Global Information Assurance Certification Paper

Security Assessment
for
GIAC Enterprises

November 2000

Dan Rose[1]
Solaris Security Analyst
511 CountyRoad 1331
Bridgeport, TX 76426

November 18, 2000

EXECUTIVE SUMMARY

This document contains a security evaluation of a single mission-critical UNIX server at GIAC Enterprises. Because GIAC is taking a more aggressive Internet-Business posture and because GIAC is becoming more internally dependant on its growing UNIX infrastructure, steps must be taken now to ensure that these mission critical systems are not compromised from external or internal attack.

This report will focus on GIAC's internal DNS/DHCP server in an effort to provide GIAC with a specific and immediate plan of action for that server, while also providing a template, or starting point, whereby other similar GIAC UNIX servers could be secured.

The internal DNS/DHCP server, at GIAC, warrants immediate attention because it provides a critical service to all desktops and to many servers at GIAC. The service area includes the corporate offices as well as all remote offices except Hawaii. The impact of a compromise on this server could be very significant to GIAC because this server is depended on ***and trusted by*** so many machines at GIAC.

To repeat, to lose the integrity of this server means not only the loss of the services it provides company wide, but also the potential compromise of any machines that trust this server.

Summary of Findings

- Probability of attack is high for this server.
- Many unnecessary services and packages are installed with vulnerabilities.
- Security patches and system audits are not periodically reviewed.
- Administrative access is not through encrypted or secured means.
- System file permissions are set too permissive.
- User account security is very weak.
- No file integrity checker is currently deployed for this server.
- System logs are at inadequate levels and easily subverted.
- Corporate Security Policies are not clearly defined and enforced.

Audit Conclusion

The server is primarily secured with the recommended security patches, of the manufacturer, from the time of installation. These patches are out of date and many other measures are missing that would place this server within best business security practices. The missing areas will be detailed and prioritized for optimum benefit. Some of the security steps already implemented will be mentioned for completeness, and to the credit of the local administrators.

Understanding Security Risks

Because this server is available to all internal networks, and provides services to a large client base over a large geographic area, the chance of attack is significant.

GIAC should not discount internal threats because there appear to be few internal users with sufficient knowledge to break into a UNIX server. The fact is that security vulnerabilities continue to be discovered and published on the Internet. These published vulnerabilities target mainstream operating systems and applications and in many cases include very simple cookbook steps necessary to break into a system.

Further, GIAC should not place blind trust in a firewall, as there are regular and often reports of internal machines being compromised via an internet server that was given only minimum access through the firewall. Furthermore, GIAC allows constant direct connectivity to its business partners without a firewall.

Finally, GIAC should not place confidence in any perceived lack of motive. While GIAC may presently have only a minor internet presence, the fact remains that many external attacks are launched on broad ranges of internet addresses for the purpose of finding host machines with which to launch much grander attacks.

Internal attacks arise from a variety of motives that range from the deliberate malicious to those seeking a technical challenge, to those just curious to know "if it is really all that easy to break into a server".

It should be understood that there is no such thing as a usable machine that is 100% secure. While the purpose of this document is not to spread doom and gloom, it aims to make the reader more aware of the threats and to encourage security through depth, instead of trust in any one security measure.

SYSTEM DESCRIPTION

The DNS/DHCP server here evaluated is a UNIX machine from Sun Microsystems Inc.[2] that was initially deployed November 10, 1999. Because this machine has operated for over one year without strong security measures, chances are higher that the machine has already been compromised. A file integrity check should be performed right away.

This server provides DHCP and DNS service to desktop PC's company wide, and DNS services for UNIX desktops and most UNIX and NT servers. While business hours are the primary exposure, jobs that are scheduled through the night also depend on DNS services. The secondary DNS/DHCP server has been deployed at a remote location in a effort to provide redundancy. Because the two servers are very similar, it must be understood that a successful attack against one server would be just as successful against the other. The hardware redundancy offers little against a security attack.

Description of the DNS/DHCP server is as follows:

Model	Ultra 10[3]
OS	Solaris 2.6[4]
Hostname	abqnet1
IP address	10.0.11.1
Mac address	8:0:20:b5:e1:11
Serial Number	FW94240111
Hostid	80b5e111
Kernel version	105181-10
Boot Prom version	OBP 3.19.4
CPU	1 X UltraSPARC-IIi@440MHZ and 2MB cache
Physical Memory	512MB
Swap	1GB
Disk	Internal=8.5GB
Network	Class-C address space on Switched 100Mbit Ethernet
Key Applications	DNS/DHCP with Cisco's NetworkRegistrar3.0[5]
Location	Tiger Plaza, Network Room E601, In locked cabinet
External Hardware	VT Terminal connected to serial port A
Hardware Redundancy	None locally, but note that a secondary server exists

.

- While a secondary/failover DNS/DHCP server exists, this evaluation focuses only on the primary. Solutions recommended should be deployed on both machines.

ANALYSIS

This section is mostly a listing of unresolved security issues. This is a logical grouping and not in order of priority.

1) Operating System Vulnerabilities

Sun Microsystems expends much effort in securing their operating systems while trying to balance ease of use. This "ease of use" combined with the complexity of modern operating systems have lent them to vulnerabilities, that when successfully exploited, may alter data, disclose sensitive data, disable the system, or cause the system to perform other undesirable and unauthorized functions. Inherent weaknesses of the default Solaris install are listed here.

a) ***Password strength*** is minimal because Solaris passwords are encrypted with a DES-56bit algorithm, which has been cracked.[6]

b) ***Core Dumps*** are enabled by default, which can allow memory dumps to be scanned for passwords or other sensitive data. Core dumps are normally written as world readable which makes them easy for anyone to scan. A core dump scan was demonstrated to the GIAC security team.

c) ***Buffer Overflow*** execution is allowed by the kernel by default. Root executed programs could be exploited to take over the machine.

d) ***Setuid Programs*** exist and are not documented, and have not been reduced with respect to the primary function of this server. Additionally, the nosuid option is omitted for /var, /export, and /opt filesystems. Setuid Scripts are particularly vulnerable. See Appendixes 5 and 7.

```
% find / -user root \( -perm –4000 –o –perm –2000 \) -ls
```

e) ***/usr mounted rw*** by default. This should be mounted read-only to prevent introduction of compromised programs.

f) ***Authentication logging*** is not recorded by default on Solaris. This information is useful to see failed login attempts, su attempts, reboots and other security information.

g) ***System and Process*** accounting are not enabled by default.

h) ***Permissive Umask*** for root level file creation is set by default for all boot-time scripts.

i) ***Permissive file permissions*** exist throughout the OS by default.

j) ***Eeprom security*** is not enabled by default. Reboots are allowed by any with physical access.

