Global Information Assurance Certification Paper

Steven F. Giessler - Sans Security DC2000
Track 6 Unix Security – Practical Examination

Security Audit: (Hostnames, IPs, and userids, have been "sanitized" with five stars - *****)
1 Sun Server: University Departmental Critical infrastructure server, web server, e-mail server.

Hardware:

Sun Ultra Enterprise 2
Memory: 16 slots, 8 slots full, total 64M*8 = 512M
Disk space: 1 internal disk (4G), two external disks (50G each)
CPU: 1 CPU, 296M

Software:

OS: Solaris 2.6
Apache Server 1.3.9 with servlet engine (jsdk2.0)
JDK1.1.6 (no JDBC support)
perl 5.004_01
gcc 2.95.2, make 3.76.1
elm 2.5.3 (Y2K compliant), pine 3.96
LeTeX 3.14159

General Use policies:

1. What is the server used for?

Web-server: Apache 1.3.9
E-mail server: Sendmail 8.6
FTP server: Standard Solaris 2.6 Daemon
Anonymous FTP allowed? No
Samba Server (mount users' home directories on Windows clients)
Netatalk Server (mount users' home directories on Macintosh clients)
Statistics and Math professors use this server for LeTeX – also used as a development machine for classroom instruction – primarily the web server is used as an instructional aid – examples, and interactive exercises using Java Servlets.
Shell accounts? Yes – all 200 users have shell accounts with telnet and ftp access – these are used for programming and personal web-space.

2. Who has physical access to the server?

Server is in a second floor room which is behind two locked doors – no deadbolt, no alarm system, windows on and around the outer door could be smashed to open the door – the windows do however have a wire mesh inside the glass that might serve as a deterrent. The outer door is locked at all times; the inner door is locked when the server room is vacant. At night the building is locked which provides a third "locked set of doors." Five people have the keys – The building manager, the custodian, two system administrators, and their supervisor. Of these people only the two system administrators and their supervisor are authorized (have accounts) to login to the console. One window to the outdoors is not easily accessible (i.e. without a ladder).

3. Who has root access?

The two System Administrators have root access; all other users have non-privileged access. Remote root logins are not allowed. Telnet is allowed but TCP wrapper 7.6 is installed and configured to limit access to

the server to machines on campus. A university affiliated dial-up network as well as a few small local dial-up ISPs are also allowed in through the TCP wrapper.

4. How are users authenticated?

NIS+ This machine is a NIS+ master server – two other Solaris machines are NIS+ clients that users are also able to login to with their accounts. Users login using NIS+ authentication using the standard RPC services installed with Solaris 2.6.

VULNERABILITY: the command "niscat passwd.org_dir" is executable by any user on the system and gives the user the encrypted password file.

5. What are the password policies?

Root password is changed infrequently – every few months – with no set schedule. Users may change their passwords if and when they wish to. No enforcement of changing them at predefined intervals – no enforcement of "good" passwords or "using similar passwords" when changing them. Passwords do not expire.

Crack 5.0 report (usernames sanitized):

```
# ./Reporter
---- passwords cracked as of Fri Aug 11 15:39:46 EDT 2000 ----

0:Guessed ****** [<no-ciphertext>]  Full Name [passwd.file /bin/tcsh]
958775573:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958776092:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958776097:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958776480:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958776968:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958807693:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958807769:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958809180:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958812035:Guessed ****** [passwd] Full Name [passwd.file /bin/csh]
958827151:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958827241:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958827269:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958827435:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958827491:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958828839:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958829109:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958831090:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958833967:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
958833968:Guessed adm [passwd]  Admin [passwd.file ]
958953807:Guessed ****** [passwd] Full Name [passwd.file /bin/tcsh]
```

Out of 200 accounts on the sytem, 21 Passwords were guessed by the Crack program. Usernames have been starred out (*****), real names changed to "Full Name" – guessed passwords were changed to "passwd". Interesting to note that most of the password's were simple dictionary words with 1 number added to the beginning or end of the password (i.e. "super8"). Also note that the "adm" account password was guessed. – **VULNERABILITY**

Operating System Vulnerabilities

1. What patches are installed? See Patchdiag analysis in **APPENDIX A**

2. File system vulnerabilities – see COPS report in **APPENDIX B**

Configuration Vulnerabilities

1. inetd.conf

```
# cat /etc/inetd.conf
#
#ident  "@(#)inetd.conf 1.27    96/09/24 SMI"   /* SVr4.0 1.5   */
#
#
# Configuration file for inetd(1M).  See inetd.conf(4).
#
# To re-configure the running inetd process, edit this file, then
# send the inetd process a SIGHUP.
#
# Syntax for socket-based Internet services:
#  <service_name> <socket_type> <proto> <flags> <user> <server_pathname> <args>
#
# Syntax for TLI-based Internet services:
#
#  <service_name> tli <proto> <flags> <user> <server_pathname> <args>
#
# Ftp and telnet are standard Internet services.
#
ftp     stream  tcp     nowait  root    /usr/sbin/in.ftpd  in.ftpd
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
#
# Tnamed serves the obsolete IEN-116 name server protocol.
#
name    dgram   udp     wait    root    /usr/sbin/tcpd  in.tnamed
# Time service is used for clock synchronization.
#
time    stream  tcp     nowait  root    internal
time    dgram   udp     wait    root    internal
# Solstice system and network administration class agent server
100232/10       tli     rpc/udp wait root /usr/sbin/tcpd        sadmind
printer         stream  tcp     nowait  root    /usr/lib/print/in.lpd   in.lpd
100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd /usr/dt/bin/rpc.ttdbserverd
536870916/1     dgram   rpc/udp wait root /opt/SUNWvts/bin/vtsk /opt/SUNWvts/bin/vtsk
# rpc.metad
100229/1        tli     rpc/tcp         wait    root    /usr/opt/SUNWmd/sbin/rpc.metad  rpc.metad
# rpc.metamhd
100230/1        tli     rpc/tcp         wait    root    /usr/opt/SUNWmd/sbin/rpc.metamhd        rpc.metamhd
#imap   stream  tcp     nowait  root    /opt/SUNWimap/lib/imapd imapd
#imap   stream  tcp     nowait  root    /usr/sbin/tcpd          /opt/SUNWimap/lib/imapd
imap    stream  tcp     nowait  root    /usr/sbin/tcpd          /usr/sbin/imapd
#pop3   stream  tcp     nowait  root    /opt/SUNWipop/lib/ipop3d ipop3d
#pop3   stream  tcp     nowait  root    /usr/sbin/tcpd          /opt/SUNWipop/lib/ipop3d
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd          /usr/sbin/ipop3d
```

Unused services had been removed from the above file or commented out. All r-services had been removed from this file.

