Global Information Assurance Certification Paper

GIAC SECURING UNIX PRACTICAL ASSIGNMENT Version 1.4

SANS2000 Conference Track 6 - UNIX

Tyrone C. Lomeli

Consultant's report from auditing a standard client UNIX Build

A. Executive Summary

This company being audited has the advantage of being able to focus their security efforts on only one flavor of UNIX (Sun Solaris) and; therefore, are able to spend more time in effectively locking down their systems. Since this company deals with hosting their clients Internet applications, they are very serious about security at the system and network levels.

When this company approached us to perform an audit on their UNIX systems, they were fairly confident that we would not find any major faults in their systems configurations, but wanted an outside opinion to verify this assumption as well. We were impressed with much of what they had already done to secure their systems, however, we did find some additional areas that needed to be changed or simply could be changed to have better housekeeping practices.

In summary, the Solaris installs that they were performing automatically by Jumpstart still had the following major issues that needed to be immediately dealt with:

1. left some services via rcx.d startup scripts up and running that they were not using,
2. some machines had telnet and ftp running even though they had already implemented ssh as a replacement,
3. Left sendmail client running as a daemon,
4. Did not limit shell access to unused accounts,
5. Did not enable stack protection and logging,
6. Failed to force NFS clients to use privileged ports
7. Did not clean-up cron jobs and permissions,
8. Had some improper file and directory permissions,
9. Did not enable eeprom password security,
10. Left some compilers on systems,
11. Had enabled core dumps on systems,
12. Was running BIND as root in a non-chrooted environment, and
13. Was not using smrsh to help protect Sendmail.

The main body of the document gives more details behind these issues, provides defined clarifications of why they are issues, and what tasks could be done to change these issues.

B. Detailed written analysis of the computer system(s) and your findings.

1. Operating system vulnerabilities

The Sun Solaris operating system (OS) is no different from any other OS in that it needs to be patched to fix programming bugs and security holes that are continuously being discovered. This company has been very diligent in updating the recommended and security patch clusters as soon as new ones come out to help minimize potential OS vulnerabilities that may be present at any given time. The OS version audited was version 2.8, however; the client also has servers running versions 2.6 and 2.7.

The administrators at this firm regularly check the Sun Patch Reports, and available recommended cluster and security patch clusters at sunsolve.sun.com. They rollout the new patches to all systems in the enterprise via rsync over ssh with automated scripts that are run out of cron to install the patches and reboot the server.

As with all forms of Unix, the potential for compromise of dynamically loadable modules and shared libraries to gain unauthorized access privileges is common, along with buffer overflow attacks, numeric overflow attacks, and exploiting race conditions. Unfortunately with the newer versions of Solaris it is very hard to impossible to get away from using dynamically loaded modules.

The most recently discovered exploits, security alerts, and package updates for Solaris can often found at securityfocus.com even before Sun publishes them. The client has been informed to subscribe to their BUGTRAQ email group.

2. Configuration vulnerabilities

The company being audited has the advantage of being able to focus their security efforts on only one flavor of UNIX (Sun Solaris) and; therefore, are able to spend more time in effectively locking down their systems. Since this company deals with hosting their clients Internet applications, they are very serious about security at the system and network levels. As such, they spent a fair amount of time researching various security related configuration changes that could be made to their systems to make them more secure. Here is a list of configuration changes they had implemented before the audit:

- Configure Time Sync (ntp.conf file)
- Configure DNS (/etc/resolv.conf, /etc/nsswitch.conf)
- SET ROUTES (Create: /etc/defaultrouter file)
- CREATE STATIC ROUTES (no dynamic routing protocols)
- FORCE 100 mbit on QFE CARDS and HME

/etc/rc3.d/S902setint

```
#!/bin/sh

ndd -set /dev/hme instance 0
ndd -set /dev/hme adv_autoneg_cap 0
ndd -set /dev/hme adv_100T4_cap 0
ndd -set /dev/hme adv_100fdx_cap 1
ndd -set /dev/hme adv_100hdx_cap 0
ndd -set /dev/hme adv_10fdx_cap 0
ndd -set /dev/hme adv_10hdx_cap 0

…….
```

chmod 755 this file

- CREATE TELNET BANNER FOR AUDIT COMPLIANCE

/etc/default create: telnetd file

In the file put this line:

BANNER= \\r\\n\\r\\nAuthorized Access Only! All other access is forbidden!!\\r\\n\\r\\n

- Comment out everything in: /etc/inetd.conf except for telnet and ftp
- Disable some /etc/rc startup files

Move the following files to small s and do the same with K scripts in rc0.d

/etc/rc2.d

S99dtlogin
S73nfs.client
S71rpc
S74autofs
S30sysid.net
S71sysid.sys
S72autoinstall
S76nscd

/etc/rc3.d

S15nfs.server (not on all boxes)
S73nfs.client (not on all boxes)
S77dmi

- Add to the bottom of /etc/init.d/inetinit:

```
ndd –set /dev/tcp tcp_conn_req_max_q0 10240
ndd –set /dev/ip ip_ignore_redirect 1
ndd –set /dev/ip ip_send_redirects 0
ndd –set /dev/ip ip_ire_flush_interval 60000
ndd –set /dev/arp arp_cleanup_interval 60
ndd –set /dev/ip ip_forward_directed_broadcasts 0
ndd –set /dev/ip ip_forward_src_routed 0
ndd –set /dev/ip ip_forwarding 0
ndd –set /dev/ip ip_strict_dst_multihoming 1
```

- Add to /etc/syslog.conf

auth.info /var/log/authlog

create /var/log/authlog, change owner to root and chmod 600

create /var/adm/loginlog to capture failed logins (chmod 600, chgrp sys, chown root)

- Create: /etc/ftpusers file with the users listed in /etc/passwd
- Install: CVS, Sudo, and Rsync, tripwire, ssh, and tcp Wrappers.
- Add: /usr/local/bin and /usr/local/sbin to the appropriate default PATH, depending on the user.
- Add: /usr/local/man to the MANPATH for all users.
- /etc/ftpusers – disallows all standard users from logging in such as root, daemon, sys,

bin, adm, lp, smtp, uucp, nuucp, listen, nobody, noaccess, and nobody4.

- /etc/issue
- /etc/motd

These files are based on US Government recommendations. They provide legal notice to users that their activities may be monitored.

- /etc/notrouter

This file disables IP forwarding between interfaces on the system by creating an /etc/notrouter file.

