If a major problem developed during the system administrator's absence, it could be devastating.

None of the backups are regularly tested for validity, and none are stored offsite. Potentially, all server data could be lost in a building fire.

Since the boot drive is not mirrored, a failure here would result in unnecessary downtime. The hard drive would have to be replaced (the customer has no spare hardware) and the OS data would have to be restored from tape.

The SDS 4.2 software has never been patched, and many patch bundles have been released. The current bundled patch version available from SUN is 106627-10. Which means the patch has gone through 10 revisions since the software was originally released.

Recommendations:

Develop policies for the most common types of events (backup/restore data, disaster recovery, security). Document the server and all "everyday" procedures associated with it. Execute "mock" failures and become familiar with the nuances with each type. A few security policies/procedures that should be in place include an *acceptable use policy* and *incident handling guidelines*.

Seek SUN professional training for the primary administrator. Select backup administrators and verify they have the skills to run the server during the primary admin's absence.

Data that has been copied to backup media normally uses minimal error checking. To validate the integrity of the information stored on the backup media, it must be restored. This should be done regularly to be sure the backup media is error-free.

The boot drive could be mirrored to another disk using SDS. It also could be mirrored offline using a simple dd script. The advantage of using SDS is that the duplicate always contains current data, where the dd script only captures an image of the data.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Keep all associated hardware and software up to date with patches. This is sometimes very important because the risk here is potential data loss or corruption.

Conclusion

This server was found to be a very easy target to be exploited, both by system mis-configuration and un-patched software. Due to the major holes found, this machine has probably already been exploited. This means that the only way to successfully secure this server is a complete operating system re-install. Securing the system "as-is" can be performed, but under the current circumstances the system may never be secure. Solaris 2.6 is an aging OS and may be dropped as a supported Sun product in the near future. Installing a current release OS (Solaris 7 or 8), and then "hardening" the server is the preeminent way to proceed. The customer should also install a firewall and intrusion detection system before an OS re-install to protect from future attacks. Below are some guidelines and appropriate man-hours to implement each step.

Step	Time (hours)	Difficulty	Outcome
Disconnect Server	NA	Trivial	Immediately disconnecting the server from the network is suggested in order to avoid any further exploitation.
Application verification	40-80	Medium	Verify all application and database data to ensure no malicious code has been introduced; May require vendor services
Application backup	16	Trivial	Dump all IMS 2000 application and database data to tape and verify (twice)
OS installation	8	Light	Install the latest release of Solaris (bare minimum OS)
OS hardening	8	Heavy	Secure the OS using latest tools and techniques, removing non-essential services and using secure services to access the server
Application restore	8	Trivial	Restore all IMS application and database data, then verify data integrity
Application verification	8	Medium	Verify normal application behavior and operation
Reconfigure network	8	Light	Consider changing IP address numbers
Setup secure network	NA	Heavy	Install a firewall and intrusion detection system to protect the entire network
Reconnect server	NA	Trivial	Reconnect the file server AFTER securing the network
System Policies	40-80	Medium	Develop and test system policies and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

			procedures.
Server Monitoring	NA	NA	Continue to monitor the server for any anomalies; Setup a firewall and compliment this with an Intrusion Detection System