2) Configuration Vulnerabilities

Many vulnerable network services are configured and enabled at this time.

a) ***NFS client*** vulnerabilities exist and are easily exploitable on abqnet1 at this time. Presently, any users that can log on to abqnet1 can take control of any devices, including disk devices or even the boot prom. This means that they can read/write any file on abqnet1, even if the permissions of that file explicitly deny access. This includes password/shadow files, or any sensitive data files. This vulnerability was demonstrated to the security team at GIAC, after management approval. See also RCP vulnerabilities below.

b) ***Sendmail*** daemon is running even though this host is not a mail server. This daemon has historically had many vulnerabilities. Sendmail buffer overflows are currently one of the top ten threats to the Internet.

c) ***RPC service*** vulnerabilities exist and are easily exploitable on abqnet1 at this time. The rpcbind daemon in support of the various rpc services uses a very weak client authentication method which opens a variety of vulnerabilities. RPC issues are currently one of the top ten threats to the Internet. These rpc services are presently enabled ***unnecessarily*** via the /etc/inetd.conf file. These include rquotad, rusersd, sprayd, walld, kcms_server, cachefsd, kerbd, rstatd, rpc.cmsd and rpc.ttdbservd. The last three of which have recently suffered immediate root level compromises on the Internet. See Appendix 2.

d) ***Telnet and ftp*** vulnerabilities exist because these services use passwords and data sent in the clear, and because they presently have inadequate logging of the access, and presently do not restrict access to a defined list of machines. Password snooping was demonstrated to the security team at GIAC.

e) ***Rlogin, rsh and rexecd*** are available and vulnerable at this time. These services are vulnerable for the same reasons as telnet and ftp, but are additionally vulnerable because they employ the use of .rhosts files which allow the users to set host-level trust relationships that may not be sound.

f) ***Other Network services*** are also being run ***unnecessarily*** from /etc/inetd.conf. Services such as comsat, talk, uucp, finger, time, printer, xaudio. Services that are not in use should be disabled until they are needed. See Appendixes 2,3.

g) ***Xwindows*** sessions are being displayed from abqnet1 with little or no authentication, and no encryption.

h) ***/etc/notrouter, /etc/ftpusers, /etc/default/ftpd, /usr/dt/config/Xaccess*** and other network limits are missing that would prevent certain types of attacks. See tools output in Appendixes 4-6.

i) ***Initial Install OS level*** vulnerabilities exist because the OS level was installed at level "End-User". Besides the necessary "Core System", this install adds NIS support, CDE, Xwindows and many others.

j) NIS is not being run on this system. However, NIS packages are still installed. NIS is also a rpc service. See RPC above.

3) Risks from installed third-party software

The only third party software installed on abqnet1 is the DNS/DHCP software "NetworkRegistrar" version 3.0 from Cisco.

- DNS/bind weaknesses are one of the top ten Internet security threats at this time.
- Which version of bind is this product based on?
- Is this DNS product patched up date with regard to known DNS vulnerabilities?
- Are there any security patches from Cisco for this product?
- This release is two versions behind the current Cisco release.
- This software runs as root and is not presently in a chrooted environment.

4) Administrative Practices

Administration is performed at GIAC by a small group of administrators who were very open to this audit and appear to be security minded. Nevertheless, security policies do not exist and password protection is weak.

a) ***Passwords*** vulnerable because OS and application administrators are sending passwords in clear text, around the network, in order to access and service this machine.

b) ***Passwords*** vulnerable because passwords are not set to expire or age. Password history list is not used.

c) ***Passwords*** vulnerable because passwords are not routinely tested for dictionary type attacks. During this audit, 25% of the passwords were guessed by "Crack", a publicly available tool. "Crack" was run by the system administrator at the request of this auditor.

d) ***File Integrity tools*** are not used on abqnet1 at this time. If the integrity of the box is ever lost due to security attack, it may otherwise go unnoticed. Without periodically checking the integrity of the system, a machine could remain under hostile control indefinitely if symptoms were kept at a minimum. Hackers want an inside base from which to work and to leverage to take over other machines. It is often not obvious that a machine has been taken over.

e) ***Administrative data*** vulnerable because OS and application administrators are doing configuration of this server remotely and without session encryption.

f) ***Trust relationship*** vulnerabilities exist because .rhosts files are allowed.

g) ***Clear policy*** on administrative practice is not defined or enforced and will result in the resurface of security issues.

5) Security patches

Sun's Patchdiag[7] tool reports that almost 50 security patches are missing, or out of date on abqnet1. See Appendix 1.

6) Sensitive Data Storage and Transmission

Highly sensitive data does not exist on the DNS/DHCP server. Backup tapes are handled with the same care as for sensitive servers. See also "Backup Issues" below.

7) Internet Issues

While the abqnet1 server is internal to GIAC and not directly available to the Internet, still issues of external attack exist.

a) ***No Firewall*** exists between GIAC vendors and GIAC. Many GIAC vendors have direct connectivity to GIAC and the connectivity and security of those networks is unknown.

b) ***The Top Ten*** threats to the Internet are significant to this internal machine because those vulnerabilities are the most documented and therefore may be the easiest for an internal attacker to exploit.

8) Limited Access

A significant line of defense is simply to insure that only those persons that need to login, may login. Extra user access is an opportunity for abuse.

a) ***/etc/motd, /etc/issue*** does not exist to prohibit unauthorized access.

b) User access has already been restricted to those persons that must perform administrative duties on this machine. Additionally, the non-user accounts of smtp, listen, uucp and nuucp could be removed.

c) Sudo is installed, and the root system password is known only by the UNIX administrators and management that are directly responsible for this machine.

d) Physical Security

To the credit of GIAC management and the local GIAC administrator, this server is secured in a locked enclosure from SkarkRack[8], in a room that requires badge access. Front and back enclosure doors were found locked and only those that require access hold keys. Note that many persons still have access to the room, and that while the enclosure is locked, still power can be removed by lifting nearby floor tiles. The ability to remove power is considered a denial of service attack, and perhaps more significantly could be used to force machine reboots. Machine reboots are needed to implement certain types of attack. Reboot logs are not checked periodically on abqnet1.

9) Backup Issues, Disaster Preparedness

Backups, logs and file integrity checks must be established with security in mind. In the case of a failed data drive, the most recent backup is sufficient. In the case of a security breach, how do you know which backup was made before the break in?

a) ***UFSdump*** vulnerabilities exist because backups are performed remotely which require trust relationships that are not sound. Additional vulnerabilities exist because of root's .rhosts file which is required to allow remote

UFSdump backups. Additionally, the root level .rhosts file is world readable at present.

b) ***An Incident Analysis CD-ROM*** does not exist at this time for abqnet1. In the event of a security breach, analysis must take place to determine the extent of the damage, and to collect evidence in the event of a prosecution. The analysis must take place on the compromised machine, but certainly the tools on the compromised machine can not be trusted to perform this analysis.

c) Offsite tape rotation is correctly implemented at this time. Two separate backup systems are being used with tapes being rotated offsite to Arcus Data Security[9]. Keys are held only by authorized persons.

d) ***Tape recycling*** is a point of vulnerability at this time in that all tapes are recycled after 1 month. A security breach could force the need to go back further.

e) ***Tape Devices*** are world readable at this time on both backup systems. Note that while an attempt has already been made to close permissions on these devices, still the exact device exists under another name/path that has not been secured. Observe how the major/minor device numbers indicate that the same device is available without secure permissions.

```
<441 user1:tapeserver> cd /dev/rmt
<442 user1:tapeserver> ls -lL 8cbn
crw-------   1 root     sys       33,2268 Nov 19 13:28 8cbn
<443 user1:tapeserver> ls -lL | grep 33,2268
crw-------   1 root     sys       33,2268 Nov 19 13:28 8cbn
crw-rw-rw-   1 root     sys       33,2268 Oct 29  1999 8ubn
```

f) ***Networked backups*** are presently not on a private switched network to minimize data transfer snooping.

g) ***A Disaster recovery plan*** is not documented or tested at this time.