- /etc/nsswitch.conf

This is an nsswitch.conf file configured so that a system will use DNS for name

Resolution (after hosts file). It is a copy of the /etc/nsswitch.dns shipped with Solaris 8 OE.

- /etc/default/telnetd

This file enables the feature available in Solaris 7 and 8 OEs to change the default TELNET banner. The banner is changed by adding the BANNER entry to the /etc/default/telnetd file.

- /etc/rc3.d/S902setint

This file is a startup script required to initialize all interfaces to the states shown in this doc.

- /etc/default/login

Uncomment CONSOLE=/dev/console to disallow login by root remotely.

- /etc/rc3.d/S80spc

These scripts disable all SunSoft™ Print Client (SPC) startup and shutdown scripts.

A standard ps listing for a standard Solaris 2.8 build with no apps on it yet is shown next.

```
  UID   PID  PPID  C    STIME TTY      TIME CMD
   root     0     0  0   Oct 23 ?       0:07 sched
   root     1     0  0   Oct 23 ?       0:07 /etc/init -
   root     2     0  0   Oct 23 ?       0:00 pageout
   root     3     0  1   Oct 23 ?      40:24 fsflush
   root   266     1  0   Oct 23 ?       0:00 /usr/lib/saf/sac -t 300
   root   269   266  0   Oct 23 ?       0:00 /usr/lib/saf/ttymon
   root   118     1  0   Oct 23 ?       0:00 /usr/sbin/rpcbind
   root    49     1  0   Oct 23 ?       0:00 /usr/lib/devfsadm/devfseventd
   root    51     1  0   Oct 23 ?       0:00 /usr/lib/devfsadm/devfsadmd
   root   297   267  0   Oct 23 console  0:00 ksh -o vi
   root   148   147  0   Oct 23 ?       0:00 /usr/sbin/ntpdate -s -w 10.1.150.11 10.1.150.12
   root   147     1  0   Oct 23 ?       0:00 /sbin/sh /etc/rc2.d/S74xntpd start
   root   141     1  0   Oct 23 ?       0:00 /usr/sbin/inetd -s
   root   150     1  0   Oct 23 ?       0:00 /usr/sbin/syslogd
   root   270   217  0   Oct 23 ?       1:22 mibiisa -r -p 32776
   root   167     1  0   Oct 23 ?       0:00 /usr/local/sbin/sshd
   root   157     1  0   Oct 23 ?       0:00 /usr/sbin/cron
   root   184     1  0   Oct 23 ?       0:00 /usr/lib/power/powerd
   root   193     1  0   Oct 23 ?       0:00 /usr/lib/utmpd
   root   204     1  0   Oct 23 ?       0:00 /usr/sbin/vold
   root   267     1  0   Oct 23 console  0:00 -sh
   root   217     1  0   Oct 23 ?       0:00 /usr/lib/snmp/snmpdx -y -c /etc/snmp/conf
   root   303   141  0   Oct 23 ?       0:00 in.telnetd
```

```
    tyl   306   303  0   Oct 23 pts/1    0:00 -ksh
   root   363   306  0   Oct 23 pts/1    0:00 sh
   root   491     1  0   Oct 26 ?        0:18
/usr/java/bin/../jre/bin/../bin/sparc/native_threads/java -Dpropdir=/usr/sadm/l
   root 17949   363  0 18:35:29 pts/1    0:00 ps -efa
    tyl 17945   141  0 18:33:34 ?        0:00 in.ftpd
```

3. Risks from installed third-party software

The client was running the latest version of BIND on Solaris, however, they were running the service as root and in a non-chrooted environment. We recommended to them that they should run BIND as a non-privileged user on the system and in a chrooted environment.

They client's Sendmail machines were not utilizing smrsh to simulates a chrooted environment for the Sendmail daemon. Since Sendmail must run as root to deliver mail to users mail folders, it is a well know security risk, since there have been so many buffer overflow and other exploits against Sendmail. Smrsh was recommended to the client to minimize this risk..

Apache, iplanet and Oracle apps are all being run as a non-privileged user and have been promptly maintained by most recent patches.

4. Administrative practices

The client utilizes Run Books for every server in the data center, which every change must be logged to. They are utilizing cvs for version control on all of the systems.

All logging is done locally and to syslog servers on the network.. Logs are kept on syslog server for one year and backed-up every night as is every system in the data center. Regular test restores are performed.

Passwords use shadow files, but no password aging is currently in effect. Engineers are required by company policy to change passwords on a bi-monthly basis.

5. Security patches up to date

The Solaris 2.8 server that we audited had the most recent patches applied. A patchadd –p for the specified system is shown below:

Patch: 109137-01 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu

Patch: 108975-03 Obsoletes: Requires: 108968-01, 108974-01, 108977-01 Incompatibles: Packages: SUNWcsu, SUNWvolu
Patch: 108528-02 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsr, SUNWcarx, SUNWcar, SUNWcsxu, SUNWhea, SUNWmdb, SUNWmdbx, SUNWsrh, SUNWtnfc, SUNWtnfcx
Patch: 108875-07 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu, SUNWcsr, SUNWcslx, SUNWcsl, SUNWcarx, SUNWarc, SUNWcstl, SUNWcstlx, SUNWhea
Patch: 109783-01 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu
Patch: 108985-02 Obsoletes: Requires: Incompatibles: Packages: SUNWcsu
Patch: 108974-03 Obsoletes: Requires: Incompatibles: Packages: SUNWcsr, SUNWcarx
Patch: 108977-01 Obsoletes: Requires: 108974-01 Incompatibles: Packages: SUNWcsr, SUNWhea, SUNWvolu, SUNWvolux
Patch: 108968-02 Obsoletes: Requires: 108974-01, 108977-01 Incompatibles: Packages: SUNWcsr, SUNWesu, SUNWhea, SUNWvolu, SUNWvolux
Patch: 108652-16 Obsoletes: Requires: Incompatibles: Packages: SUNWxwfnt, SUNWxwplt, SUNWxwplx, SUNWxwinc, SUNWxwman, SUNWxwpmn, SUNWxwslb
Patch: 109320-01 Obsoletes: Requires: Incompatibles: Packages: SUNWpcu, SUNWpsu

6. Sensitive data is stored encrypted and how

Passwords on the client's systems are encrypted with the UNIX standard crypt() in /etc/shadow and other locations for apache authentication. Ssh is used on all systems with MD5 encrypted public key – private key authentication only.

As stated before, the client still has telnet and ftp opened up on all servers and has been informed that ssh can and should be used to perform all of the same tasks as ftp and telnet so that unencrypted passwords are not sent over the network any longer.