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A

PatchDiag tool output:

```
================================================================================
System Name: server     SunOS Vers: 5.6        Arch: sparc
Cross Reference File Date: Oct/24/00

PatchDiag Version: 1.0.4
================================================================================
Report Note:

Recommended patches are considered the most important and highly
recommended patches that avoid the most critical system, user, or
security related bugs which have been reported and fixed to date.
A patch not listed on the recommended list does not imply that it
should not be used if needed.  Some patches listed in this report
may have certain platform specific or application specific dependencies
and thus may not be applicable to your system.  It is important to
carefully review the README file of each patch to fully determine
the applicability of any patch with your system.
================================================================================
INSTALLED PATCHES
Patch  Installed Latest   Synopsis
  ID   Revision  Revision
------ -------- -------- ------------------------------------------------------
104172   16       23    Solstice DiskSuite 4.1: Product patch
105160   02       12    CDE 1.2: dtterm libDtTerm.so.1 patch
105181   20       23    SunOS 5.6: Kernel update patch
105189   02       03    OBSOLETED by 106040
105210   27       32    SunOS 5.6: libaio, libc & watchmalloc patch
105214   01    CURRENT  OBSOLETED by 105181
105216   03       04    SunOS 5.6: /usr/sbin/rpcbind patch
105222   03    CURRENT  OBSOLETED by 105181
105223   04       05    SunOS 5.6: pln/soc drivers & ssafirmware patch
105284   33       37    Motif 1.2.7: Runtime library patch
105338   07       25    CDE 1.2: dtmail patch
105356   05       16    SunOS 5.6: /kernel/drv/ssd and /kernel/drv/sd patch
105357   01       04    SunOS 5.6: /kernel/drv/ses patch
105360   10       34    Creator 2.6: FFB Graphics Patch
105361   03       11    VIS/XIL 2.6: Graphics Patch
105362   08       28    PGX 2.6: M64 Graphics Patch
105363   05       31    Elite3D 2.6: AFB Graphics Patch
105364   01       02    SunOS 5.6: SX Graphics Patch
105375   07       25    SunOS 5.6: sf & socal driver patch
105377   03       05    SunOS 5.6: BCP patch
105379   03       06    SunOS 5.6: /kernel/misc/nfssrv patch
105390   02    CURRENT  SunOS 5.6: SGML Manual Pages Patch
105393   02       07    OBSOLETED by 105621
105397   02    CURRENT  SunOS 5.6: /usr/sbin/passmgmt patch
105400   02    CURRENT  SunOS 5.6: Greek keyboard layout incorrect on Sparc
105401   09       28    SunOS 5.6: libnsl and NIS+ commands patch
105403   01       03    SunOS 5.6: ypbind/ypserv patch
105405   01       02    SunOS 5.6: libcurses.a & libcurses.so.1 patch
105407   01    CURRENT  SunOS 5.6: /usr/bin/volrmmount patch
105416   01    CURRENT  SunOS 5.6: /usr/lib/acct/acctdisk patch
105421   01    CURRENT  SunOS 5.6: /etc/init.d/asppp patch
105426   01    CURRENT  SunOS 5.6: /usr/lib/libtnfprobe.so.1 patch
105464   02    CURRENT  OpenWindows 3.6: Multiple xterm fixes
105472   02       07    SunOS 5.6: /usr/lib/autofs/automountd patch
105486   02       04    SunOS 5.6: /kernel/fs/hsfs patch
105490   04       07    OBSOLETED by 107733
105492   02    CURRENT  SunOS 5.6: cgsix driver patch
105497   01    CURRENT  OpenWindows 3.6: printtool patch
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

105516 01 05 SunOS 5.6: /usr/lib/fs/ufs/fsck and mountall patch
105518 01 CURRENT OBSOLETED by 105395
105528 01 CURRENT SunOS 5.6: /kernel/drv/be patch
105529 01 09 SunOS 5.6: /kernel/drv/tcp patch
105552 02 03 SunOS 5.6: /usr/sbin/rpc.nisd_resolv patch
105558 01 04 CDE 1.2: dtpad patch