VULNERABILITY: ftp daemon is NOT passing through the tcp wrapper and is vulnerable to outside attack. The line should read:

```
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd
```

2. Umask for System Daemons set to 022 – this is good.

3. /etc/notrouter file does not exist – should create it since this machine is not serving as a router.

4. Could also add additional configuration tuning parameters to /etc/initd./inetinit to help prevent various buffer overflow attacks.

5. /etc/vfstab

```
# more /etc/vfstab
#device        device          mount           FS      fsck    mount   mount
#to mount      to fsck         point           type    pass    at boot options
#
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr         ufs     1       yes     -
fd      -       /dev/fd fd      -       no      -
/proc   -       /proc   proc    -       no      -
/dev/dsk/c0t0d0s1       -       -       swap    -       no      -
/dev/dsk/c0t0d0s0       /dev/rdsk/c0t0d0s0      /       ufs     1       no      -
/dev/dsk/c0t0d0s4       /dev/rdsk/c0t0d0s4      /usr    ufs     1       no      -
/dev/dsk/c0t0d0s3       /dev/rdsk/c0t0d0s3      /var    ufs     1       no      -
/dev/dsk/c0t0d0s5       /dev/rdsk/c0t0d0s5      /opt    ufs     2       yes     -
#/dev/dsk/c0t5d0s2      /dev/rdsk/c0t5d0s2      /ext02 ufs      2       yes     -
/dev/dsk/c0t1d0s6       /dev/rdsk/c0t1d0s6      /ext01  ufs     2       yes     -
/dev/dsk/c0t3d0s6       /dev/rdsk/c0t3d0s6      /stat   ufs     2       yes     -
swap    -       /tmp    tmpfs   -       yes     -
```

VULNERABILITY: Might want to re-mount filesystems with the nosuid mount option (if no suid binaries or scripts are in use or needed on these filesystems).

6. System logging:

/etc/syslog.conf did not contain an auth.info line:

auth.info /var/log/authlog

7. #eeprom

The parameter:

security-mode=none

Indicates that the eeprom setting for the machine is set to "none" – **VULNERABILITY**

8. NFS exported filesystems:

```
# cat /etc/dfs/dfstab
#       Place share(1M) commands here for automatic execution
#       on entering init state 3.
#
#       Issue the command '/etc/init.d/nfs.server start' to run the NFS
#       daemon processes and the share commands, after adding the very
#       first entry to this file.
#
#       share [-F fstype] [ -o options] [-d "<text>"] <pathname> [resource]
#       .e.g,
#       share  -F nfs  -o rw=engineering  -d "home dirs"  /export/home2

share -F nfs -o rw=server1:server2:server3 -d "binary shares"      /share

share -F nfs -o rw=server1:server2:server3 -d "mail"              /var/mail

share -F nfs -o rw=server1:server2:server3 -d "home"              /home
```

Three directories are exported via NFS. Two other Sun servers have them mounted remotely - /home is all of the users' home directories, /share is the shared programs on the system, and /var/mail is all of the users' mail folders. – **VULNERABILITY**

9. Network vulnerability scan: See Nessus report – APPENDIX C

Risks from installed third-party software

SSH 1.2.22 is running – vulnerable to buffer overflow - **VULNERABILITY**

Sendmail 8.6 – Multible Vulnerabilities. (See Nessus report in this document) - **VULNERABILITY**

Pine 3.96 installed – no well documented security holes, but should upgrade to latest version

Elm 2.5.3 installed – this is the latest version

Lynx 2.8.3 installed – this is the latest version

Samba 2.0.7 installed – this is the latest version

Netatalk 1.3.3 is installed - no documented security holes, however may pose as a security risk since it allows filesystems to be mounted remotely and in the clear (on Macintosh client machines).

Administrative Practices

1. No formal account management process. Accounts are requested through e-mail and accounts are distributed by e-mail. – **VULNERABILITY**

2. Software is installed only by the two primary System Administrators with root access.

3. Hardware and Software upgrades are only done by the two primary System Adminstrators.

4. System logs are looked at infrequently by System Administrators. Logs have no automated monitoring.

5. User accounts are not set to expire, nor are they purged from the system when a user leaves the university. There are many old accounts that are no longer used and still taking up space on the system. Also the owners of these accounts may still login at any time if they wish.

Backup policies, disaster preparedness, etc.

VULNERABILITY: Networked backup in use. Solstice Backup 5.1 (Legatto Networker repackaged by Sun) is used to backup this server over the LAN to a tape library connected to another Sun server. This entire backup of the server passes over the network in the clear to the tape library.

Backup policies: Incremental backup done nightly at 1 am. Full backup done once a week at 1 am on Sunday. The Cybernetics tape library holds fourteen 50 gig tapes and it is holds data from 4 Sun servers. The tapes are recycled when they are full and old data is overwritten. At present this occurs approximately once every 2 months (retention period).

VULNERABILITY: There is no "master backup" set of tapes stored in another building – recommended (In the event of a fire – all would be lost).

Restores of individual files have been tested and do work. Also, Legatto Networker has it's own fairly sophisticated disaster recovery procedures.