7. Data is sent over the Internet encrypted

SSL encryption is enabled on all of the web servers that the client has in production at this time. SQLNET and other database querying is done solely via point-to-point connections to the client's sites.

As previously stated above, telnet and ftp unencrypted passwords sent over the internet is a very large security risk and should be discontinued immediately.

8. Anti-virus software is updated (if used as a server for Windows systems)

There is virtually no interaction between Windows and Solaris servers in the data center of the client.

9. Access is restricted to those with a need to know

All racks are physically locked when not in immediate use by engineers. Only senior UNIX administrators and above have login accounts and passwords to the servers.

The systems are located in a class 2 data center that is surrounded by reinforced block walls and bullet-proof glass. There are no external peripherals (keyboard, monitor, printer, hard drives, etc) attached to the systems. While the reset and power buttons are still active on the CPU case and the power cords would be physically accessible if the racks were left open, they are always kept locked.

The data center allows access only to those who have had their thumb print and security code programmed into the security database system. Access to the vault is both manually and electronically logged. A security guard guards the main entrance to the building and key card access is needed as well. An alarm system is installed in the data center along with fire suppression.

10. Backup policies, disaster preparedness, etc.

The client is currently using Veritas Netbackup version 3.4 GA. A Compaq 1850 server with a StorageTek tape library backs up all of the NT clients. A SUN Enterprise 3500 using an ADIC tape library backups all the UNIX clients.

Backup Schedules/Classes

- Full backups are scheduled to run Monday and Tuesday from 4:00 PM to 8:00 AM for all production servers that are not DB servers.
- Full backups are scheduled to run Monday thru Saturday 12:00 AM to 6:00 AM for all production servers that are DB servers. The client has a SQL backup module loaded which allows the database to be backed up online.
- Differential backups are scheduled to run Sunday and Wednesday thru Saturday from 7:00 PM to 7:00 AM which backup files that have only changed since the last full backup.

Retention Policies

- The full backup schedule has a retention period of one year and a frequency of five days. Therefore, tapes cannot be overwritten for one year, and once a successful full backup is completed, a new one will not be tried for at least five days. Full backups are taken offsite every Wednesday.
- The differential backup schedule has a retention period of two weeks and a frequency of one day. Therefore, tapes can only be overwritten after two weeks, and once a successful backup is completed, a new one will not be tried for one day. Differential backups are kept on site for a period of 30 days, then are erased and recycled to be used again

Rebuild Procedure (Disaster Recovery)

Random "fire drills" where certain files or complete servers are restored to a test server are scheduled weekly to ensure that every site can be restored from tape at any time.

- Hardware fails (not drives):
  - Sun will fix hardware through client's Platinum support contract. (2 hour max response time)
  - Reboot server and continue.

- Hard drive fails (including root – v.3.0.4 with mirroring): No problem with VxVM installed or SDS and continues to run off mirrored disk.

  - Run vxdiskadm and select #4 remove disk for replacement.
  - Replace the drive and run vxdiskadm
  - Select #5, replace failed or removed disk.
  - System stays up and running.
  - Hard drive fails with SDS
  - Remove metadbs on disk.
  - Detach from the mirror.
  - Replace the disk and reattach the disk to the mirror.
  - System needs to be rebooted to perform operations at a scheduled maintenance time.).

- If major disaster occurs to a machine or the data/OS requires a complete rebuild:

  - Run a network cable to the switch that is attached to the Jumpstart server.
  - Power system on and get the MAC address of system.
  - Run config script on the Jumpstart server for the server you are building.
  - Enter: boot net - install at the boot PROM prompt and wait for ~ 30 minutes to 1 hour depending on what you have told the Jumpstart server to load.

- OS, most config files, SDS or VxVM are loaded and mirror the root disk and install other patches and packages you deem necessary for the server.
- Configure additional drive volumes in SDS or VxVM, configure applications (such as iplanet web and app servers, Oracle, etc.) and restore data from backup (or reconnect via NFS to EMC).
- Complete time for total rebuild - 30 minutes to 2 hours depending on the client. For example, a standard client will take approximately 30 to 45 minutes. If the client requires Oracle or other customized apps, then the time frame is more like 2 hours.
- Unix admin starts the process of a rebuild.

The client currently has no methods or tools for handling a break-in of any magnitude. We have informed the client to obtain a "Rootkit" with necessary tools of their own that the can fit onto a CD in case of a potential break-in. Additionally, we pointed them to the web sites for obtaining information on the tasks to perform if they are broken into: http://www.fish.com/forensics/, http://www.porcupine.org/forensics/, http://www.cert.org/, and ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist. The nutshell of these links are summarized by the following:

Secure & Isolate the system - If possible, a good first step is to simply disconnect the system from the network. .

Record – record in a notebook what systems are being affected, the time, date, who discovered the problem and how you were made aware of it.

Evidence - The systematic search for evidence is what is needed next. The Coroner's Toolkit from http://www.porcupine.org/forensics/ is a good starting point for the necessary tools needed in case of a break-in. Collect binaries, shared libraries, config. files, etc. that will be needed. Remember to collect the most volatile of data first (memory) and then file system data later.

Evidence Inspection – Use tools such as Tripwire, Sherpa, RIACS Auditing package, or L5 to assess what may have changed on the file system.

Prosecution – collect evidence found for prosecution of the hacker on the system.

11. Other issues/vulnerabilities as appropriate

None that have not been already mentioned or specifically discussed below.

C. A prioritized list of security vulnerabilities or issues uncovered by your audit

The remaining vulnerabilities uncovered by this audit with the assistance of some tools (some output listed in Appendices) and popular books or guides are listed in this section.