10)Other issues

These issues are more related to reliability and safety than security alone.

a) ***Backup power*** is provided by a UPS that can maintain power for only 45 minutes. However, a secondary DNS/DHCP server is located remotely.

b) ***Automatic Water sprinklers*** are in the ceiling as fire protection. This is dangerous and should be replaced with a Halon-type suppression product.[10]

PRIORITIZED LIST OF VULNERABILITIES

This list is ordered according to the risk to abqnet1 in its present environment.

1) User and administrator passwords are being transmitted in the clear.
2) Easily guessed passwords are being used, and for extended periods.
3) Vulnerable Network services from /etc/inetd.conf and Sendmail are enabled.
4) Recommended Security Patches from Sun are not kept up to date.

5) NFS client services are making all devices vulnerable.
6) The kernel allows buffer overflow execution.
7) Some external network traffic is not blocked or filtered by a firewall.
8) The security posture of the third party DNS/DHCP software is not known.
9) Administrative access is not restricted at the network level.
10) Unwarranted trust relationships exist on the machine, between other machines and within the OS file permissions.
11) Backup tapes are readable by anyone on the backup server.
12) Operating System integrity is not periodically confirmed.
13) Logging and accounting are virtually unused.
14) Defined security and administrative policies do not exist.

Recommendations

These recommendations should be implemented quickly, but can not be considered a once-and-for-all solution. Security is a moving target, and requires constant system and network monitoring and periodic enhancements in the form of patches, software and OS upgrades, and improved security tools. GIAC must implement a security policy from the corporate level, to insure that this monitoring is implemented and automated for these servers, and that patches, and system integrity are periodically confirmed.

The most critical steps to perform immediately on this server follow. These are ordered partly by impact and largely by ease/speed of implementation.

1) Disable all network services that are not explicitly required. See Nmap[11] output in Appendix 2.
   a) Edit /etc/inetd.conf and remove all unnecessary services. Sadmind was already disabled in /etc/inetd.conf. Sadmind is one of the top ten threats to the Internet.
      - Optionally rename /etc/rc2.d/S72inetsvc and don't run inetd.
      - Optionally rename /etc/rc2.d/S71rpc and don't run rpcbind.
   b) Prevent Sendmail from starting
      - Rename /etc/rc2.d/S88sendmail
      - Add cron entry to periodically flush mail queue 0 * * * * /usr/lib/sendmail -q
2) Disable most buffer overflow execution at the kernel level.
   a) Edit /etc/system and add the following

      set noexec_user_stack = 1

      set noexec_user_stack_log = 1
   b) Reboot required to take effect.

3) Download and apply Sun's "Recommended and Security Solaris Patch Cluster" for this OS version.[12]
   a) Use wget[13] via cron to automatically download the current patchdiag.xref file monthly.

      0 0 1 * * wget –m –L –I2 –A patchdiag.xref "http://sunsolve.sun.com/autopatch"

   b) Run Patchdiag from cron monthly and e-mail results to admin team.
   c) Define policy and assign task such that missing security patches are applied monthly.
   d) Run Sun's Explorer script monthly and request your Sun Enterprise Services representative to proactively tell you when your patches are not current.
4) Disable NFS client services
   a) rename /etc/rc2.d/S73nfs.client and /etc/rc3.d/S15nfs.server
   b) delete /etc/auto_* and /etc/dfs/dfstab
5) Fix permissions on tape devices on backup server.

   cd /dev/rmt ; chmod 600 *
6) Run crack[14] from cron monthly to flush out weak passwords. Weak passwords are one of the top ten threats to the Internet.
7) Perform general internal lock-down and removal of unsound trust relationships.
   a) Run fix-modes[15], then Yassp[16] or Titan to set sane system file permissions and to enable various network restrictions, and to eliminate various unsound trust relationships. See Appendix 6 for a Titan dry run.
   b) Periodically run one or more of Sara[17], Tara[18], Cops[19], and Titan[20] to confirm that misc. lockdown steps are still in place.
   c) Edit /etc/pam.conf to disable the use of .rhosts
   d) Edit /etc/vfstab to mount /usr as read-only and /var, /local as nosuid.
   e) Enable eeprom security % eeprom security-mode=command
   f) Disable L1-A, stop-A sequence by editing /etc/default/kbd and insert KEYBOARD_ABORT=disabled
8) Install tcp_wrappers[21] to restrict and verbosely log network access to the server.
   - Take care that this does not restrict normal user requests of DNS/DHCP.
9) Remove telnet, ftp, rlogin, rsh and replace with ssh[22] and scp.
   - This will allow same functionality but with strong authentication and session encryption.

10) Install Tripwire[23] or run Signatures from Tiger or Tara or the Solaris Fingerprint Database from sunsolve.sun.com

11) Enable security logging.

    a) Add line to /etc/syslog.conf

       auth.info<tab>/var/log/authlog

    b) Create security related log files

       % touch /var/log/authlog; touch /var/adm/loginlog

       % chmod 600 /var/log/authlog /var/adm/loginlog

    c) Install/Configure NTP[24] so that logs show exact times.

12) Purchase and install a Firewall between GIAC and directly connected business partners.

13) Remove the extra packages from when OS was installed at End-User level, to reduce the number of vulnerable programs. See the *Solaris Advanced Installation Guide* for specific packages to remove.[25]

14) Contact Cisco to determine security level of DNS/DHCP software. Upgrade to current release.

15) Put Security and Administrative Policies in place and enforce them otherwise these issues will continuously resurface.

    It should be noted that when defined policies and procedures are in place, the time and expense to keep machines reasonably secure is very insignificant, especially when compared to the cost of having critical servers compromised.