Other issues

1. Monitor plugged into Uninterruptable Power Supply. Should probably not be plugged in there to increase the life of the battery during a power failure.

2. X-windows server running on the machine. No control over who can use this remotely.

Prioritized list of security vulnerabilities or issues uncovered by the audit (ordered highest to lowest priority):

1. Sendmail 8.6 running in daemon mode. Arbitrary commands may be accepted by the system – could be used to gain root access.

2. SSH 1.2.22 Vulnerability – buffer overflow – may be used to gain root access.
http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D797

3. RPC services running – these 3 daemons all have known security holes that may be exploited to gain root access to the machine:

statd – network status monitor
sadmin - distributed system administration daemon
cmsd – calendar manager daemon

4. Telnet service running – All information in these sessions is being passed over the network in the clear and can be captured by an attacker and used in exploiting the system.

5. SNMP Agent responds to default community names – allows an attacker to gather information about the network and use it to plan an attack

6. NIS+ master server – all 200 accounts on the system (except root) are distributed to two other machines with NIS+.

7. NFS exported directories – all home directories are exported via NFS, also the mail directory and a shared binaries directory are also exported via NFS

8. SSH – kerberos used – and tickets are stored in NFS exported home directories – home directories also accessible via SMB and Netatalk.

9. Numerous Solaris Security Patches not installed – See **APPENDIX A**

10. COPS report – numerous files and user directories are world writable - including several files in the /etc directory – See **APPENDIX B**

11. niscat passwd.org_dir command – any user can read password file and crack passwords

12. Poor passwords – more than 10% of the passwords were cracked by Crack 5.0

13. EEPROM password set to "none"

14. FTP daemon is not passing through the tcp wrapper

15. Suid binaries may be run from any filesystem

16. Networked backup in use – Solstice Backup – whole filesystems are transferred in the clear over the network.

17. No master set of backup tapes located in off premises.

Prioritized list of recommended fixes (ordered highest to lowest priority):

1. Update Sendmail to version 8.9 or higher to prevent buffer overflow attacks and possilbe remote root access.

2. Update SSH to latest version to prevent buffer overflow attacks and possilbe remote root access.

3. Turn off the RPC services statd, sadm, and cmsd, if they are not being used.

4. Disable the telnet daemon and require all users to use SSH to login to their shell accounts.

5. Change the SNMP Agent Community names to something other than the defaults. This is especially dangerous because an attacker might use it to quickly gain info about other servers on the LAN.

6. If possible, remove NIS+ competely and have all users accounts stored as regular local accounts. Since there are only two other machines that users can login to with NIS+, this shouldn't be too difficult, also, it may be prudent to question the need for these users to be able to login to all three systems. Perhaps only certain accounts need to go onto certain machines.

7. If possible, turn off NFS and it's associated daemons. Filesystems that are exported, should be copied to the machines where they are needed.

8. Install the recommended patch cluster for Solaris 2.6 from http://www.sunsolve.com. Then Run "Patchdiag" again to be sure that all necessary patches were installed. If not, download and install each missing one individually.

9. Based on the COPS report in **APPENDIX B,** go through and change file modes and directory modes to a more reasonable (safer) set. Do this manually, and/or run th program "fix-modes, by Casper Dik"

10. To prevent any user from reading the password file and cracking passwords using the command "niscat passwd.org_dir" – chmod 700 the niscat executable. If NIS+ is removed completely, this is a moot point of course.

11. Enforce "good password policy" to eliminate Crack's ability to guess user passwords. Do this by installing "Password +" and/or explaining to users in a system wide e-mail, how to create a good password. Expire passwords periodically, and have "Password +" keep a history of passwords so users aren't tempted to swap back and for the between two or three passwords.

12. Set the EEPROM password. If this is not done, an attacker could potentially set the password himself, change the security mode to "full" and reboot the machine – creating a very nasty denial of service attack (cannot use machine until EEPROM is replaced by Sun – could take a month or more).

13. Change /etc/inetd.conf so that ftp connections pass throught the tcp wrapper before connecting to the ftp daemon. The line should read:

```
ftp    stream  tcp    nowait  root    /usr/sbin/tcpd  in.ftpd
```

14. In /etc/vfstab, set mount options to "nosuid" for non-root partitions.

15. Remove the Networked backup System and install dedicated tape drives for each server. If this cannot be done, then perhaps there is a way to tunnel this information through SSH, or provide a dedicated network (separate from the LAN) for the backups.

16. Download and install the YASSP (Yet Another Solaris Security Package) hardening scripts and install them.

18. Create obscure (or bogus) banner and version entries for FTP server, Apache web-server, Sendmail POP3 server, SSH, telnet (if used), Solaris version, and for any other daemon listening on a port that will report it's name and/or version number.

19. Create an /etc/issue file warning against unauthorized access to the machine and notifying those who connect that all activites are logged and may be used as evidence in prosecution of a person obtaining unauthorized access and/or conducting unauthorized activities on the server.

20.. After all of the above is completed and tested thoroughly, make a "gold" master backup of the server and place the tapes in a secure location off premises. This way, in the event of an environmental disaster (fire, flood, etc) all is not lost.

Optional, yet highly recommended improvements:

1. Install and use a program like Tripwire to monitor file integrity.

2. Install and use a program like Logcheck to help automate the monitoring of logs.

3. Install NTP (Network Time Protocol) and have the clock synchronized to an NTP server.

4. Setup a syslog server and point all logging entries in /etc/syslog.conf to the syslog server so you have redundant logging.

5. Use Kerberos user authentication instead of the standard Unix authentication.

6. Change the root password regularly (at least once a month).

7. Create a system of recordkeeping for managing user accounts. Write policy to govern this. Purge old accounts according to policy and in a timely fashion following the user's departure from the university.

8. Purchase a shredder and have it available near system printers. Shred any and all documents containing "sensitive" information – i.e. user accounts, passwords, etc.