Even after making the changes shown in the section titled "Configuration Vulnerabilities," there were some additional changes that needed to be made to make the system even more secure. These changes were mostly pointed out by various scanning tools such as:

COPS (use Kuang only to try and break into system) –
ftp://coast.cs.purdue.edu/pub/tools/unix/scanners/cops

TIGER (use all of it to try and find potential problems on system) –
ftp://coast.cs.purdue.edu/pub/tools/unix/scanners/tiger

Crack (used for cracking user's passwords – testing for strength of passwords) -
ftp://coast.cs.purdue.edu/pub/tools/unix/pwdutils/crack

Fix-modes – written by Casper Dik of Sun to find poor permissions on OS and alert and/or correct them. ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/fix-modes

ISS – (internet security scanner). The free version has much less features that commercially available version.
ftp://coast.cs.purdue.edu/pub/tools/unix/scanners/iis

Logcheck – used on syslog server to analyze log files for errors, or problems that admins should know about and send an email with info.
ftp://coast.cs.purdue.edu/pub/tools/unix/logutils/logcheck

Lsof – tool used to analyze what files are open and what processes are using them.
ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/lsof

Nessus – awesome state-of-the-art scanning tool to find weaknesses in systems. Many DDOS attacks! ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/nessus

Nfsbug – tool used to find nfs/ portmapper related weaknesses in systems.
ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/nfsbug

Nmap – tool used to map out the network contents, hostnames, rlogin hops, etc.
ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/nmap

Openssh – multipurpose tool used to encrypt basically all kinds of tcp traffic between machines, in lieu of telnet, rsh, rlogin, etc…
ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/openssh

Satan – a popular scanning tool (created by Farmer and Wietz)
ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/satan that has been superceded by:

Sara – scanning tool implemented by many gov. facilities to look for potential openings on systems. ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/sara

Saint – another scanning tool very closely based on Satan, except more modernized. ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/saint

Shadow – a cool and powerful intrusion detection tool.
ftp://coast.cs.purdue.edu/pub/tools/unix/ids/shadow

Snort – slightly less featureful IDS tool, that has been the Unix admins. Best friend for years. ftp://coast.cs.purdue.edu/pub/tools/unix/ids/snort

And many more that could have been used that overlap with those mentioned above.

References:

Some of the books/ guides that were employed were:

- "Solaris Security," by Peter H. Gregory. Sun Microsystems Press. Prentice Hall, Inc., 2000.
- "Solaris Security Step By Step," by The SANS Institute. V. 1.0. 1999.
- "Solaris Practicum, Track 6: Securing Unix Systems," by Hal Pomeranz, Deer Run Associates. 2000.
- "Running UNIX Applications Securely, Track 6: Securing Unix Systems," by Lee Brotzman and Hal Pomeranz. 2000.
- "Common Issues and Vulnerabilities in UNIX Security, Track 6: Securing Unix Systems," by Hal Pomeranz, Deer Run Associates. 2000.
- "Deploying DNS and Sendmail: SANS 2000 Course Book," March 22, 2000. By Hal Pomeranz.
- UNIX@Night, UNIX Forensics, by John Green. SANS 2000 Course Book. October 21, 2000.

D. A prioritized list of recommended fixes

With the use of these tools, the following additional recommendations were made to the client to further their security enhancements:

- /etc/default/ftpd

This file enables the feature available in the Solaris 7 and 8 OEs to change the default FTP banner. The banner is changed by adding a BANNER entry to the /etc/default/ftpd file. Like /etc/default/telnetd… (We will turn off inetd all together once ssh is fully implemented).

- /etc/init.d/inetsvc

Replace the default /etc/init.d/inetsvc with a minimized version containing only those commands required for the configuration of the network interfaces only.

- /etc/rc2.d/S47asppp

Turn off asynchronous PPP.

- /etc/rc2.d/S85power

Turn off autoshutdown features. And create /noautoshutdown file.

- /etc/rc2.d/S90webm

Turn off wbem support.

- /etc/rc2.d/S80PRESERVE

Turn preservation of vi file edits if vi or session crashes. This a well known security issue since preserve runs suid as root…

- set sendmail flag to –q

(no daemon mode, but flush que periodically 0 * * * * /usr/lib/sendmail –q in cron), or turn off sendmail start scripts all together and run job out of cron to flush que every five, ten… minutes.

- /etc/rc2.d/S72slpd

Turn off Service Locater Protocol support.

- Limit shell access to unused accounts in /etc/passwd.

Daemon, nuucp, smtp, listen, nobody, noaccess, nobody4 should not have the ability to gain a shell.

- /etc/rc2.d/S70uucp

Turn off uucp protocol support.

- /etc/default/inetinit

Enable RFC 1948 unique-per-connection ID sequence number generation by setting the /etc/default/inetinit TCP_STRONG_ISS value to 2.

This enables stack protection and logging included in all Solaris OE releases since version 2.6. These options are enabled by adding the following two commands to the /etc/system file:

- set noexec_user_stack = 1
- set noexec_user_stack_log = 1

After the two variables are set, the system denies attempts to execute the stack directly, and logs any stack execution attempt through SYSLOG. This facility is enabled to protect the system from common buffer overflow attacks.

- Set nfssrv:nfs_portmon = 1
- Set nfs:nfs_portmon = 1

This forces NFS clients to use privileged ports – protecting us from some common script-kiddie NFS exploits.

- Create an empty at.allow file in /etc/cron.d.

An empty at.allow file forces the system to check the at.deny file for unauthorized at users. In the at.deny file place all the users that you wish to disallow access to at. All users who require at access must now be added to the at.allow file.

- Create a new /etc/cron.d/cron.allow file to restrict access to the cron subsystem.

Only one account, root, is included in the new cron.allow file. No other system accounts are added. In the cron.deny file place all the users that you wish to disallow access to cron. The root account will be the only account able to schedule tasks through the cron subsystem, unless you specify allowed users in the cron.allow file.

- Run fix-modes (written by Casper Dik of Sun) script on system to check and modify permissions on the system.

mkdir fix-modes
mv fix-modes.tar.gz fix-modes
cd fix-modes
gunzip -c fix-modes.tar.gz | tar xf –
Build the software and simply tar up the fix-modes directory created above and copy the tar file over to the target platform.
……
sh fix-modes

The usage of fix-modes changed the permissions of roughly 1/3 of all the files on the system to more secure permissions.

- eeprom security-mode=command

Turn on EEPROM security functionality (this will only prompt for password if system is manually rebooted, not if system reboots itself). If a hacker gets in and brings system to prom level and sets a password of his own, we are in bad shape! We should do this…

- /etc/default/login

Uncomment RETRIES=5 and change 5 to 3 so that by reducing the logging threshold, additional information may be gained by syslog.

- Remove .rhosts support from PAM module (/etc/pam.conf)

- Remove all programming tools and libraries that comes on full distribution that they are installing (make, ar, ld, etc. and /usr/include stuff)

- use syslog-ng using tcp not udp and tunnel traffic through ssh to syslog server.

Everything should still be logged locally, but the only messages that should go to the syslog server are emerg, alert, crit, err, and auth.

- Turn off core dump in /etc/system -> set sys:coredumpsize=0

This prevents malicious users on system from forcing a core and analyzing the file's contents for passwords, etc. in the memory.

- Make empty .rhosts and hosts.equiv files in users home directory mode 600 (user and group = root).