Appendix 1

Output from Patchdiag

```
================================================================================
System Name: abqnet1    SunOS Vers: 5.6       Arch: sparc
Cross Reference File Date: Nov/16/00

PatchDiag Version: 1.0.4
================================================================================

UNINSTALLED SECURITY PATCHES

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev        ID         ID
------ --- --- --- --------- --------- ----------------------------------------
105395 N/A  06 522                     SunOS 5.6: /usr/lib/sendmail patch
105665 N/A  03 801                     SunOS 5.6: /usr/bin/login patch
105667 N/A  02 764                     SunOS 5.6: /usr/bin/rdist patch
106222 N/A  01 935                     OpenWindows 3.6: filemgr (ff.core) fixes
106235 N/A  06 110                     SunOS 5.6: lp patch
106257 N/A  05 289                     SunOS 5.6: /usr/lib/libpam.so.1 patch
106271 N/A  06 421                     SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
106301 N/A  01 928                     SunOS 5.6: /usr/sbin/in.ftpd patch
106415 N/A  03 564                     OpenWindows 3.6: xdm patch
106437 N/A  03 291 105669-06           CDE 1.2: Print Manager Patch
106448 N/A  01 858                     SunOS 5.6: /usr/sbin/ping patch
106468 N/A  02 233                     SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
106522 N/A  04 183                     SunOS 5.6: /usr/bin/ftp patch
106569 N/A  01 794                     SunOS 5.6: libauth.a & libauth.so.1 patch
106592 N/A  03 218                     SunOS 5.6: /usr/lib/nfs/statd patch
106625 N/A  08 144                     SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/uf
106629 N/A  20 233           105181-08 SunOS 5.6: CS6400 kernel update patch
106639 N/A  05 144                     SunOS 5.6: /kernel/strmod/rpcmod patch
106648 N/A  01 808                     OpenWindows 3.6: libce suid/sgid security fix
106649 N/A  01 808                     OpenWindows 3.6: libdesksetpatch
106650 N/A  04 333 106648-01           OpenWindows 3.6: mailtool attachment security patc
                   106649-01
106834 N/A  01 667                     SunOS 5.6: cp/ln/mv patch
106882 N/A  02  82                     SunOS 5.6: /usr/lib/nfs/nfsd patch
106894 N/A  01 684                     SunOS 5.6: /usr/bin/uux patch
107336 N/A  01 610                     OpenWindows 3.6: KCMS configure tool has a vulner
107565 N/A  02 400                     SunOS 5.6: /usr/sbin/in.tftpd patch
107618 N/A  01 375                     SunOS 5.6: Permissions problem in /vol.
107733 N/A  09  45                     SunOS 5.6: Linker patch
107758 N/A  01 542                     SunOS 5.6: Pax incorrectly change mode of symlink
107766 N/A  01 467                     SunOS 5.6: ASET cklist reports unchanged 6month ol
107774 N/A  01 529                     SunOS 5.6: inetd denial-of-service attack
107991 N/A  01 512                     SunOS 5.6: /usr/sbin/static/rcp patch
108199 N/A  01 432                     CDE 1.2: dtspcd Patch
108201 N/A  01 432                     CDE 1.2: dtaction Patch
108307 N/A  02 218                     SunOS 5.6: keyserv fixes
108333 N/A  02  94                     SunOS 5.6: jserver buffer overflow
108346 N/A  03 218                     SunOS 5.6: patch usr/sbin/rpc.nispasswdd
108468 N/A  02 177                     SunOS 5.6: ldterm streams module fixes
108492 N/A  01 347                     SunOS 5.6: Snoop may be exploited to gain root acc
108499 N/A  01 299                     SunOS 5.6: ASET sets the gid on /tmp, /var/tmp whe
108660 N/A  01 330                     SunOS 5.6: Patch for sadmind
108804 N/A  01 166                     SunOS 5.6: tip has buffer overrun with security im
108890 N/A  01 218                     SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
108893 N/A  01 218                     SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
108895 N/A  01 218                     SunOS 5.6: patch /usr/sbin/rpc.bootparamd
109266 N/A  01 193                     SunOS 5.6: security: /bin/mail has buffer overflow
109339 N/A  01 177                     SunOS 5.6: nscd has a potential security problem
109388 N/A  01 169                     SunOS 5.6: patch /usr/vmsys/bin/chkperm
================================================================================
```

Appendix 2

Output from Nmap

```
% nmap -O -sU -sT abqnet1

Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap)
Interesting ports on abqnet1 (10.0.11.1):
Port    State       Protocol  Service
7       open        udp        echo
7       open        tcp        echo
9       open        udp        discard
9       open        tcp        discard
13      open        udp        daytime
13      open        tcp        daytime
19      open        udp        chargen
19      open        tcp        chargen
21      open        tcp        ftp
23      open        tcp        telnet
25      open        tcp        smtp
37      open        udp        time
37      open        tcp        time
42      open        udp        nameserver
49      open        tcp        tacacs
53      open        udp        domain
53      open        tcp        domain
67      open        udp        bootps
79      open        tcp        finger
80      open        tcp        http
111     open        udp        sunrpc
111     open        tcp        sunrpc
161     open        udp        snmp
177     open        udp        xdmcp
512     open        udp        biff
512     open        tcp        exec
513     open        tcp        login
514     open        udp        syslog
514     open        tcp        shell
515     open        tcp        printer
517     open        udp        talk
540     open        tcp        uucp
647     open        udp        unknown
1103    open        tcp        xaudio
1645    open        udp        radius
1646    open        udp        radacct
4045    open        udp        lockd
4045    open        tcp        lockd
6000    open        tcp        X11
6112    open        tcp        dtspc
7100    open        tcp        font-service

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=34812 (Worthy challenge)
Remote operating system guess: Solaris 2.6 - 2.7
```

Appendix 3

Output from Sara 3.1.6

Host: abqnet1.giac.com

Vulnerability information:

- tooltalk version may be vulnerable to buffer overflow(RED)
- calendar manager version may be vulnerable to buffer overflow(RED)
- printer version may be vulnerable to buffer overflow(RED)
- Information from rusersd could help hacker(BROWN)
- Possible smtp relay (spam)(BROWN)
- Excessive finger information(BROWN)
- rpc.statd on SunOS is vulnerable if not patched(BROWN)
- Is your host a DoS threat?(BROWN)
- R Series: rlogin could be vulnerable(BROWN)
- Information from rstatd could help hacker(BROWN)

Appendix 4

Output from Cops

```
ATTENTION:
Security Report for Tue Nov 21 17:53:57 CST 2000
from host abqnet1, COPS v. Version 1.04+


**** root.chk ****
**** dev.chk ****
**** is_able.chk ****
Warning!  /etc/security is _World_ readable!
**** rc.chk ****
**** cron.chk ****
**** group.chk ****
**** home.chk ****
**** passwd.chk ****
Warning!  Password file, line 7, user smtp has uid = 0 and is not root
       smtp:x:0:0:Mail Daemon User:/:
**** user.chk ****
**** misc.chk ****
**** ftp.chk ****
Warning!  /etc/ftpusers should exist!
**** pass.chk ****
**** kuang ****
**** bug.chk ****
Warning!  /usr/lib/sendmail could have a hole/bug!  (CA-88:01)
Warning!  /bin/login could have a hole/bug!  (CA-89:01)
Warning!  /usr/ucb/rdist could have a hole/bug!  (CA-91:20)
Warning!  /usr/lib/sendmail could have a hole/bug!  (CA-90:01)
Warning!  /bin/mail could have a hole/bug!  (CA-91:01a)
```