105562 01 03 SunOS 5.6: chkey and keylogin patch
105564 02 04 SunOS 5.6: /kernel/misc/rpcsec patch
105566 07 08 CDE 1.2: calendar manager patch
105568 16 18 SunOS 5.6: /usr/lib/libthread.so.1 patch
105570 01 05 SunVideo 1.3: Patch
105572 03 11 OBSOLETED by 106625
105580 05 16 SunOS 5.6: /kernel/drv/glm patch
105600 05 19 SunOS 5.6: /kernel/drv/isp patch
105604 05 09 OBSOLETED by 105181
105615 03 08 SunOS 5.6: /usr/lib/nfs/mountd patch
105618 01 CURRENT OpenWindows 3.6: Xcms patch
105621 19 24 SunOS 5.6: c2audit, libbsm and cron patch
105630 01 02 CDE 1.2: libDtWidget patch
105633 38 48 OpenWindows 3.6: Xsun patch
105637 01 CURRENT SunOS 5.6: /usr/lib/power/powerd patch
105642 03 08 SunOS 5.6: prtdiag patch
105651 06 12 SunOS 5.6: ac/environ/fhc/sysctrl driver patch
105654 03 CURRENT SunOS 5.6: driver_aliases/driver_classes/name_to_major patch
105669 10 CURRENT CDE 1.2: libDtSvc Patch
105686 02 CURRENT OBSOLETED by 105621
105693 03 09 SunOS 5.6: cachefs patch
105703 03 23 CDE 1.2: dtlogin patch
105705 02 CURRENT SunOS 5.6: /usr/kernel/drv/audiocs patch
105718 02 CURRENT SunOS 5.6: /usr/bin/su patch
105720 03 12 SunOS 5.6: /kernel/fs/nfs patch
105722 01 05 SunOS 5.6: /usr/lib/fs/ufs/ufsdump and ufsrestore patch
105724 01 CURRENT OBSOLETED by 105722
105736 01 CURRENT OBSOLETED by 105395
105741 02 07 SunOS 5.6: /kernel/drv/ecpp patch
105742 03 05 SunOS 5.6: /kernel/drv/le patch
105743 01 CURRENT OBSOLETED by 107228
105746 01 02 SunOS 5.6: /usr/bin/cpio patch
105755 03 08 SunOS 5.6: libresolv, in.named, named-xfer, nslookup, nstest patch
105757 01 CURRENT SunOS 5.6: /usr/bin/echo patch
105778 01 CURRENT SunOS 5.6: /kernel/fs/specfs patch
105780 01 05 SunOS 5.6: /kernel/fs/fifofs patch
105786 03 13 SunOS 5.6: /kernel/drv/ip patch
105792 02 05 SunOS 5.6: /usr/sbin/tar patch
105795 03 08 SunOS 5.6: /kernel/drv/hme patch
105797 02 06 OBSOLETED by 105356
105798 03 CURRENT SunOS 5.6: sun4m, sun4u & sun4u1 cprboot patch
105800 05 06 SunOS 5.6: /usr/bin/admintool, y2000 patch
105802 03 12 OpenWindows 3.6: ToolTalk patch
105836 02 03 SunOS 5.6: /kernel/drv/qe patch
105837 02 03 CDE 1.2: dtappgather Patch, including SDE 1.0 installations
105845 01 CURRENT OBSOLETED by 105621
105847 01 07 SunOS 5.6: /kernel/drv/st.conf and /kernel/drv/st patch
105867 01 CURRENT SunOS 5.6: /usr/sbin/tapes patch
105924 03 10 SunOS 5.6: kbd, se and zs drivers patch
105926 01 CURRENT SunOS 5.6: /usr/sbin/static/tar patch
105953 01 CURRENT SunOS 5.6: /usr/bin/xargs patch
105959 01 CURRENT SunOS 5.6: /usr/kernel/strmod/ppp patch
105988 01 CURRENT SunOS 5.6: /usr/sbin/rwall patch
105990 01 03 SunOS 5.6: vi/ex/edit/view/vedit patch
106025 01 CURRENT CDE 1.2: sdtfprop patch for group permissions
106027 01 09 CDE 1.2 / SDE 1.0: dtsession patch
106029 01 04 SunOS 5.6: /usr/ccs/bin/sccs and /usr/ccs/bin/make patch
106031 02 CURRENT OBSOLETED by 105181
106033 01 CURRENT OBSOLETED by 105621
106035 01 CURRENT SunOS 5.6: /usr/bin/getopt patch
106040 13 14 SunOS 5.6: X Input & Output Method patch
106044 01 03 SunOS 5.6: /usr/lib/nss_nisplus.so.1 patch
106049 01 CURRENT SunOS 5.6: /usr/sbin/in.telnetd patch
106064 01 CURRENT OBSOLETED by 105621

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

106075 01 CURRENT OBSOLETED by 105621
106084 01 04 OBSOLETED by 107013
106112 01 06 CDE 1.2: dtfile patch
106123 01 04 SunOS 5.6: sgml patch
106125 07 10 SunOS 5.6: Patch for patchadd and patchrm
106138 01 CURRENT OpenWindows 3.6: mp fails to set correct A4 paper size information
106141 01 CURRENT SunOS 5.6: /usr/bin/mkdir patch
106150 01 03 SunOS 5.6: in.dhcpd and pntadm patch
106168 02 CURRENT SunOS 5.6: dma driver patch
106169 02 CURRENT SunOS 5.6: sbusmem driver patch
106170 02 03 SunOS 5.6: /kernel/drv/esp patch
106171 01 CURRENT SunOS 5.6: /kernel/drv/lebuffer patch