D. Appendices:

Output from full Nessus scan (with nmap support):

1 20 5 5 172.16.66.210 Security holes found
172.16.66.210 ftp 21 tcp Security notes found unknown 22 tcp
Security notes found telnet 23 tcp
Security warning found sunrpc 111 tcp
Security notes found unknown 5987 tcp
Security notes found general/tcp general tcp
Security warning found general/udp general udp
Security notes found unknown 161 udp
Security hole found general/icmp general icmp
Security warning found Information ftp 21 Remote FTP server banner : idctest03.iisidc.com ftp server (sunos 5.8) ready.
Information unknown 22 Remote SSH version : ssh-2.0-openssh_2.1.1
Warning telnet 23 The Telnet service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords. You should disable this service and use OpenSSH instead. (www.openssh.com) Solution : Comment out the 'telnet' line in /etc/inetd.conf. Risk factor : Low CVE : CAN-1999-0619
Information telnet 23 Remote telnet banner : Warning general/tcp general The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. Solution : Contact your vendor for a patch Risk factor : Low
Information general/tcp general Nmap found that this host is running Sun Solaris 8 early acces beta through actual release
Information general/udp general For your information, here is the traceroute to 172.16.66.210 :
172.16.66.210 Vulnerability unknown 161 SNMP Agent responded as expected with community name: public CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: private CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: system CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: write CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: all CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: monitor CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: agent CVE : CAN-1999-0517

Vulnerability unknown 161 SNMP Agent responded as expected with community name: manager CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: OrigEquipMfr CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: admin CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: default CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: password CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: tivoli CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: openview CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: community CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: snmp CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: snmpd CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: Secret C0de CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: security CVE : CAN-1999-0517
Vulnerability unknown 161 SNMP Agent responded as expected with community name: all private CVE : CAN-1999-0517
Warning unknown 161 SNMP Agent port open, it is possible to execute SNMP GET and SET, (with the proper community names)
Warning general/icmp general The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentifications protocols. Solution : filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524
Warning general/icmp general The remote host answered to an ICMP_MASKREQ query and sent us its netmask. An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters. Solution : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17. Risk factor : Low CVE : CAN-1999-0524

Note: The SNMP info cannot be correct as the /etc/snmp/conf/snmpd.conf file specifies read-only to the public community and read-only to the local community we established.

Output from Tiger:

```
Security scripts *** undetermined ***
Thu Oct 26 21:55:52 GMT 2000
21:55> Beginning security report for idctest03 (sun4u SunOS 5.8).

# Performing check of passwd files...

# Performing check of group files...

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

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

```
# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

# Performing check of PATH components...
# Only checking user 'root'
--WARN-- [path001w] /bin/rstartd in root's PATH from .login is group `bin'
        writable.
--WARN-- [path001w] /usr/bin/rstartd in root's PATH from .login is group `bin'
        writable.
--WARN-- [path001w] /usr/sbin/install.d in root's PATH from .login is group
        `bin' writable.
--WARN-- [path001w] /usr/sbin/install.d in root's PATH from default is group
        `bin' writable.
--WARN-- [path001w] /usr/bin/rstartd in root's PATH from default is group
        `bin' writable.

# Performing check of anonymous FTP...

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

# Performing check of `cron' entries...
--WARN-- [cron001w] cron entry for root does not use full pathname
        command = [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
--WARN-- [cron001w] cron entry for root does not use full pathname
        command = [ -x /usr/lib/gss/gsscred_clean ] &&
        /usr/lib/gss/gsscred_clean

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet003f] The port for service pop-2 is assigned to service pop2.
--ERROR-- [init005e] Don't have required file INETDFILE.

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm001w] The owner of /etc/uucp/Permissions should be root (owned
        by uucp).
--WARN-- [perm021w] Disk device /dev/dsk/c0t0d0s0 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t0d0s0 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t0d0s7 has read access for group
```

```
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t0d0s7 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t0d0s5 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t0d0s5 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t0d0s6 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t0d0s6 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t0d0s1 has read access for group
        sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t0d0s1 has read access for group
        sys.

# Performing signature check of system binaries...
--ERROR-- [init005e] Don't have required file SIGNATURE_FILE.

# Checking for known intrusion signs...

# Performing check of files in system mail spool...

# Performing system specific checks...
# Performing checks for SunOS/5...
--WARN-- [no-id] The PROM monitor is not in secure mode.
--WARN-- [misc008w] NFS port checking disabled in kernel.
--ERROR-- [misc005w] Can't find check_sendmail'...

# Checking setuid executables...
--FAIL-- [fsys001f] File /etc/lp/alerts/printer is a setuid script:
-r-sr-xr-x   1 lp       lp         203 Dec 16  1999 /etc/lp/alerts/printer
--WARN-- [fsys002w] setuid program /usr/bin/nispasswd has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/passwd has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/yppasswd has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/fbconfig/SUNWifb_config has
        relative pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/fs/ufs/ufsrestore has relative
        pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/sendmail has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/kcms_calibrate has
        relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/kcms_configure has
        relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/sparcv9/kcms_configure has
        relative pathnames.
```

```
--WARN-- [fsys002w] setuid program /usr/openwin/bin/sys-suspend has relative
        pathnames.
--WARN-- [suidxxx] Setuid file `/usr/openwin/bin/xlock' which is group `bin'
        writable.

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

--CONFIG-- [fsys003c] No setuid list... listing all setuid files
---s--x--x root     bin      /usr/lib/pt_chmod
---s--x--x root     root     /usr/local/bin/sudo
---s--x--x root     uucp     /usr/bin/ct
---s--x--x uucp     uucp     /usr/bin/cu
---s--x--x uucp     uucp     /usr/bin/uucp
---s--x--x uucp     uucp     /usr/bin/uuglist
---s--x--x uucp     uucp     /usr/bin/uuname
---s--x--x uucp     uucp     /usr/bin/uustat
---s--x--x uucp     uucp     /usr/bin/uux
---s--x--x uucp     uucp     /usr/lib/uucp/remote.unknown
---s--x--x uucp     uucp     /usr/lib/uucp/uucico
---s--x--x uucp     uucp     /usr/lib/uucp/uusched
---s--x--x uucp     uucp     /usr/lib/uucp/uuxqt
-r-s--x--x root     bin      /usr/lib/lp/bin/netpr
-r-s--x--x root     lp       /usr/bin/cancel
-r-s--x--x root     lp       /usr/bin/lp
-r-s--x--x root     lp       /usr/bin/lpset
-r-s--x--x root     lp       /usr/bin/lpstat
-r-s--x--x root     lp       /usr/sbin/lpmove
-r-s--x--x root     sys      /usr/bin/admintool
-r-s--x--x uucp     bin      /usr/bin/tip
-r-sr-sr-x bin      bin      /usr/vmsys/bin/chkperm
-r-sr-sr-x root     bin      /usr/openwin/bin/ff.core
-r-sr-sr-x root     daemon   /usr/dt/bin/sdtcm_convert
-r-sr-sr-x root     sys      /usr/bin/nispasswd
-r-sr-sr-x root     sys      /usr/bin/passwd
-r-sr-sr-x root     sys      /usr/bin/yppasswd
-r-sr-sr-x root     sys      /usr/dt/bin/dtaction
-r-sr-xr-x lp       lp       /etc/lp/alerts/printer
-r-sr-xr-x root     bin      /usr/bin/crontab
-r-sr-xr-x root     bin      /usr/bin/eject
-r-sr-xr-x root     bin      /usr/bin/fdformat
-r-sr-xr-x root     bin      /usr/bin/login
-r-sr-xr-x root     bin      /usr/bin/pfexec
-r-sr-xr-x root     bin      /usr/bin/rcp
```