Appendix 5

Output from Tara

```
Security scripts *** 2.0.9 ARC, 1999.0907.2100 ***
Tue Nov 21 18:18:13 CST 2000
18:18> Beginning security report for abqnet1 (sun4u SunOS 5.6).

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc001w] Login ID adm is disabled, but still has a valid shell.
--WARN-- [acc005w] Login ID adm is disabled, but has a 'cron' file or cron
         entries.
--WARN-- [acc001w] Login ID bin is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID daemon is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID listen is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID lp is disabled, but still has a valid shell.
--WARN-- [acc005w] Login ID lp is disabled, but has a 'cron' file or cron
         entries.
--WARN-- [acc001w] Login ID noaccess is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID nobody4 is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID sys is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID uucp is disabled, but still has a valid shell.
--WARN-- [acc006w] Login ID adm's home directory (/var/adm) has group `sys'
         write access.
--WARN-- [acc006w] Login ID bin's home directory (/usr/bin) has group `bin'
         write access.
--WARN-- [acc006w] Login ID userabc's home directory (/tmp) has group `sys'
         and world write access.
# Checking accounts from NIS.

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

# Checking accounts from /etc/passwd...
--WARN-- [rcmd006w] User root's .rhosts file has group `other' and world read
         access.

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

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

# Performing check of system file permissions...
--WARN-- [perm001w] /etc should not have group write.
--WARN-- [perm001w] /export should not have group write.
--WARN-- [perm001w] /sbin should not have group write.
--WARN-- [perm001w] /usr should not have group write.
--WARN-- [perm001w] /usr/4lib should not have group write.
--WARN-- [perm001w] /usr/openwin should not have group write.
--WARN-- [perm001w] /usr/demo should not have group write.
--WARN-- [perm001w] /usr/games should not have group write.
--WARN-- [perm001w] /usr/bin should not have group write.
--WARN-- [perm001w] /usr/lib should not have group write.
--WARN-- [perm001w] /usr/ucb should not have group write.
--WARN-- [perm001w] /var should not have group write.
--WARN-- [perm001w] /var/spool should not have group write.
--WARN-- [perm001w] /dev should not have group write.
--WARN-- [perm001w] /.rhosts should not have group read.
--WARN-- [perm001w] /.rhosts should not have world read.
--WARN-- [perm001w] /etc/mail should not have group write.
--WARN-- [perm001w] /etc/dfs should not have group write.
--WARN-- [perm001w] /etc/vfstab should not have group write.
--WARN-- [perm001w] /usr/bin/tip should not have owner write.
--ALERT-- [perm024a] /usr/sbin/arp is setgid to `bin'.
```

```
# Performing checks for SunOS/5...
--WARN-- [no-id] The PROM monitor is not in secure mode.
--WARN-- [misc008w] NFS port checking disabled in kernel.
# Running './scripts/check_sendmail'...

# Checking sendmail...

# Checking setuid executables...
--FAIL-- [fsys001f] File /etc/lp/alerts/printer is a setuid script:
-r-sr-xr-x   1 lp       lp           203 Jul  2  1997 /etc/lp/alerts/printer
--WARN-- [fsys002w] setuid program /usr/lib/libnet15d.so has relative
         pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/libstd15d.so has relative
         pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/libtls15d.so has relative
         pathnames.
--WARN-- [suidxxx] Setuid file `/usr/openwin/bin/xlock' which is group `bin'
         writable.

--WARN-- [fsys002w] setuid program /usr/sbin/pgxconfig has relative pathnames.

---s--x--x root     root     /usr/local/bin/sudo
-r-s--x--x root     sys      /usr/bin/admintool
-r-sr-xr-x root     bin      /usr/sbin/m64config
-r-sr-xr-x root     bin      /usr/sbin/pgxconfig
-rwsr-sr-x root     other    /usr/lib/libnet15d.so
-rwsr-sr-x root     other    /usr/lib/libstd15d.so
-rwsr-sr-x root     other    /usr/lib/libtls15d.so
```