106172 02 04 SunOS 5.6: /kernel/drv/fas patch
106173 02 03 SunOS 5.6: /kernel/misc/scsi patch
106183 03 05 SunOS 5.6: cfgadm utility & libraries
106193 03 05 SunOS 5.6: y2000 sysid unzip patch
106216 01 03 SunOS 5.6: /platform/sun4u/kernel/drv/envctrl patch
106219 01 03 SunOS 5.6: luxadm.1m Manual Page Patch
106260 01 CURRENT SunOS 5.6: Manual Pages Patch for ffbconfig.1m
106261 01 CURRENT SunOS 5.6: Manual Pages Patch cfgadm.1m config_admin.3x libcfgadm.
106262 01 CURRENT SunOS 5.6: Manual Pages Patch for qfe.7d
106317 01 CURRENT SunOS 5.6: upgrade_script terminated abnormally during upgrade
106323 01 CURRENT SunOS 5.6: /etc/inet/services patch
106828 01 CURRENT SunOS 5.6: /usr/bin/date patch
107492 01 CURRENT SunOS 5.6: Y2000, runacct cannot update /var/adm/acct/sum/loginlog
107733 06 09 SunOS 5.6: Linker patch
107988 01 CURRENT SunOS 5.6: Patch for SPARCompiler Binary Compatibility Libraries
==========

UNINSTALLED RECOMMENDED PATCHES

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
105395	N/A	06	498			SunOS 5.6: /usr/lib/sendmail patch
105665	N/A	03	777			SunOS 5.6: /usr/bin/login patch
105667	N/A	02	740			SunOS 5.6: /usr/bin/rdist patch
106222	N/A	01	911			OpenWindows 3.6: filemgr (ff.core) fixes
106226	N/A	01	876			SunOS 5.6: /usr/sbin/format patch
106235	N/A	06	86			SunOS 5.6: lp patch
106242	N/A	02	658			CDE 1.2: libDtHelp.so.1 fixes
106257	N/A	05	265			SunOS 5.6: /usr/lib/libpam.so.1 patch
106271	N/A	06	397			SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
106292	N/A	09	204			SunOS 5.6: pkgadd/pkginstall & related utilities
106301	N/A	01	904			SunOS 5.6: /usr/sbin/in.ftpd patch
106415	N/A	03	540			OpenWindows 3.6: xdm patch
106437	N/A	03	267	105669-06		CDE 1.2: Print Manager Patch
106439	N/A	06	231			SunOS 5.6: /usr/sbin/syslogd patch
106448	N/A	01	834			SunOS 5.6: /usr/sbin/ping patch
106468	N/A	02	209			SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
106495	N/A	01	855			SunOS 5.6: truss & truss support library patch
106522	N/A	04	159			SunOS 5.6: /usr/bin/ftp patch
106569	N/A	01	770			SunOS 5.6: libauth.a & libauth.so.1 patch
106592	N/A	03	194			SunOS 5.6: /usr/lib/nfs/statd patch
106625	N/A	08	120			SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/ufs patch
106639	N/A	05	120			SunOS 5.6: /kernel/strmod/rpcmod patch
106648	N/A	01	784			OpenWindows 3.6: libce suid/sgid security fix
106649	N/A	01	784			OpenWindows 3.6: libdeskset patch
106650	N/A	04	309	106648-01 106649-01		OpenWindows 3.6: mailtool attachment security patch
106834	N/A	01	643			SunOS 5.6: cp/ln/mv patch
106882	N/A	02	58			SunOS 5.6: /usr/lib/nfs/nfsd patch
106894	N/A	01	660			SunOS 5.6: /usr/bin/uux patch
107336	N/A	01	586			OpenWindows 3.6: KCMS configure tool has a security vulnerability
107434	N/A	01	569			CDE 1.2: Spell checking occasionally kills mail
107565	N/A	02	376			SunOS 5.6: /usr/sbin/in.tftpd patch
107618	N/A	01	351			SunOS 5.6: Permissions problem in /vol.
107758	N/A	01	518			SunOS 5.6: Pax incorrectly change mode of symlink target file
107766	N/A	01	443			SunOS 5.6: ASET cklist reports unchanged 6month older files as new

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

107774 N/A 01 505 SunOS 5.6: inetd denial-of-service attack
107991 N/A 01 488 SunOS 5.6: /usr/sbin/static/rcp patch
108199 N/A 01 408 CDE 1.2: dtspcd Patch
108201 N/A 01 408 CDE 1.2: dtaction Patch
108307 N/A 02 194 SunOS 5.6: keyserv fixes
108333 N/A 02 70 SunOS 5.6: jserver buffer overflow
108346 N/A 03 194 SunOS 5.6: patch usr/sbin/rpc.nispasswdd
108468 N/A 02 153 SunOS 5.6: ldterm streams module fixes
108492 N/A 01 323 SunOS 5.6: Snoop may be exploited to gain root access
108499 N/A 01 275 SunOS 5.6: ASET sets the gid on /tmp, /var/tmp when setting med hi
108660 N/A 01 306 SunOS 5.6: Patch for sadmind