9. Create a new system for distributing accounts. Requests for new accounts might come through e-mail, but have one person responsible for checking the IDs of the requestors in person, and giving them the account information form that is not on the network (i.e. paper). Don't use e-mail to distribute account information.

10. Run Crack regularly to be sure your users are choosing "good" passwords.

11. Come up with a way to encrypt remote X-sessions or disable this functionality.

APPENDIX A

```
# ./patchdiag
================================================================================
System Name: *****     SunOS Vers: 5.6        Arch: sparc
Cross Reference File Date: 07/Aug/00

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

Recommended patches are considered the most important and highly
recommended patches that avoid the most critical system, user, or
security related bugs which have been reported and fixed to date.
A patch not listed on the recommended list does not imply that it
should not be used if needed.  Some patches listed in this report
may have certain platform specific or application specific dependencies
and thus may not be applicable to your system.  It is important to
carefully review the README file of each patch to fully determine
the applicability of any patch with your system.
================================================================================
INSTALLED PATCHES
Patch  Installed Latest   Synopsis
 ID   Revision  Revision
------ --------- -------- ------------------------------------------------------
105181   11        22    SunOS 5.6: Kernel update patch
105210   24        32    SunOS 5.6: libaio, libc & watchmalloc patch
105216   03        04    SunOS 5.6: /usr/sbin/rpcbind patch
105284   05        37    Motif 1.2.7: Runtime library patch
105338   14        25    CDE 1.2: dtmail patch
105346   05        12    Solstice Internet Mail Server 2.0: Misc. fixes
105356   04        16    SunOS 5.6: /kernel/drv/ssd and /kernel/drv/sd patch
105357   01        04    SunOS 5.6: /kernel/drv/ses patch
105375   06        24    SunOS 5.6: sf & socal driver patch
105379   05    CURRENT   SunOS 5.6: /kernel/misc/nfssrv patch
105393   01        07    OBSOLETED by 105621
105401   08        28    SunOS 5.6: libnsl and NIS+ commands patch
105407   01    CURRENT   SunOS 5.6: /usr/bin/volrmmount patch
105464   01        02    OpenWindows 3.6: Multiple xterm fixes
105490   07    CURRENT   OBSOLETED by 107733
105518   01    CURRENT   OBSOLETED by 105395
105558   01        04    CDE 1.2: dtpad patch
105615   04        08    SunOS 5.6: /usr/lib/nfs/mountd patch
105621   02        24    SunOS 5.6: c2audit, libbsm and cron patch
105665   01        03    SunOS 5.6: /usr/bin/login patch
105667   01        02    SunOS 5.6: /usr/bin/rdist patch
105669   02        10    CDE 1.2: libDtSvc Patch
105686   02    CURRENT   OBSOLETED by 105621
105703   07        22    CDE 1.2: dtlogin patch
105720   06        12    SunOS 5.6: /kernel/fs/nfs patch
105736   01    CURRENT   OBSOLETED by 105395
105755   03        08    SunOS 5.6: libresolv, in.named, named-xfer, nslookup, nstest patch
105786   04        13    SunOS 5.6: /kernel/drv/ip patch
105795   05        08    SunOS 5.6: /kernel/drv/hme patch
105800   05        06    SunOS 5.6: /usr/bin/admintool, y2000 patch
105802   07        12    OpenWindows 3.6: ToolTalk patch
105837   02        03    CDE 1.2: dtappgather Patch, including SDE 1.0 installations
105845   01    CURRENT   OBSOLETED by 105621
105926   01    CURRENT   SunOS 5.6: /usr/sbin/static/tar patch
106033   01    CURRENT   OBSOLETED by 105621
106049   01    CURRENT   SunOS 5.6: /usr/sbin/in.telnetd patch
106112   02        06    CDE 1.2: dtfile patch
106125   05        10    SunOS 5.6: Patch for patchadd and patchrm
106222   01    CURRENT   OpenWindows 3.6: filemgr (ff.core) fixes
106235   02        06    SunOS 5.6: lp patch
106301   01    CURRENT   SunOS 5.6: /usr/sbin/in.ftpd patch
106448   01    CURRENT   SunOS 5.6: /usr/sbin/ping patch
106522   01        04    SunOS 5.6: /usr/bin/ftp patch
106569   01    CURRENT   SunOS 5.6: libauth.a & libauth.so.1 patch
```

```
106648    01     CURRENT  OpenWindows 3.6: libce suid/sgid security fix
106649    01     CURRENT  OpenWindows 3.6: libdeskset patch
106650    03       04     OpenWindows 3.6: mailtool attachment security patch
==========================================================================

UNINSTALLED RECOMMENDED PATCHES

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev       ID         ID
------ --- --- --- --------- -------- ----------------------------------
105395 N/A  06 420                     SunOS 5.6: /usr/lib/sendmail patch
105403 N/A  03 116                     SunOS 5.6: ypbind/ypserv patch
105472 N/A  07 579                     SunOS 5.6: /usr/lib/autofs/automountd patch
105529 N/A  09  53                     SunOS 5.6: /kernel/drv/tcp patch
105552 N/A  03 116                     SunOS 5.6: /usr/sbin/rpc.nisd_resolv patch
105562 N/A  03 769                     SunOS 5.6: chkey and keylogin patch
105568 N/A  18  39 105210-27           SunOS 5.6: /usr/lib/libthread.so.1 patch
105580 N/A  15  78                     SunOS 5.6: /kernel/drv/glm patch
105600 N/A  19  47 105181-05           SunOS 5.6: /kernel/drv/isp patch
105642 N/A  08 118                     SunOS 5.6: prtdiag patch
105722 N/A  05  76                     SunOS 5.6: /usr/lib/fs/ufs/ufsdump and ufsrestore patch
105741 N/A  07 139                     SunOS 5.6: /kernel/drv/ecpp patch
105780 N/A  05  75                     SunOS 5.6: /kernel/fs/fifofs patch
106040 N/A  13 267                     SunOS 5.6: X Input & Output Method patch
106123 N/A  04 582                     SunOS 5.6: sgml patch
106172 N/A  04 631 105181-05           SunOS 5.6: /kernel/drv/fas patch
106193 N/A  05  48                     SunOS 5.6: y2000 sysid unzip patch
106226 N/A  01 798                     SunOS 5.6: /usr/sbin/format patch
106257 N/A  05 187                     SunOS 5.6: /usr/lib/libpam.so.1 patch
106271 N/A  06 319                     SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
106439 N/A  06 153                     SunOS 5.6: /usr/sbin/syslogd patch
106468 N/A  02 131                     SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
106495 N/A  01 777                     SunOS 5.6: truss & truss support library patch
106592 N/A  03 116                     SunOS 5.6: /usr/lib/nfs/statd patch
106625 N/A  08  42                     SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/ufs patch
106639 N/A  05  42                     SunOS 5.6: /kernel/strmod/rpcmod patch
106828 N/A  01 649                     SunOS 5.6: /usr/bin/date patch
106834 N/A  01 565                     SunOS 5.6: cp/ln/mv patch
106894 N/A  01 582                     SunOS 5.6: /usr/bin/uux patch
107565 N/A  02 298                     SunOS 5.6: /usr/sbin/in.tftpd patch
107618 N/A  01 273                     SunOS 5.6: Permissions problem in /vol.
107733 N/A  08  75                     SunOS 5.6: Linker patch
107758 N/A  01 440                     SunOS 5.6: Pax incorrectly change mode of symlink target file
107766 N/A  01 365                     SunOS 5.6: ASET cklist reports unchanged 6month older files as new
107774 N/A  01 427                     SunOS 5.6: inetd denial-of-service attack
107991 N/A  01 410                     SunOS 5.6: /usr/sbin/static/rcp patch
108307 N/A  02 116                     SunOS 5.6: keyserv fixes
108346 N/A  03 116                     SunOS 5.6: patch usr/sbin/rpc.nispasswdd
108468 N/A  02  75                     SunOS 5.6: ldterm streams module fixes
108492 N/A  01 245                     SunOS 5.6: Snoop may be exploited to gain root access
108499 N/A  01 197                     SunOS 5.6: ASET sets the gid on /tmp, /var/tmp when setting med hi
108660 N/A  01 228                     SunOS 5.6: Patch for sadmind
108804 N/A  01  64                     SunOS 5.6: tip has buffer overrun with security implications
108890 N/A  01 116                     SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
108893 N/A  01 116                     SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
108895 N/A  01 116                     SunOS 5.6: patch /usr/sbin/rpc.bootparamd
109266 N/A  01  91                     SunOS 5.6: security: /bin/mail has buffer overflow
109339 N/A  01  75                     SunOS 5.6: nscd has a potential security problem
109388 N/A  01  67                     SunOS 5.6: patch /usr/vmsys/bin/chkperm
105566 N/A  08 168                     CDE 1.2: calendar manager patch
106027 N/A  08 176 106125-08           CDE 1.2: SDE 1.0: dtsession patch
106242 N/A  02 580                     CDE 1.2: libDtHelp.so.1 fixes
106437 N/A  03 189 105669-06           CDE 1.2: Print Manager Patch
107434 N/A  01 491                     CDE 1.2: Spell checking occasionally kills mail
108199 N/A  01 330                     CDE 1.2: dtspcd Patch
108201 N/A  01 330                     CDE 1.2: dtaction Patch
105633 N/A  41  76                     OpenWindows 3.6: Xsun patch
106415 N/A  03 462                     OpenWindows 3.6: xdm patch
107336 N/A  01 508                     OpenWindows 3.6: KCMS configure tool has a security vulnerability
==========================================================================
```