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

Appendix 6

Output from Titan

```
_____________________________________________________
*=*=*=*=* Running modules/add-umask.sh now.....
Output to ../logs/modules/add-umask.sh.V.183307
-----------------------------------------------------
No umask file /etc/init.d/umask.sh found - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/adjust-arp-timers.sh now.....
Output to ../logs/modules/adjust-arp-timers.sh.V.183307
-----------------------------------------------------

Checking for ARP timers in /etc/rc2.d/S69inet

ARP timers are not set - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/aset.sh now.....
Output to ../logs/modules/aset.sh.V.183307
-----------------------------------------------------
ASET not installed - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/automount.sh now.....
Output to ../logs/modules/automount.sh.V.183307
-----------------------------------------------------
File /etc/rc2.d/S74autofs exists...
Automounter =
/usr/lib/autofs/automountd /usr/sbin/automount - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/automount2.sh now.....
Output to ../logs/modules/automount2.sh.V.183307
-----------------------------------------------------
File /etc/rc2.d/S74autofs exists...
Automounter =
/usr/lib/autofs/automountd /usr/sbin/automount - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/bsm.sh now.....
Output to ../logs/modules/bsm.sh.V.183307
-----------------------------------------------------
WARNING - BSM is not enabled
File /etc/security/audit_control exists checking contents....
auditing not configured - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/cde.sh now.....
Output to ../logs/modules/cde.sh.V.183307
-----------------------------------------------------
/usr/dt/config/Xaccess allows XDMCP login connections. - FAILS CHECK 1


_____________________________________________________
*=*=*=*=* Running modules/create-issue.sh now.....
Output to ../logs/modules/create-issue.sh.V.183307
-----------------------------------------------------
Cannot read /etc/issue - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/cronset.sh now.....
Output to ../logs/modules/cronset.sh.V.183307
```

```
-------------------------------------------------
CRONLOG entry found - PASSES CHECK
/var/cron permissions - FAILS CHECK
/etc/cron.d/logchecker LIMIT - FAILS CHECK


_________________________________________________
*=*=*=*=* Running modules/defloginparams.sh now.....
Output to ../logs/modules/defloginparams.sh.V.183307
-------------------------------------------------
login defaults CONSOLE - FAILS CHECK
login defaults UMASK - FAILS CHECK
login defaults SYSLOG - PASSES CHECK
login defaults TIMEOUT - FAILS CHECK
login defaults PASSREQ - PASSES CHECK
login defaults ALTSHELL - PASSES CHECK


_________________________________________________
*=*=*=*=* Running modules/defpwparams.sh now.....
Output to ../logs/modules/defpwparams.sh.V.183307
-------------------------------------------------
passwd MINWEEKS - FAILS CHECK
passwd MAXWEEKS - FAILS CHECK
passwd WARNWEEKS - FAILS CHECK
passwd PASSLENGTH - PASSES CHECK


_________________________________________________
*=*=*=*=* Running modules/disable-L1-A.sh now.....
Output to ../logs/modules/disable-L1-A.sh.V.183307
-------------------------------------------------
Abort sequence set to enable - FAILS CHECK


_________________________________________________
*=*=*=*=* Running modules/disable-NFS-2.6.sh now.....
Output to ../logs/modules/disable-NFS-2.6.sh.V.183307
-------------------------------------------------
Verifying TCP NFS port settings using ndd

NFS TCP port definition is set as privlidged - PASSES CHECK

Verifying UDP NFS port settings using ndd

NFS UDP port definition is set as privlidged - PASSES CHECK



_________________________________________________
*=*=*=*=* Running modules/disable-NFS.bind.sh now.....
Output to ../logs/modules/disable-NFS.bind.sh.V.183307
-------------------------------------------------
ERROR - This script is Only needed on Solaris 2.5.1 and older
Please us the disable-NFS-2.6.sh for your OS


_________________________________________________
*=*=*=*=* Running modules/disable-accounts.sh now.....
Output to ../logs/modules/disable-accounts.sh.V.183307
-------------------------------------------------
Checking 12 Users....
Checking that shell set to noshell for:

daemon bin sys adm lp smtp uucp nuucp listen nobody noaccess nobody4
Verify shell status....

daemon shell = - FAILS CHECK
bin shell = - FAILS CHECK
```

```
sys shell = - FAILS CHECK
adm shell = - FAILS CHECK
lp shell = - FAILS CHECK
smtp shell = - FAILS CHECK
uucp shell = - FAILS CHECK
nuucp shell = /usr/lib/uucp/uucico - FAILS CHECK
listen shell = - FAILS CHECK
nobody shell = - FAILS CHECK
noaccess shell = - FAILS CHECK
nobody4 shell = - FAILS CHECK

12 Users Not Secured Out Of 12


_____________________________________________________
*=*=*=*=* Running modules/disable-core.sh now.....
Output to ../logs/modules/disable-core.sh.V.183307
-----------------------------------------------------
Core dump size has not been set: FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/disable-ping-echo.sh now.....
Output to ../logs/modules/disable-ping-echo.sh.V.183307
-----------------------------------------------------
Ping echo response allowed - FAILS CHECK



_____________________________________________________
*=*=*=*=* Running modules/disable_ip_holes.sh now.....
Output to ../logs/modules/disable_ip_holes.sh.V.183307
-----------------------------------------------------
Checking kernel settings using ndd
IP source routing is currently set to 1
System allows source routed packet forwarding - FAILS CHECK
IP forwarding is currently set to 0
System does not Forward IP packets - PASSES CHECK
IP forwarding directed broadcast is currently set to 1
System allows forwarding of directed broadcasts - FAILS CHECK
IP ignore redirect is currently set to 0
System is not set to ignore redirected packets - FAILS CHECK
IP strict multihoming is currently set to 0
System is not set to do strict destination multihoming - FAILS CHECK
/etc/notrouter does not exist - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/dmi-2.6.sh now.....
Output to ../logs/modules/dmi-2.6.sh.V.183307
-----------------------------------------------------
dmi daemon is enabled - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/eeprom.sh now.....
Output to ../logs/modules/eeprom.sh.V.183307
-----------------------------------------------------
Architecture = sun4u
eeprom security-mode is currently NOT SET! - FAILS CHECK
We strongly recommend it be set to -command- by the Administration Staff


_____________________________________________________
*=*=*=*=* Running modules/file-own.sh now.....
Output to ../logs/modules/file-own.sh.V.183307
-----------------------------------------------------
Checking /usr file ownership
Found 5339 files in /usr that should be root owned
```

```
Checking /sbin file ownership
Found 13 files in /sbin that should be root owned
Checking /usr group permissions
Found 0 files in /usr that should be set group g-w
Checking /sbin group permissions
Found 0 files in /sbin that should be set group g-w
Checking /etc group permissions
Found 0 files in /etc that should be set group g-w
Checking /opt group permissions
Found 0 files in /opt that should be set group g-w


_____________________________________________________
*=*=*=*=* Running modules/fix-cronpath.sh now.....
Output to ../logs/modules/fix-cronpath.sh.V.183307
-----------------------------------------------------
File /var/spool/cron/crontabs/root exists; continuing
       /etc is not writable by world - PASSES CHECK.
       /etc is writable by group - FAILS CHECK
       /etc/cron.d is not writable by world - PASSES CHECK.
       /etc/cron.d is not writable by group - PASSES CHECK.
       /usr is not writable by world - PASSES CHECK.
       /usr is writable by group - FAILS CHECK
       /usr/sbin is not writable by world - PASSES CHECK.
       /usr/sbin is writable by group - FAILS CHECK
       /usr/lib is not writable by world - PASSES CHECK.
       /usr/lib is writable by group - FAILS CHECK
       /usr/lib/fs is not writable by world - PASSES CHECK.
       /usr/lib/fs is writable by group - FAILS CHECK
       /usr/lib/fs/nfs is not writable by world - PASSES CHECK.
       /usr/lib/fs/nfs is not writable by group - PASSES CHECK.
       /usr/bin is not writable by world - PASSES CHECK.
       /usr/bin is writable by group - FAILS CHECK

    /etc/cron.d/logchecker ownership should be changed to root
    /usr/lib/newsyslog ownership should be changed to root
    /usr/bin/rdate ownership should be changed to root

         No cron.allow file - FAILS CHECK

        No at.allow file - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/fix-stack.sol2.6.sh now.....
Output to ../logs/modules/fix-stack.sol2.6.sh.V.183307
-----------------------------------------------------
Stack Protection not currently set - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/ftp-2.6_secure.sh now.....
Output to ../logs/modules/ftp-2.6_secure.sh.V.183307