108804 N/A 01 142 SunOS 5.6: tip has buffer overrun with security implications
108890 N/A 01 194 SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
108893 N/A 01 194 SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
108895 N/A 01 194 SunOS 5.6: patch /usr/sbin/rpc.bootparamd
109266 N/A 01 169 SunOS 5.6: security: /bin/mail has buffer overflow
109339 N/A 01 153 SunOS 5.6: nscd has a potential security problem
109388 N/A 01 145 SunOS 5.6: patch /usr/vmsys/bin/chkperm
==========

UNINSTALLED SECURITY PATCHES

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

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
105395	N/A	06	498			SunOS 5.6: /usr/lib/sendmail patch
105665	N/A	03	777			SunOS 5.6: /usr/bin/login patch
105667	N/A	02	740			SunOS 5.6: /usr/bin/rdist patch
106222	N/A	01	911			OpenWindows 3.6: filemgr (ff.core) fixes
106235	N/A	06	86			SunOS 5.6: lp patch
106257	N/A	05	265			SunOS 5.6: /usr/lib/libpam.so.1 patch
106271	N/A	06	397			SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
106301	N/A	01	904			SunOS 5.6: /usr/sbin/in.ftpd patch
106415	N/A	03	540			OpenWindows 3.6: xdm patch
106437	N/A	03	267	105669-06		CDE 1.2: Print Manager Patch
106448	N/A	01	834			SunOS 5.6: /usr/sbin/ping patch
106468	N/A	02	209			SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
106522	N/A	04	159			SunOS 5.6: /usr/bin/ftp patch
106569	N/A	01	770			SunOS 5.6: libauth.a & libauth.so.1 patch
106592	N/A	03	194			SunOS 5.6: /usr/lib/nfs/statd patch
106625	N/A	08	120			SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/ufs patch
106629	N/A	20	209	105181-08		SunOS 5.6: CS6400 kernel update patch
106639	N/A	05	120			SunOS 5.6: /kernel/strmod/rpcmod patch
106648	N/A	01	784			OpenWindows 3.6: libce suid/sgid security fix
106649	N/A	01	784			OpenWindows 3.6: libdesksetpatch
106650	N/A	04	309	106648-01 106649-01		OpenWindows 3.6: mailtool attachment security patch
106834	N/A	01	643			SunOS 5.6: cp/ln/mv patch
106882	N/A	02	58			SunOS 5.6: /usr/lib/nfs/nfsd patch
106894	N/A	01	660			SunOS 5.6: /usr/bin/uux patch
107336	N/A	01	586			OpenWindows 3.6: KCMS configure tool has a security vulnerability
107565	N/A	02	376			SunOS 5.6: /usr/sbin/in.tftpd patch
107618	N/A	01	351			SunOS 5.6: Permissions problem in /vol.
107758	N/A	01	518			SunOS 5.6: Pax incorrectly change mode of symlink target file
107766	N/A	01	443			SunOS 5.6: ASET cklist reports unchanged 6month older files as new
107774	N/A	01	505			SunOS 5.6: inetd denial-of-service attack
107991	N/A	01	488			SunOS 5.6: /usr/sbin/static/rcp patch
108199	N/A	01	408			CDE 1.2: dtspcd Patch
108201	N/A	01	408			CDE 1.2: dtaction Patch
108307	N/A	02	194			SunOS 5.6: keyserv fixes
108333	N/A	02	70			SunOS 5.6: jserver buffer overflow
108346	N/A	03	194			SunOS 5.6: patch usr/sbin/rpc.nispasswdd
108468	N/A	02	153			SunOS 5.6: ldterm streams module fixes
108492	N/A	01	323			SunOS 5.6: Snoop may be exploited to gain root access
108499	N/A	01	275			SunOS 5.6: ASET sets the gid on /tmp, /var/tmp when setting med hi
108660	N/A	01	306			SunOS 5.6: Patch for sadmind

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

108804	N/A	01	142	SunOS 5.6: tip has buffer overrun with security implications
108890	N/A	01	194	SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
108893	N/A	01	194	SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
108895	N/A	01	194	SunOS 5.6: patch /usr/sbin/rpc.bootparamd
109266	N/A	01	169	SunOS 5.6: security: /bin/mail has buffer overflow
109339	N/A	01	153	SunOS 5.6: nscd has a potential security problem
109388	N/A	01	145	SunOS 5.6: patch /usr/vmsys/bin/chkperm

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix B

/etc/rc2.d and /etc/rc3.d directory listings. The items listed in red are not required for normal server operation.