UNINSTALLED SECURITY PATCHES - **VULNERABILITY**

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

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
105395	N/A	06	420			SunOS 5.6: /usr/lib/sendmail patch
105403	N/A	03	116			SunOS 5.6: ypbind/ypserv patch
105529	N/A	09	53			SunOS 5.6: /kernel/drv/tcp patch
105552	N/A	03	116			SunOS 5.6: /usr/sbin/rpc.nisd_resolv patch
105562	N/A	03	769			SunOS 5.6: chkey and keylogin patch
105722	N/A	05	76			SunOS 5.6: /usr/lib/fs/ufs/ufsdump and ufsrestore patch
105780	N/A	05	75			SunOS 5.6: /kernel/fs/fifofs patch
106123	N/A	04	582			SunOS 5.6: sgml patch
106193	N/A	05	48			SunOS 5.6: y2000 sysid unzip patch
106257	N/A	05	187			SunOS 5.6: /usr/lib/libpam.so.1 patch
106271	N/A	06	319			SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
106468	N/A	02	131			SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
106592	N/A	03	116			SunOS 5.6: /usr/lib/nfs/statd patch
106625	N/A	08	42			SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/ufs patch
106639	N/A	05	42			SunOS 5.6: /kernel/strmod/rpcmod patch
106834	N/A	01	565			SunOS 5.6: cp/ln/mv patch
106894	N/A	01	582			SunOS 5.6: /usr/bin/uux patch
107565	N/A	02	298			SunOS 5.6: /usr/sbin/in.tftpd patch
107618	N/A	01	273			SunOS 5.6: Permissions problem in /vol.
107733	N/A	08	75			SunOS 5.6: Linker patch
107758	N/A	01	440			SunOS 5.6: Pax incorrectly change mode of symlink target file
107766	N/A	01	365			SunOS 5.6: ASET cklist reports unchanged 6month older files as new
107774	N/A	01	427			SunOS 5.6: inetd denial-of-service attack
107991	N/A	01	410			SunOS 5.6: /usr/sbin/static/rcp patch
108307	N/A	02	116			SunOS 5.6: keyserv fixes
108346	N/A	03	116			SunOS 5.6: patch usr/sbin/rpc.nispasswdd
108468	N/A	02	75			SunOS 5.6: ldterm streams module fixes
108492	N/A	01	245			SunOS 5.6: Snoop may be exploited to gain root access
108499	N/A	01	197			SunOS 5.6: ASET sets the gid on /tmp, /var/tmp when setting med hi
108660	N/A	01	228			SunOS 5.6: Patch for sadmind
108804	N/A	01	64			SunOS 5.6: tip has buffer overrun with security implications
108890	N/A	01	116			SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
108893	N/A	01	116			SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
108895	N/A	01	116			SunOS 5.6: patch /usr/sbin/rpc.bootparamd
109266	N/A	01	91			SunOS 5.6: security: /bin/mail has buffer overflow
109339	N/A	01	75			SunOS 5.6: nscd has a potential security problem
109388	N/A	01	67			SunOS 5.6: patch /usr/vmsys/bin/chkperm
105566	N/A	08	168			CDE 1.2: calendar manager patch
106027	N/A	08	176	106125-08		CDE 1.2: SDE 1.0: dtsession patch
106437	N/A	03	189	105669-06		CDE 1.2: Print Manager Patch
108199	N/A	01	330			CDE 1.2: dtspcd Patch
108201	N/A	01	330			CDE 1.2: dtaction Patch
105633	N/A	41	76			OpenWindows 3.6: Xsun patch
106415	N/A	03	462			OpenWindows 3.6: xdm patch
107336	N/A	01	508			OpenWindows 3.6: KCMS configure tool has a security vulnerability