-----------------------------------------------------
/etc/default/ftpd does not exist - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/ftpusers.sh now.....
Output to ../logs/modules/ftpusers.sh.V.183307
-----------------------------------------------------
No /etc/ftpusers file in place - FAILS CHECK
Should contain at least:

root
daemon
sys
```

```
bin
adm
lp
smtp
uucp
nuucp
listen
nobody
noaccess
news
ingres
audit
admin
sync
nobody4

_____________________________________________________
*=*=*=*=* Running modules/inetd.sh now.....
Output to ../logs/modules/inetd.sh.V.183307
-----------------------------------------------------
File /etc/inet/inetd.conf exists - Checking...
name Open - FAILS CHECK
exec Open - FAILS CHECK
comsat Open - FAILS CHECK
talk Open - FAILS CHECK
uucp Open - FAILS CHECK
finger Open - FAILS CHECK
rquotad Open - FAILS CHECK
rusersd Open - FAILS CHECK
sprayd Open - FAILS CHECK
walld Open - FAILS CHECK
shell Open - FAILS CHECK
login Open - FAILS CHECK
exec Open - FAILS CHECK
comsat Open - FAILS CHECK
time Open - FAILS CHECK
echo Open - FAILS CHECK
discard Open - FAILS CHECK
daytime Open - FAILS CHECK
chargen Open - FAILS CHECK
rstatd Open - FAILS CHECK
100068 Open - FAILS CHECK
100083 Open - FAILS CHECK
100221 Open - FAILS CHECK
fs Open - FAILS CHECK
100235 Open - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/inetd2.sh now.....
Output to ../logs/modules/inetd2.sh.V.183307
-----------------------------------------------------
File /etc/inet/inetd.conf has services running that should be disabled - FAILS
CHECK

_____________________________________________________
*=*=*=*=* Running modules/inetsvc.sh now.....
Output to ../logs/modules/inetsvc.sh.V.183307
-----------------------------------------------------
File /etc/init.d/inetsvc has services running that should be disabled - FAILS
CHECK

_____________________________________________________
*=*=*=*=* Running modules/keyserv.sh now.....
```

```
Output to ../logs/modules/keyserv.sh.V.183307
--------------------------------------------------
File /etc/rc2.d/S71rpc keyserv ; user nobody enabled - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/log-tcp.sh now.....
Output to ../logs/modules/log-tcp.sh.V.183307
--------------------------------------------------
/etc/rc2.d/S72inetsvc - has the system default . - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/loginlog.sh now.....
Output to ../logs/modules/loginlog.sh.V.183307
--------------------------------------------------
/var/adm/loginlog missing - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/lpsched.sh now.....
Output to ../logs/modules/lpsched.sh.V.183307
--------------------------------------------------
In /etc/rc2.d/S80lp lpsched is enabled - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/nddconfig.sh now.....
Output to ../logs/modules/nddconfig.sh.V.183307
--------------------------------------------------
/etc/init.d/nddconfig does not exists - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/nfs-portmon.sh now.....
Output to ../logs/modules/nfs-portmon.sh.V.183307
--------------------------------------------------
NFS port monitor disabled - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/nsswitch.sh now.....
Output to ../logs/modules/nsswitch.sh.V.183307
--------------------------------------------------
netgroup -> nis - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/nuke-nscd.sh now.....
Output to ../logs/modules/nuke-nscd.sh.V.183307
--------------------------------------------------
Name Service Directory Cache is enabled in /etc/rc2.d/S76nscd - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/nuke-sendmail.sh now.....
Output to ../logs/modules/nuke-sendmail.sh.V.183307
--------------------------------------------------
Sendmail is enabled in /etc/rc2.d/S88sendmail - FAILS CHECK

_____________________________________________________
*=*=*=*=* Running modules/pam-rhosts-2.6.sh now.....
Output to ../logs/modules/pam-rhosts-2.6.sh.V.183307
--------------------------------------------------
PAM allows rhosts for rlogin : FAILS CHECK
PAM allows rhosts for rsh : FAILS CHECK

_____________________________________________________
_____________________________________________________
*=*=*=*=* Running modules/psfix.sh now.....
Output to ../logs/modules/psfix.sh.V.183307
```

```
-------------------------------------------------
Could not find /etc/rc3.d/S??tmpfix - FAILS CHECK


_________________________________________________
*=*=*=*=* Running modules/rhosts.sh now.....
Output to ../logs/modules/rhosts.sh.V.183307
-------------------------------------------------
Running against /etc/passwd...
Found //.rhosts... - FAILS CHECK
---------------------------------------
---------------------------------------
---------------------------------------
---------------------------------------
Running against passwd.byname...


_________________________________________________
*=*=*=*=* Running modules/rmmount.sh now.....
Output to ../logs/modules/rmmount.sh.V.183307
-------------------------------------------------
Rmount allows mounting of CD filesystems with suid binaries enabled - FAILS
CHECK
Rmount allows mounting of Floppy filesystems with suid binaries enabled - FAILS
CHECK


_________________________________________________
*=*=*=*=* Running modules/rootchk.sh now.....
Output to ../logs/modules/rootchk.sh.V.183307
-------------------------------------------------
/etc/skel/local.cshrc - Contains . - FAILS CHECK
        /etc/skel/local.login - Clean of . - PASSES CHECK
       /etc/skel/local.profile - Contains . - FAILS CHECK

Checking all directories in roots path
    /bin is owned by root. PASSES CHECK.
     /bin is writable by group. FAILS CHECK.
    /usr/bin is writable by group. FAILS CHECK.
    /sbin is writable by group. FAILS CHECK.
    /tmp/Titan,v3.5/arch/sol2sun4/bin/lib is owned by root. PASSES CHECK.


_________________________________________________
*=*=*=*=* Running modules/routed.sh now.....
Output to ../logs/modules/routed.sh.V.183307
-------------------------------------------------

The route daemon advertises routes - FAILS CHECK


_________________________________________________
*=*=*=*=* Running modules/sendmail-forward.sh now.....
Output to ../logs/modules/sendmail-forward.sh.V.183307
-------------------------------------------------
forwarding NOT restricted to /usr/local/forward - FAILS CHECK
/usr/local/forward missing - FAILS CHECK


_________________________________________________
*=*=*=*=* Running modules/sendmail.sh now.....
Output to ../logs/modules/sendmail.sh.V.183307
-------------------------------------------------
No sendmail.cf.titan2 exists - FAILS CHECK
Checking for smrsh
smrsh not found in /sbin - FAILS CHECK


_________________________________________________
*=*=*=*=* Running modules/smtp-banner.sh now.....
```

```
Output to ../logs/modules/smtp-banner.sh.V.183307
--------------------------------------------------
No /etc/mail/sendmail.cf.titan1 exists - FAILS CHECK


_____________________________________________________
_____________________________________________________
*=*=*=*=* Running modules/snmpdx-2.6.sh now.....
Output to ../logs/modules/snmpdx-2.6.sh.V.183307
--------------------------------------------------
Snmpdx daemon is enabled: FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/syslog.sh now.....
Output to ../logs/modules/syslog.sh.V.183307
--------------------------------------------------
File /etc/syslog.conf exists checking contents....
Syslog auth notice messages disabled - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/tcp-sequence.sh now.....
Output to ../logs/modules/tcp-sequence.sh.V.183307
--------------------------------------------------
/etc/default/inetinit - has the system default . - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/telnet-banner.sh now.....
Output to ../logs/modules/telnet-banner.sh.V.183307
--------------------------------------------------
telnet banner not disabled - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/useraddset.sh now.....
Output to ../logs/modules/useraddset.sh.V.183307
--------------------------------------------------
default user group for useradd - FAILS CHECK
useradd defaults - FAILS CHECK


_____________________________________________________
*=*=*=*=* Running modules/userumask.sh now.....
Output to ../logs/modules/userumask.sh.V.183307
--------------------------------------------------
 Checking for umask 022 in
 /etc/.login
 /etc/default/login
 /etc/profile
 /etc/skel/local.cshrc
 /etc/skel/local.login
 /etc/skel/local.profile

       Umask value other than 022 in /etc/.login - FAILS CHECK
       Umask value other than 022 in /etc/.login - FAILS CHECK
       Umask value other than 022 in /etc/skel/local.login - FAILS CHECK
       Umask value other than 022 in /etc/skel/local.profile - FAILS CHECK

       UMASK value other than 022 in /etc/default/login - FAILS CHECK
_____________________________________________________
*=*=*=*=* Running modules/vold.sh now.....
Output to ../logs/modules/vold.sh.V.183307
--------------------------------------------------

File /etc/rc2.d/S92volmgt and /usr/sbin/vold exists - FAILS CHECK
```