```
-r-sr-xr-x root    bin     /usr/bin/rdist
-r-sr-xr-x root    bin     /usr/bin/rlogin
-r-sr-xr-x root    bin     /usr/bin/rsh
-r-sr-xr-x root    bin     /usr/bin/sparcv7/uptime
-r-sr-xr-x root    bin     /usr/bin/sparcv7/w
-r-sr-xr-x root    bin     /usr/bin/sparcv9/uptime
-r-sr-xr-x root    bin     /usr/bin/sparcv9/w
-r-sr-xr-x root    bin     /usr/bin/volcheck
-r-sr-xr-x root    bin     /usr/bin/volrmmount
-r-sr-xr-x root    bin     /usr/dt/bin/dtappgather
-r-sr-xr-x root    bin     /usr/dt/bin/dtprintinfo
-r-sr-xr-x root    bin     /usr/dt/bin/dtsession
-r-sr-xr-x root    bin     /usr/lib/fbconfig/SUNWifb_config
-r-sr-xr-x root    bin     /usr/lib/fs/ufs/quota
-r-sr-xr-x root    bin     /usr/lib/fs/ufs/ufsdump
-r-sr-xr-x root    bin     /usr/lib/fs/ufs/ufsrestore
-r-sr-xr-x root    bin     /usr/lib/utmp_update
-r-sr-xr-x root    bin     /usr/sbin/afbconfig
-r-sr-xr-x root    bin     /usr/sbin/aspppls
-r-sr-xr-x root    bin     /usr/sbin/ffbconfig
-r-sr-xr-x root    bin     /usr/sbin/igsconfig
-r-sr-xr-x root    bin     /usr/sbin/m64config
-r-sr-xr-x root    bin     /usr/sbin/pgxconfig
-r-sr-xr-x root    bin     /usr/sbin/ping
-r-sr-xr-x root    bin     /usr/sbin/pmconfig
-r-sr-xr-x root    bin     /usr/sbin/sparcv7/whodo
-r-sr-xr-x root    bin     /usr/sbin/sparcv9/whodo
-r-sr-xr-x root    bin     /usr/sbin/static/rcp
-r-sr-xr-x root    bin     /usr/sbin/traceroute
-r-sr-xr-x root    other   /usr/lib/sendmail
-r-sr-xr-x root    sys     /usr/bin/chkey
-r-sr-xr-x root    sys     /usr/bin/sparcv7/ps
-r-sr-xr-x root    sys     /usr/bin/sparcv9/ps
-r-sr-xr-x root    sys     /usr/bin/su
-r-sr-xr-x root    sys     /usr/ucb/sparcv7/ps
-r-sr-xr-x root    sys     /usr/ucb/sparcv9/ps
-rwsr-sr-x root    bin     /usr/openwin/bin/kcms_calibrate
-rwsr-sr-x root    bin     /usr/openwin/bin/kcms_configure
-rwsr-sr-x root    bin     /usr/openwin/bin/sparcv9/kcms_configure
-rwsr-xr-x root    adm     /usr/lib/acct/accton
-rwsr-xr-x root    bin     /usr/openwin/bin/sys-suspend
-rwsr-xr-x root    bin     /usr/openwin/lib/mkcookie
-rwsr-xr-x root    bin     /usr/sbin/allocate
-rwsr-xr-x root    bin     /usr/sbin/deallocate
-rwsr-xr-x root    bin     /usr/sbin/list_devices
-rwsr-xr-x root    bin     /usr/sbin/mkdevalloc
```

```
-rwsr-xr-x root     bin      /usr/sbin/mkdevmaps
-rwsr-xr-x root     sys      /usr/bin/at
-rwsr-xr-x root     sys      /usr/bin/atq
-rwsr-xr-x root     sys      /usr/bin/atrm
-rwsr-xr-x root     sys      /usr/bin/newgrp
-rwsr-xr-x root     sys      /usr/sbin/sacadm
-rwsrwxr-x root     bin      /usr/openwin/bin/xlock

--ERROR-- [init005e] Don't have required file SIGNATURE_FILE.

# Checking setgid executables...

--CONFIG-- [fsys003c] No setgid list... listing all setgid files
--ERROR-- [init005e] Don't have required file SIGNATURE_FILE.

# Checking unusual file names...

# Looking for unusual device files...

# Checking symbolic links...

# Checking for writable directories...
--INFO-- [fsys008i] The following directories are world writable:
/var/dt/dtpower/schemes/
/var/dt/tmp/
/var/mail/
/var/preserve/
/var/run/rpc_door/
/var/spool/lp/fifos/public/
/var/spool/pkg/
/var/spool/uucppublic/

The following files have undefined groups ownership:


# Performing check of embedded pathnames...
--WARN-- [embed001w] Path `/etc/lp/alerts/jobdone' contains `/etc/lp' which is
        not owned by root (owned by lp).
        Embedded references in: /usr/lib/lp/local/lp->/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/default(PATH)
--WARN-- [embed003w] Path `/etc/lp/alerts/jobdone' contains `/etc/lp' which is
        group `lp' writable.
        Embedded references in: /usr/lib/lp/local/lp->/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/default(PATH)
```