UNINSTALLED Y2K PATCHES

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

Patch ID	Ins Rev	Lat Rev	Age	Require ID	Incomp ID	Synopsis
106193	N/A	05	48			SunOS 5.6: y2000 sysid unzip patch
106828	N/A	01	649			SunOS 5.6: /usr/bin/date patch
107492	N/A	01	491			SunOS 5.6: Y2000, runacct cannot update /var/adm/acct/sum/loginlog
107988	N/A	01	284			SunOS 5.6: Patch for SPARCompiler Binary Compatibility Libraries
105566	N/A	08	168			CDE 1.2: calendar manager patch
108667	N/A	03	181			CDE 1.2: perfmeter is not Y2K compliant in SunOS 5.6 Supplement
108671	N/A	03	28			OpenWindows 3.6: Calendar Manager patch

APPENDIX B

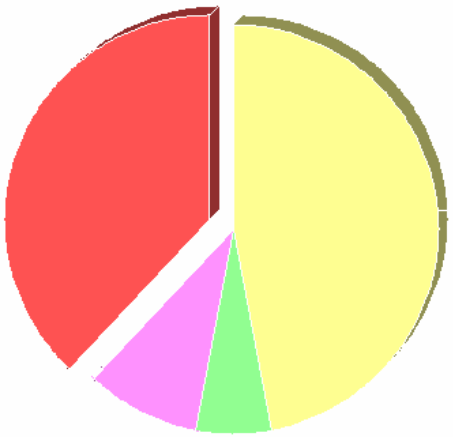
COPS Report:

ATTENTION:
Security Report for Fri Aug 11 14:33:03 EDT 2000
from host *****

**** root.chk ****
**** dev.chk ****
**** is_able.chk ****
Warning! /etc/security is _World_ readable! - **VULNERABILITY**
Warning! /etc/driver_aliases is _World_ writable! - **VULNERABILITY**
Warning! /etc/driver_classes is _World_ writable! - **VULNERABILITY**
Warning! /etc/group.dirty is _World_ writable! - **VULNERABILITY**
Warning! /etc/minor_perm is _World_ writable! - **VULNERABILITY**
Warning! /etc/name_to_major is _World_ writable! - **VULNERABILITY**
Warning! /etc/netgroup is _World_ writable! - **VULNERABILITY**
Warning! /etc/netgroup~ is _World_ writable! - **VULNERABILITY**
Warning! /etc/passwd.dirty is _World_ writable! - **VULNERABILITY**
Warning! /etc/rem_name_to_major is _World_ writable! - **VULNERABILITY**
Warning! /etc/rmtab is _World_ writable! - **VULNERABILITY**
Warning! /etc/shadow.dirty is _World_ writable! - **VULNERABILITY**
Warning! /etc/ski is _World_ writable! - **VULNERABILITY**
Warning! /etc/smb.conf is _World_ writable! - **VULNERABILITY**
Warning! /usr/adm/spellhist is _World_ writable! - **VULNERABILITY**
Warning! /usr/adm/vold.log is _World_ writable! - **VULNERABILITY**
**** rc.chk ****
Warning! File /etc/rem_name_to_major (in /etc/rc2.d/S05RMTMPFILES) is _World_ writable! - **VULNERABILITY**
**** cron.chk ****
**** group.chk ****
**** home.chk ****
Warning! User nuucp's home directory /var/spool/uucppublic is mode 01777! - **VULNERABILITY**
Warning! User nuucp's home directory /var/spool/uucppublic is mode 01777! - **VULNERABILITY**
Warning! User jatkins's home directory /home/cs/jatkins is mode 0777! - **VULNERABILITY**
**** passwd.chk ****
Warning! Duplicate uid(s) found in /etc/passwd:
adm
Warning! Password file, line 7, user smtp has uid = 0 and is not root
smtp:x:0:0:Mail Daemon User:/:
**** user.chk ****
Warning! User qtu: /home/stat391/qtu/.cshrc is mode 0777! - **VULNERABILITY**
**** misc.chk ****
**** ftp.chk ****
Warning! /etc/ftpusers should exist! - **VULNERABILITY**
**** pass.chk ****
**** kuang ****
**** bug.chk ****
Warning! /usr/lib/sendmail could have a hole/bug! (CA-88:01)
Warning! /usr/lib/sendmail could have a hole/bug! (CA-90:01)
Warning! /bin/mail could have a hole/bug! (CA-91:01a)