Appendix 7

Output from % find / -user root \(-perm -4000 -o -perm -2000 \) -ls

```
 62484   13 -r-sr-xr-x   1 root     bin         13260 Jul 15  1997 /usr/lib/fs/ufs/quota
 62489  168 -r-sr-sr-x   1 root     tty        156212 Jan 15  1998 /usr/lib/fs/ufs/ufsdump
 62490  712 -r-sr-xr-x   1 root     bin        717540 Jan 15  1998 /usr/lib/fs/ufs/ufsrestore
  3988   22 -r-sr-xr-x   1 root     bin         22392 Jul 15  1997 /usr/lib/exrecover
  4046    4 ---s--x--x   1 root     bin          3996 Jul 15  1997 /usr/lib/pt_chmod
  4047  240 -r-sr-x--x   1 root     bin        233288 Jul 15  1997 /usr/lib/sendmail
  4053    8 -r-sr-xr-x   1 root     bin          8088 Jul 15  1997 /usr/lib/utmp_update
144530   19 -r-s--x--x   1 root     bin         18660 Jul 15  1997 /usr/lib/lp/bin/netpr
  4183  528 -rwsr-sr-x   1 root     other      528340 Mar 23  2000 /usr/lib/libnet15d.so
  4184  424 -rwsr-sr-x   1 root     other      420832 Mar 23  2000 /usr/lib/libstd15d.so
  4185 1808 -rwsr-sr-x   1 root     other     1839908 Mar 23  2000 /usr/lib/libtls15d.so
144532   62 -rwxr-sr-x   1 root     sys         62480 Apr 12  2000 /usr/platform/sun4u/sbin/prtdiag
 35159  896 -rwxr-sr-x   1 root     root       903512 Jul  7  1997 /usr/openwin/bin/Xsun
 35181   65 -rwsrwxr-x   1 root     bin         65908 Jul  8  1997 /usr/openwin/bin/xlock
 35265   14 -r-sr-sr-x   1 root     bin         14128 Jun 26  1997 /usr/openwin/bin/ff.core
 35275  640 -r-xr-sr-x   1 root     mail       643244 Jul  2  1997 /usr/openwin/bin/mailtool
 43012   23 -rwsr-xr-x   1 root     bin         22952 Jul  7  1997 /usr/openwin/lib/mkcookie
242066   34 -rwsr-xr-x   1 root     sys         34200 Dec  9  1999 /usr/bin/at
242069   13 -rwsr-xr-x   1 root     sys         13048 Dec  9  1999 /usr/bin/atq
242070   12 -rwsr-xr-x   1 root     sys         11840 Dec  9  1999 /usr/bin/atrm
242071   16 -r-sr-xr-x   1 root     bin         16016 Dec  9  1999 /usr/bin/crontab
242112   13 -r-sr-xr-x   1 root     bin         13144 Jul 15  1997 /usr/bin/eject
242117   28 -r-sr-xr-x   1 root     bin         28148 Jul 15  1997 /usr/bin/fdformat
242162   29 -r-sr-xr-x   1 root     bin         29192 Jul 15  1997 /usr/bin/login
242178   11 -rwsr-xr-x   1 root     sys         10616 Jul 15  1997 /usr/bin/newgrp
242185   95 -r-sr-sr-x   3 root     sys         96796 Jul 15  1997 /usr/bin/passwd
242197   26 -r-sr-xr-x   1 root     sys         26372 Jul 15  1997 /usr/bin/ps
242201   20 -r-sr-xr-x   1 root     bin         20292 Jul 15  1997 /usr/bin/rcp
242203   53 -r-sr-xr-x   1 root     bin         53308 Jul 15  1997 /usr/bin/rdist
242205   16 -r-sr-xr-x   1 root     bin         15808 Jul 15  1997 /usr/bin/rlogin
242209    9 -r-sr-xr-x   1 root     bin          8772 Jul 15  1997 /usr/bin/rsh
242222   18 -r-sr-xr-x   1 root     sys         18360 Jan 15  1998 /usr/bin/su
242238   12 -r-sr-xr-x   2 root     bin         11848 Jul 15  1997 /usr/bin/uptime
242238   12 -r-sr-xr-x   2 root     bin         11848 Jul 15  1997 /usr/bin/w
242185   95 -r-sr-sr-x   3 root     sys         96796 Jul 15  1997 /usr/bin/yppasswd
242094  344 -r-s--x--x   1 root     sys        343556 Dec  9  1999 /usr/bin/admintool
242370   22 -r-sr-xr-x   1 root     sys         22020 Jan 15  1998 /usr/bin/chkey
242185   95 -r-sr-sr-x   3 root     sys         96796 Jul 15  1997 /usr/bin/nispasswd
242394   10 -r-s--x--x   1 root     lp           9268 Jul 15  1997 /usr/bin/cancel
242395   21 -r-s--x--x   1 root     lp          20956 Jul 15  1997 /usr/bin/lp
242397    7 -r-s--x--x   1 root     lp           6264 Jul 15  1997 /usr/bin/lpset
242398   20 -r-s--x--x   1 root     lp          19532 Jul 15  1997 /usr/bin/lpstat
242399    6 -r-sr-xr-x   1 root     bin          5840 Jul 15  1997 /usr/bin/volcheck
242400   11 -r-sr-xr-x   1 root     bin         10608 Jan 15  1998 /usr/bin/volrmmount
195435   17 -rwsr-xr-x   3 root     bin         16904 Dec  9  1999 /usr/sbin/allocate
195236    8 -r-xr-sr-x   1 root     bin          7940 Jul 15  1997 /usr/sbin/arp
195302   10 -rwsr-xr-x   1 root     bin          9256 Jul 15  1997 /usr/sbin/mkdevalloc
195303   10 -rwsr-xr-x   1 root     bin          9512 Jul 15  1997 /usr/sbin/mkdevmaps
195321   19 -r-sr-xr-x   1 root     bin         19424 Jul 15  1997 /usr/sbin/ping
195329   19 -r-xr-sr-x   1 root     sys         18508 Jul 15  1997 /usr/sbin/prtconf
195344   22 -rwsr-xr-x   1 root     sys         22084 Jul 15  1997 /usr/sbin/sacadm
195360   24 -r-xr-sr-x   1 root     sys         23992 Jul 15  1997 /usr/sbin/sysdef
195375   12 -r-sr-xr-x   1 root     bin         12140 Jul 15  1997 /usr/sbin/whodo
195435   17 -rwsr-xr-x   3 root     bin         16904 Dec  9  1999 /usr/sbin/deallocate
195435   17 -rwsr-xr-x   3 root     bin         16904 Dec  9  1999 /usr/sbin/list_devices
195441   28 -r-sr-xr-x   1 root     bin         27724 Jan  6  1999 /usr/sbin/m64config
195424    7 -r-s--x--x   1 root     lp           6416 Jul 15  1997 /usr/sbin/lpmove
195440  392 -r-sr-xr-x   1 root     bin        393216 Mar 18  1999 /usr/sbin/pgxconfig
  7852   22 -r-sr-sr-x   1 root     sys         22420 Jun 26  1997 /usr/dt/bin/dtaction
  7870   33 -r-sr-xr-x   1 root     bin         33120 Feb 20  1998 /usr/dt/bin/dtappgather
  7886  304 -r-sr-sr-x   1 root     daemon     297572 Dec  9  1999 /usr/dt/bin/sdtcm_convert
  7902  336 -r-sr-xr-x   1 root     bin        334168 Jun 26  1997 /usr/dt/bin/dtprintinfo
  7923  144 -r-sr-xr-x   1 root     bin        138012 Feb 20  1998 /usr/dt/bin/dtsession
 78187   22 -rwsr-xr-x   1 root     sys         21536 Jul 15  1997 /usr/ucb/ps
269427   56 ---s--x--x   1 root     root        56692 Apr 17  2000 /usr/local/bin/sudo
```

REFERENCES

Book List

Solaris Advanced Installation Guide Solaris 2.6

Sun Microsystems, August 1997.

Nemeth et al, Unix System Administration Handbook,

Prentice Hall, ISBN 0-13-151051-7

Pomeranz, Hal, Ed. Solaris Security, Step by Step, Version1.0

The SANS Institute, 2000.

Pomeranz, Hal, Ed. Common Issues and Vulnerabilities in UNIX Security

The SANS Institute, 2000.

Bishop,Matt, Ed. UNIX Security Tools and Their Uses

The SANS Institute, 2000.

Pomeranz, Hal, Ed. Solaris Practicum

The SANS Institute, 2000.

Pomeranz, Hal, Ed. Network Time Protocol

The SANS Institute, 2000.

Acheson, Steve, Ed. Secure Shell (SSH)

The SANS Institute, 2000.

Green, John, Ed. UNIX Forensics

The SANS Institute, 2000.

[1] Dan Rose is a Certified Sun Solaris Administrator with 10+ years of UNIX experience.
[2] http://www.sun.com
[3] http://www.sun.com/desktop/products/Ultra10
[4] http://www.sun.com/software/solaris/2.6
[5] http://www.cisco.com/warp/public/44/jump/network_management.shtml
[6] Sans Network Security 2000: See www.eff.org and search on "DEScracker"
[7] http://sunsolve.sun.com (must login to see "Diagnostic Tools")
[8] http://www.sharkrack.com
[9] http://w3.arcusds.com
[10] http://www.reliablefire.com/inergenfolder/inergen.html
[11] http://www.insecure.org/nmap
[12] ftp://sunsolve.sun.com/pub.patches/2.6_Recommended.tar.Z
[13] http://www.sunfreeware.com
[14] ftp://coast.cs.purdue.edu/pub/tools/unix
[15] ftp://ftp.fwi.uva.nl/pub/solaris/fix-modes.tar.gz
[16] http://yassp.parc.xerox.com/pkg/yassp.tar.Z
[17] http://www-arc.com/sara/
[18] http://www-arc.com/tara/index.html

[19] ftp://coast.cs.purdue.edu/pub/tools/unix/scanners/cops
[20] http://www.fish.com/titan
[21] ftp://ftp.cert.org/pub/tools/tcp_wrappers/
[22] http://www.cs.hut.fi/ssh http://www.ssh.fi/sshprotocols2/download.html
[23] ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire
[24] ftp://ftp.udel.edu/pub/ntp/ntp3/xntp3-X.X.tar.gz
[25] Solaris Advanced Installation Guide, Solaris 2.6. p142-160

Last Updated: July 23rd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**