```
--WARN-- [embed001w] Path `/etc/lp/alerts/jobdone' contains `/etc/lp/alerts'
        which is not owned by root (owned by lp).
        Embedded references in: /usr/lib/lp/local/lp->/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/default(PATH)
--WARN-- [embed003w] Path `/etc/lp/alerts/jobdone' contains `/etc/lp/alerts'
        which is group `lp' writable.
        Embedded references in: /usr/lib/lp/local/lp->/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/default(PATH)
--WARN-- [embed002w] Path `/etc/lp/alerts/jobdone' is not owned by root (owned
        by lp).
        Embedded references in: /usr/lib/lp/local/lp->/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /usr/lib/lp/local/lp->/usr/bin/lp->/default(PATH)
--WARN-- [embed001w] Path `/etc/lp/alerts/sendMsg' contains `/etc/lp' which is
        not owned by root (owned by lp).
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed003w] Path `/etc/lp/alerts/sendMsg' contains `/etc/lp' which is
        group `lp' writable.
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed001w] Path `/etc/lp/alerts/sendMsg' contains `/etc/lp/alerts'
        which is not owned by root (owned by lp).
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed003w] Path `/etc/lp/alerts/sendMsg' contains `/etc/lp/alerts'
        which is group `lp' writable.
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                                /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed002w] Path `/etc/lp/alerts/sendMsg' is not owned by root (owned
        by lp).
```

```
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                        /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                        /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed003w] Path `/usr/dt/bin/dtaction' contains `/usr/dt' which is
        group `bin' writable.
        Embedded references in: /usr/dt/bin/dtprintinfo->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtaction' contains `/usr/dt/bin' which
        is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtprintinfo->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtchooser' contains `/usr/dt' which is
        group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtchooser' contains `/usr/dt/bin' which
        is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtgreet' contains `/usr/dt' which is
        group `bin' writable.
        Embedded references in: /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/.login(PATH)
                        /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/default(PATH)
--WARN-- [embed003w] Path `/usr/dt/bin/dtgreet' contains `/usr/dt/bin' which
        is group `bin' writable.
        Embedded references in: /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/.login(PATH)
                        /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/default(PATH)
--WARN-- [embed003w] Path `/usr/dt/bin/dtlogin' contains `/usr/dt' which is
        group `bin' writable.
        Embedded references in: /etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtlogin' contains `/usr/dt/bin' which
        is group `bin' writable.
        Embedded references in: /etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtpad' contains `/usr/dt' which is
        group `bin' writable.
        Embedded references in: /usr/dt/bin/Xsession->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtpad' contains `/usr/dt/bin' which is
        group `bin' writable.
        Embedded references in: /usr/dt/bin/Xsession->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtprintinfo' contains `/usr/dt' which
        is group `bin' writable.
        Embedded references in: /etc/init.d/dtlogin
```

--WARN-- [embed003w] Path `/usr/dt/bin/dtprintinfo' contains `/usr/dt/bin' which is group `bin' writable.
Embedded references in: /etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtsession_res' contains `/usr/dt' which is group `bin' writable.
Embedded references in: /usr/dt/config/Xpasswd->/usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtsession_res' contains `/usr/dt/bin' which is group `bin' writable.
Embedded references in: /usr/dt/config/Xpasswd->/usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtterm' contains `/usr/dt' which is group `bin' writable.
Embedded references in: /usr/dt/config/Xpasswd->/usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/dtterm' contains `/usr/dt/bin' which is group `bin' writable.
Embedded references in: /usr/dt/config/Xpasswd->/usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/sdt_firstlogin' contains `/usr/dt' which is group `bin' writable.
Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/sdt_firstlogin' contains `/usr/dt/bin' which is group `bin' writable.
Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/Xsession' contains `/usr/dt' which is group `bin' writable.
Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/bin/Xsession' contains `/usr/dt/bin' which is group `bin' writable.
Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/config/Xpasswd' contains `/usr/dt' which is group `bin' writable.
Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/config/Xpasswd' contains `/usr/dt/config' which is group `bin' writable.
Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/config/Xpasswd2' contains `/usr/dt' which is group `bin' writable.
Embedded references in: /usr/dt/config/Xpasswd->/usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/config/Xpasswd2' contains `/usr/dt/config' which is group `bin' writable.
Embedded references in: /usr/dt/config/Xpasswd->/usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/config/Xsession.ow' contains `/usr/dt'

```
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/sdt_firstlogin->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/dt/config/Xsession.ow' contains
        `/usr/dt/config' which is group `bin' writable.
        Embedded references in: /usr/dt/bin/sdt_firstlogin->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
--WARN-- [embed001w] Path `/usr/lib/sa/sadc' contains `/usr/lib/sa' which is
        not owned by root (owned by adm).
        Embedded references in: /bin/sar->/.login(PATH)
                        /bin/timex->/.login(PATH)
                        /etc/init.d/perf
                        /usr/bin/sar->/.login(PATH)
                        /usr/bin/sar->/default(PATH)
                        /usr/bin/timex->/.login(PATH)
                        /usr/bin/timex->/default(PATH)
                        /usr/sbin/sar->/.login(PATH)
                        /usr/sbin/sar->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/cmdtool' contains
        `/usr/openwin/bin' which is group `bin' writable.
        Embedded references in: /bin/admintool->/.login(PATH)
                        /usr/bin/admintool->/.login(PATH)
                        /usr/bin/admintool->/default(PATH)
                        /usr/sbin/swmtool->/.login(PATH)
                        /usr/sbin/swmtool->/default(PATH)
--WARN-- [embed004w] Path `/usr/openwin/bin/cmdtool' is group `bin' writable.
        Embedded references in: /bin/admintool->/.login(PATH)
                        /usr/bin/admintool->/.login(PATH)
                        /usr/bin/admintool->/default(PATH)
                        /usr/sbin/swmtool->/.login(PATH)
                        /usr/sbin/swmtool->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/fbconsole' contains
        `/usr/openwin/bin' which is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/bin/fs' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/Xsession->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/bin/fs' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/Xsession->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/bin/fs' contains
        `/usr/openwin/bin/xfs' which is group `bin' writable.
        Embedded references in: /usr/dt/bin/Xsession->/usr/dt/bin/dtlogin-
>/etc/init.d/dtlogin
```