APPENDIX C

Nessus – Network Vulnerability Scan Report:
List of open ports :



* ftp (21/tcp) (Security notes found)
* ssh (22/tcp) (Security warnings found)
* telnet (23/tcp) (Security warnings found)
* smtp (25/tcp) (Security hole found)
* time (37/tcp)
* www (80/tcp) (Security notes found)
* pop-3 (110/tcp) (Security notes found)
* sunrpc (111/tcp)
* netbios-ssn (139/tcp)
* imap2 (143/tcp)
* printer (515/tcp)
* webster (765/tcp)
* unknown (2049/tcp) (Security warnings found)
* unknown (4045/tcp)
* unknown (6000/tcp)
* unknown (7777/tcp) (Security warnings found)
* unknown (7937/tcp)
* unknown (8007/tcp)
* unknown (8888/tcp) (Security warnings found)
* general/tcp (Security notes found)
* netbios-ns (137/udp) (Security warnings found)
* general/udp (Security notes found)
* snmp (161/udp) (Security hole found)
* unknown (32781/tcp) (Security warnings found)
* unknown (32788/udp) (Security hole found)
* unknown (43317/udp) (Security hole found)
* unknown (43318/udp) (Security warnings found)
* unknown (4045/udp) (Security warnings found)
* unknown (2049/udp) (Security warnings found)
* unknown (43319/udp) (Security hole found)
* unknown (764/udp) (Security warnings found)
* general/icmp (Security warnings found)

Information found on port ftp (21/tcp)

Remote FTP server banner :
***** ftp server (sunos 5.6) ready.

Warning found on port ssh (22/tcp)

You are running a version of SSH which is
older than (or as old as) version 1.2.27.
If this version was compiled against the
RSAREF library, then it is very likely to
be vulnerable to a buffer overflow which
may be exploited by a cracker to gain
root on your system.

To determine if you compiled ssh against
the RSAREF library, type 'ssh -V' on the

remote host.

Risk factor : High
Solution : Use ssh 2.x, or do not compile ssh
against the RSAREF library
CVE : CVE-1999-0834

Warning found on port ssh (22/tcp)

You are running a version of SSH which is
older than (or as old as) version 1.2.27.

If you compiled ssh with kerberos support,
then an attacker may eavesdrop your users
kerberos tickets, as sshd will set
the environment variable KRB5CCNAME to
'none', so kerberos tickets will be stored
in the current working directory of the
user, as 'none'.

If you have nfs/smb shared disks, then an attacker
may eavesdrop the kerberos tickets of your
users using this flaw.

** If you are not using kerberos, then
ignore this warning.

Risk factor : Serious
Solution : use ssh 1.2.28 or newer
CVE : CAN-2000-0575

Information found on port ssh (22/tcp)

Remote SSH version : ssh-1.5-1.2.22

Warning found on port telnet (23/tcp)

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 found on port telnet (23/tcp)

Remote telnet banner :
SunOS 5.6

Vulnerability found on port smtp (25/tcp)

The remote SMTP server did not complain when issued the command :
MAIL FROM: |testing

This probably means that it is possible to send mail
that will be bounced to a program, which is
a serious threat, since this allows anyone to execute
arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since
some MTAs will not complain to this test, but instead
just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0203

Warning found on port smtp (25/tcp)

The remote SMTP server
answers to the EXPN and/or VRFY commands.

The EXPN command can be used to find
the delivery adress of mail aliases, or
even the full name of the recipients, and
the VRFY command may be used to check the
validity of an account.

Your mailer should not allow remote users to
use any of these commands, because it gives
them too much informations.

Solution : if you are using sendmail, add the
option
O PrivacyOptions=goaway
in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

Warning found on port smtp (25/tcp)

The remote STMP server seems to allow remote users to
send mail anonymously by providing a too long argument
to the HELO command (more than 1024 chars).

This problem may allow bad guys to send hate
mail, or threatening mail using your server
and keep their anonymity.

Risk factor : Low.

Solution : If you are using sendmail, upgrade to
version 8.9.x. If you do not run sendmail, contact
your vendor.
CVE : CAN-1999-0098

Warning found on port smtp (25/tcp)

The remote SMTP server is vulnerable to a redirection
attack. That is, if a mail is sent to :

user@hostname1@victim

Then the remote SMTP server (victim) will happily send the
mail to :
user@hostname1

Using this flaw, an attacker may route a message
through your firewall, in order to exploit other
SMTP servers that can not be reached from the
outside.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
SOME SMTP SERVERS LIKE POSTFIX WILL NOT
COMPLAIN BUT DROP THIS MESSAGE ***

Solution : if you are using sendmail, then at the top
of ruleset 98, in /etc/sendmail.cf, insert :
R$*@$*@$* $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

Risk factor : Low

Warning found on port smtp (25/tcp)

The remote SMTP server allows the relaying. This means that
it allows spammers to use your mail server to send their mails to
the world, thus wasting your network bandwidth.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a relay
any more.

CVE : CAN-1999-0512

Information found on port smtp (25/tcp)

Remote SMTP server banner :
stat.wvu.edu Sendmail SMI-8.6/SMI-SVR4 ready at Mon, 14 Aug 2000 13:07:18 -0400
214-Commands:214- HELO MAIL RCPT DATA RSET

214- NOOP QUIT HELP VRFY EXPN

214-For more info use "HELP <topic>".

214-smtp

214-To report bugs in the implementation contact Sun Microsystems

214-Technical Support.

214-For local information contact postmaster at this site.