```
lrwxrwxrwx   1 root     root          13 Oct 25  1999 K20spc -> ../init.d/spc
-rwxr--r--   5 root     sys         1738 Jul 15  1997 K60nfs.server
-rwxr-xr-x   3 root     sys          677 Jul 15  1997 K76snmpdx
-rwxr-xr-x   3 root     sys          951 Jul 15  1997 K77dmi
-rw-r--r--   1 root     sys         1369 Jul 15  1997 README
-rwxr--r--   3 root     sys          619 Jul 15  1997 S01MOUNTFSYS
-rwxr--r--   2 root     sys         2272 Jul 15  1997 S05RMTMPFILES
-rwxr--r--   2 root     sys          822 Jul 15  1997 S20sysetup
-rwxr--r--   2 root     sys          548 Jul 15  1997 S21perf
-rwxr-xr-x   2 root     other       1644 Jul  2  1997 S30sysid.net
-rwxr--r--   4 root     sys         1474 Jan 15  1998 S47asppp
-rwxr--r--   2 root     sys         5645 Jul 15  1997 S69inet
-rwxr--r--   2 root     sys          212 Jul 15  1997 S70uucp
-rwxr--r--   4 root     sys         2891 Jul 15  1997 S71rpc
-rwxr-xr-x   2 root     other       1498 Jul  2  1997 S71sysid.sys
-rwxr-xr-x   2 root     other       1558 Jul  2  1997 S72autoinstall
-rwxr--r--   2 root     sys         4386 Jul 15  1997 S72inetsvc
-rwxr--r--   2 root     sys          579 Jul 15  1997 S73cachefs.daemon
-rwxr--r--   4 root     sys         1236 Jul 15  1997 S73nfs.client
-rwxr--r--   4 root     sys          602 Jul 15  1997 S74autofs
-rwxr--r--   4 root     sys          621 Jul 15  1997 S74syslog
-rwxr--r--   4 root     sys         1266 Jul 15  1997 S74xntpd
-rwxr--r--   4 root     sys          513 Jul 15  1997 S75cron
lrwxrwxrwx   1 root     other         21 Dec  2  1999 S75etherlite -> /etc/init.d/etherlite
-rwxr--r--   4 root     sys          568 Jul 15  1997 S76nscd
-rwxr--r--   2 root     sys          218 Jul 15  1997 S80PRESERVE
-rwxr--r--   4 root     sys          403 Jul 15  1997 S80lp
lrwxrwxrwx   1 root     root          13 Oct 25  1999 S80spc -> ../init.d/spc
-rwxr--r--   3 root     sys         2452 Jul 15  1997 S85power
-rwxr--r--   4 root     sys         1215 Jul 15  1997 S88sendmail
-rwxr--r--   4 root     sys          492 Jul 15  1997 S88utmpd
lrwxrwxrwx   1 root     root          31 Oct 25  1999 S89bdconfig -> ../init.d/buttons_n_dials-setup
lrwxrwxrwx   1 root     other         17 Dec  6  1999 S90hpnpd -> /etc/init.d/hpnpd
-rwxr-xr-x   2 root     sys          1759 Apr  2  1998 S91afbinit
-rwxr--r--   2 root     sys         1400 May 20  1997 S91agaconfig
-rwxr-xr-x   2 root     sys         2433 Nov 25  1996 S91leoconfig
-r-xr-xr-x   2 root     sys         1159 Jun 27  1997 S92rtvc-config
-rwxr--r--   3 root     sys          524 Jul 15  1997 S92volmgt
-rwxr--r--   2 root     sys          373 Jul 15  1997 S93cacheos.finish
lrwxrwxrwx   1 root     other         21 Oct 25  1999 S95SUNWmd.sync -> ../init.d/SUNWmd.sync
-rwxr-xr-x   1 root     other        850 Dec  2  1999 S98upsd
-rwxr--r--   4 root     sys          460 Jul 15  1997 S99audit
-rwxr--r--   4 root     sys         2613 Jun 26  1997 S99dtlogin
nmsic1# ls -l /etc/rc3.d
total 16
-rw-r--r--   1 root     sys         1708 Jul 15  1997 README
-rwxr--r--   5 root     sys         1738 Jul 15  1997 S15nfs.server
lrwxrwxrwx   1 root     other         21 Oct 25  1999 S25mdlogd -> ../init.d/init.mdlogd
-rwxr-xr-x   1 root     other        448 Oct  9  1998 S33hclnfs
-rwxr-xr-x   3 root     sys          677 Jul 15  1997 S76snmpdx
-rwxr-xr-x   3 root     sys          951 Jul 15  1997 S77dmi
```

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix C

NMAP output: (This inventories the listening TCP network services on the system)