```
--WARN-- [embed003w] Path `/usr/openwin/bin/gfxres' contains
        `/usr/openwin/bin' which is group `bin' writable.
        Embedded references in: /usr/sbin/GFXconfig->/.login(PATH)
                        /usr/sbin/GFXconfig->/default(PATH)
                        /usr/sbin/pgxconfig->/.login(PATH)
                        /usr/sbin/pgxconfig->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/mp' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /bin/lp_1251->/.login(PATH)
                        /usr/bin/lp_1251->/.login(PATH)
                        /usr/bin/lp_1251->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/sys-suspend' contains
        `/usr/openwin/bin' which is group `bin' writable.
        Embedded references in: /usr/lib/power/powerd->/usr/sbin/pmconfig-
>/.login(PATH)
                        /usr/lib/power/powerd->/usr/sbin/pmconfig->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/ttsession' contains
        `/usr/openwin/bin' which is group `bin' writable.
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                        /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                        /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed004w] Path `/usr/openwin/bin/ttsession' is group `bin'
        writable.
        Embedded references in: /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/bin/lp-
>/.login(PATH)
                        /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp->/.login(PATH)
                        /etc/lp/alerts/jobdone->/usr/lib/lp/local/lp->/usr/bin/lp-
>/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/winsysck' contains
        `/usr/openwin/bin' which is group `bin' writable.
        Embedded references in: /bin/eject->/.login(PATH)
                        /usr/bin/eject->/.login(PATH)
                        /usr/bin/eject->/default(PATH)
--WARN-- [embed004w] Path `/usr/openwin/bin/winsysck' is group `bin' writable.
        Embedded references in: /bin/eject->/.login(PATH)
                        /usr/bin/eject->/.login(PATH)
                        /usr/bin/eject->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/X' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/bin/X' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/bin/xauth' contains `/usr/openwin/bin'
```

```
        which is group `bin' writable.
        Embedded references in: /usr/local/sbin/sshd->/.login(PATH)
--WARN-- [embed004w] Path `/usr/openwin/bin/xauth' is group `bin' writable.
        Embedded references in: /usr/local/sbin/sshd->/.login(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/xlock' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/.login(PATH)
                        /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/default(PATH)
--WARN-- [embed004w] Path `/usr/openwin/bin/xlock' is group `bin' writable.
        Embedded references in: /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/.login(PATH)
                        /usr/openwin/bin/sys-suspend->/usr/lib/power/powerd-
>/usr/sbin/pmconfig->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/bin/xrdb' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed004w] Path `/usr/openwin/bin/xrdb' is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/bin/xterm' contains `/usr/openwin/bin'
        which is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed004w] Path `/usr/openwin/bin/xterm' is group `bin' writable.
        Embedded references in: /usr/dt/bin/dtlogin->/etc/init.d/dtlogin
--WARN-- [embed003w] Path `/usr/openwin/lib/X11/rstart/rstartd.real' contains
        `/usr/openwin/lib' which is group `bin' writable.
        Embedded references in: /bin/rstartd->/.login(PATH)
                        /usr/bin/rstartd->/.login(PATH)
                        /usr/bin/rstartd->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/lib/X11/rstart/rstartd.real' contains
        `/usr/openwin/lib/X11' which is group `bin' writable.
        Embedded references in: /bin/rstartd->/.login(PATH)
                        /usr/bin/rstartd->/.login(PATH)
                        /usr/bin/rstartd->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/server/etc/pgxresinfo' contains
        `/usr/openwin/server' which is group `bin' writable.
        Embedded references in: /usr/sbin/GFXconfig->/.login(PATH)
                        /usr/sbin/GFXconfig->/default(PATH)
                        /usr/sbin/pgxconfig->/.login(PATH)
                        /usr/sbin/pgxconfig->/default(PATH)
--WARN-- [embed003w] Path `/usr/openwin/server/etc/pgxresinfo' contains
        `/usr/openwin/server/etc' which is group `bin' writable.
        Embedded references in: /usr/sbin/GFXconfig->/.login(PATH)
                        /usr/sbin/GFXconfig->/default(PATH)
                        /usr/sbin/pgxconfig->/.login(PATH)
```

/usr/sbin/pgxconfig->/default(PATH)
--WARN-- [embed004w] Path `/usr/sadm/lib/wbem/cimomboot' is group `sys'
writable.
Embedded references in: /etc/init.d/init.wbem
--WARN-- [embed004w] Path `/usr/sadm/lib/wbem/wbemconfig' is group `sys'
writable.
Embedded references in: /usr/sadm/lib/wbem/cimomboot->/etc/init.d/init.wbem

Output from crack (edited to preserve security):

---- passwords cracked as of Wed Nov 1 00:07:27 GMT 2000 ----

973032354:Guessed xxxxx [xxxxx] [/usr/local/crack/passwd /bin/ksh]
973032362:Guessed xxxxx [xxxxx] [/usr/local/crack/passwd /bin/ksh]
973032364:Guessed xxxxx [xxxxx] [/usr/local/crack/passwd /bin/ksh]
973032366:Guessed xxxxx [xxxxx] [/usr/local/crack/passwd /bin/ksh]
973032368:Guessed xxxxx [xxxxx] [/usr/local/crack/passwd /bin/ksh]
973032370:Guessed xxxxx [xxxxx] [/usr/local/crack/passwd /bin/ksh]

---- errors and warnings ----

E:973032234:StoreDataHook: invalid ciphertext: adm NP
E:973032234:StoreDataHook: invalid ciphertext: bin NP
E:973032234:StoreDataHook: invalid ciphertext: daemon NP
E:973032234:StoreDataHook: invalid ciphertext: lp NP
E:973032234:StoreDataHook: invalid ciphertext: noaccess NP
E:973032234:StoreDataHook: invalid ciphertext: nobody NP
E:973032234:StoreDataHook: invalid ciphertext: nobody4 NP
E:973032234:StoreDataHook: invalid ciphertext: nuucp NP
E:973032234:StoreDataHook: invalid ciphertext: sys NP
E:973032234:StoreDataHook: invalid ciphertext: uucp NP
E:973032234:StoreDataHook: wg='adm Admin' un='adm' cm='Admin [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='bin ' un='bin' cm=' [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='daemon ' un='daemon' cm=' [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='lp Line Printer Admin' un='lp' cm='Line Printer Admin [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='noaccess No Access User' un='noaccess' cm='No Access User [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='nobody Nobody' un='nobody' cm='Nobody [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='nobody4 SunOS 4.x Nobody' un='nobody4' cm='SunOS 4.x Nobody [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='nuucp uucp Admin' un='nuucp' cm='uucp Admin [/usr/local/crack/passwd /usr/lib/uucp/uucico]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='sys ' un='sys' cm=' [/usr/local/crack/passwd]' ct='NP' sk='NP'
E:973032234:StoreDataHook: wg='uucp uucp Admin' un='uucp' cm='uucp Admin [/usr/local/crack/passwd]' ct='NP' sk='NP'

Output from Satan, Sara, Saint, and iss resulted in no errors, warnings or notices.