214 End of HELP info

Information found on port www (80/tcp)

The remote web server type is :
Apache/1.3.9 (Unix) ApacheJServ/1.0

We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

Information found on port pop-3 (110/tcp)

The remote POP server banner is : POP3 ***** v7.59 server ready

Warning found on port unknown (2049/tcp)

Here is the export list of ***** :
/ext01/sharehost,host,host,
/ext01/mail host,host,host,
/ext01/home host,host,host,

CVE : CVE-1999-0554

Warning found on port unknown (7777/tcp)

a ssh server is running on this port

Warning found on port unknown (7777/tcp)

You are running a version of SSH which is
older than (or as old as) version 1.2.27.
If this version was compiled against the
RSAREF library, then it is very likely to
be vulnerable to a buffer overflow which
may be exploited by a cracker to gain
root on your system.

To determine if you compiled ssh against
the RSAREF library, type 'ssh -V' on the
remote host.

Risk factor : High
Solution : Use ssh 2.x, or do not compile ssh
against the RSAREF library
CVE : CVE-1999-0834

Warning found on port unknown (7777/tcp)

You are running a version of SSH which is
older than (or as old as) version 1.2.27.

If you compiled ssh with kerberos support,
then an attacker may eavesdrop your users
kerberos tickets, as sshd will set
the environment variable KRB5CCNAME to
'none', so kerberos tickets will be stored
in the current working directory of the
user, as 'none'.

If you have nfs/smb shared disks, then an attacker
may eavesdrop the kerberos tickets of your
users using this flaw.

** If you are not using kerberos, then
ignore this warning.

Risk factor : Serious
Solution : use ssh 1.2.28 or newer
CVE : CAN-2000-0575

Information found on port unknown (7777/tcp)

Remote SSH version : ssh-1.5-1.2.22

Warning found on port unknown (8888/tcp)

a web server is running on this port

Information found on port general/tcp

Nmap found that this host is running Solaris 2.6 - 2.7, Solaris 7

Warning found on port netbios-ns (137/udp)

. The following 7 NetBIOS names have been gathered :
*****
*****
*****
*****
*****
*****
*****

. This SMB server seems to be a SAMBA server (this is not a security risk, this is for your information). This can be told because this server claims to have a null MAC address

If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port.

Risk factor : Medium

Information found on port general/udp

For your information, here is the traceroute to ***** :
*****

Vulnerability found on port snmp (161/udp)

SNMP Agent responded as expected with community name: public
CVE : CAN-1999-0517

Vulnerability found on port snmp (161/udp)

SNMP Agent responded as expected with community name: private
CVE : CAN-1999-0517

Warning found on port unknown (32781/tcp)

The tooltalk RPC service is running.
An possible implementation fault in the

ToolTalk object database server may allow a
cracker to execute arbitrary commands as
root.

** This warning may be a false
positive since the presence
of the bug was not tested **

Solution : Disable this service.
See also : CERT Advisory CA-98.11

Risk factor : High
CVE : CVE-1999-0003

Vulnerability found on port unknown (32788/udp)

The statd RPC service is running.
This service has a long history of
security holes, so you should really
know what you are doing if you decide
to let it run.

* NO SECURITY HOLE REGARDING THIS
PROGRAM HAVE BEEN TESTED, SO
THIS MIGHT BE A FALSE POSITIVE *

We suggest you to disable this
service.

Risk factor : High
CVE : CVE-1999-0018

Vulnerability found on port unknown (43317/udp)

The sadmin RPC service is running.
There is a bug in Solaris versions of
this service that allow an intruder to
execute arbitrary commands on your system.

Solution : disable this service
Risk factor : High

Warning found on port unknown (43318/udp)

The rquotad RPC service is running.
If you do not use this service, then
disable it as it may become a security
threat in the future, if a vulnerability
is discovered.

Risk factor : Low
CVE : CAN-1999-0625

Warning found on port unknown (4045/udp)

The nlockmgr RPC service is running.
If you do not use this service, then
disable it as it may become a security
threat in the future, if a vulnerability
is discovered.

Risk factor : Low
CVE : CAN-2000-0508

Warning found on port unknown (2049/udp)

The nfsd RPC service is running.
There is a bug in older versions of
this service that allow an intruder to
execute arbitrary commands on your system.

Make sure that you have the latest version
of nfsd

Risk factor : High
CVE : CAN-1999-0832

Vulnerability found on port unknown (43319/udp)

The cmsd RPC service is running.
This service has a long history of
security holes, so you should really
know what you are doing if you decide
to let it run.

* NO SECURITY HOLE REGARDING THIS
PROGRAM HAS BEEN TESTED, SO
THIS MIGHT BE A FALSE POSITIVE *

We suggest you to disable this
service.

Risk factor : High
CVE : CVE-1999-0320

Warning found on port unknown (764/udp)

The remote host is a NIS server.
NIS is used to share password files among
the hosts of a given network, which
must not be intercepted by crackers.

Usually, the first step of their attack
is to determine whether they are attacking
a NIS server, which make the host a more
valuable target.

Since we could determine that the remote host

is a NIS server, they can determine too,
which is not a good thing.

Solution : filter incoming UDP traffic to
prevent them from connecting to the portmapper
and to the NIS server.

Risk factor : Low
CVE : CAN-1999-0620

Warning found on port general/icmp

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 found on port general/icmp

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

This file was generated by Nessus, the open-sourced security scanner.

References

Sun's Patchdiag Tool. URL: http://sunsolve.Sun.COM (August 2000).

Matt Bishop. Unix Security Tools and Their Uses. Sans Security DC 2000. (July 2000).

SSH 1.2.22 Vulnerability – buffer overflow http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D797 (Noverber 1999).

Dan Farmer. COPS – System configuration checker. ftp://coast.cs.purdue.edu/pub/tools/unix/cops/cops.1.04.tar.gz. (August 2000).

Jean Chouanard. YASSP. Yet Another Solaris Security Package. http://yassp.parc.xerox.com/. (July 2000).

Renaud Deraison. Nessus network vulnerability scanner. http://www.nessus.org/ (August 2000).

Casper Dik. Fix-modes script. http://www.ja.net/CERT/Software/fix-modes/fix-modes (March 1998).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
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**