```
Starting nmap V. 2.53 by fyodor@insecure.org (www.insecure.org/nmap/)
Host  (server) appears to be up ... good.
Initiating SYN half-open stealth scan against  (server)
Adding TCP port 32771 (state open).
Adding TCP port 37 (state open).
Adding TCP port 19 (state open).
Adding TCP port 2049 (state open).
Adding TCP port 32777 (state open).
Adding TCP port 79 (state open).
Adding TCP port 6112 (state open).
Adding TCP port 7100 (state open).
Adding TCP port 515 (state open).
Adding TCP port 21 (state open).
Adding TCP port 32780 (state open).
Adding TCP port 32773 (state open).
Adding TCP port 7 (state open).
Adding TCP port 13 (state open).
Adding TCP port 540 (state open).
Adding TCP port 514 (state open).
Adding TCP port 32774 (state open).
Adding TCP port 6000 (state open).
Adding TCP port 111 (state open).
Adding TCP port 23 (state open).
Adding TCP port 32779 (state open).
Adding TCP port 1103 (state open).
Adding TCP port 32775 (state open).
Adding TCP port 513 (state open).
Adding TCP port 9 (state open).
Adding TCP port 25 (state open).
Adding TCP port 32776 (state open).
Adding TCP port 4045 (state open).
Adding TCP port 2766 (state open).
Adding TCP port 32772 (state open).
Adding TCP port 512 (state open).
The SYN scan took 259 seconds to scan 1541 ports.
```

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Sys Admin, November 2000, Securing Solaris, Ido Dubrawsky
Solaris Practicum (6.6), Hal Pomeranz, SANS 2000
Running Unix Applications Securely (6.4), Lee Brotzman-Hal Pomeranz, SANS 2000
UNIX Security Tools and Their Uses (6.3), Matt Bishop, SANS 2000
IMS 2000 http://www.qedinfo.com
AntiOnline.com, http://www.antionline.com/cgi-bin/anticode/anticode.pl?dir=solaris-exploits
SecurityFocus.com, http://www.securityfocus.com
Fix-modes, ftp://ftp.fwi.uva.nl/pub/solaris/fix-modes.tar.gz

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.