Hardening Solaris

Compass Security

Draft 0.86

November 4, 2000

Document name:	Hardening_Solaris_V0.86
Version:	V 0.86
Author:	Ivan Buetler, Compass Security AG ivan.buetler@csnc.ch http://www.csnc.ch/
References:	a couple of other hardening doc / experience
Date of delivery:	November 4, 2000
Document state:	PUBLIC

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

CONTENT

Date: Nov 5, 2000

1 Hardening Solaris

1.1 Introduction

This document describes how to harden a Solaris box in order to gain more security according to the

- network security
- local security

aspect.

This document is still a draft and Compass is working on it.

1.2 Related documents

This document references to other documents. Especially:

- how to install tripwire
- how to install arpwatch
- how to install swatch
- how to install ssh2
- how to install npasswd

These documents are also in a draft status. Be aware of 3 levels of security (Application Security / Network Security / Local Security) A description of this definition will be documented in chapter 1.6. Pls. read these sections in order to fully understand the recommendations in this document.

1.3 Monitoring / Alarming and Alerting

Alarming and alerting is very need but also specific for your company. The tools described above might help you to monitor your systems and activities. But how do you want proceed by a pattern match. What actions do you want to define?

1.4 Version control

Version	Author	Description	Filename
0.82	Ivan Bütler ivan.buetler@csnc.ch	Initial version saved on http://www.csnc.ch/download	Hardening Solaris V0.82.pdf
0.83	Sven Scherler sven.scherler@crysec.com	Review of the first official Internet version 0.82. http://www.crysec.com	Hardening_Solaris_V0.83.pdf
0.86	Phil Waterbury pwaterbury@att.com	Input about reference of titan	Hardening_Solaris_V0.86.pdf

[Ivan] I would like to improve the checklist as well. But as you know---time is the problem. If you feel like having something you would like to see in this document, pls. let me know. I will leave the version control chapter in the future. So everybody can see who did what on this document.

[Ivan] The permission settings (I have experience with) will be included into the next version.

1.5 Hardening Solaris steps

H = Hardening

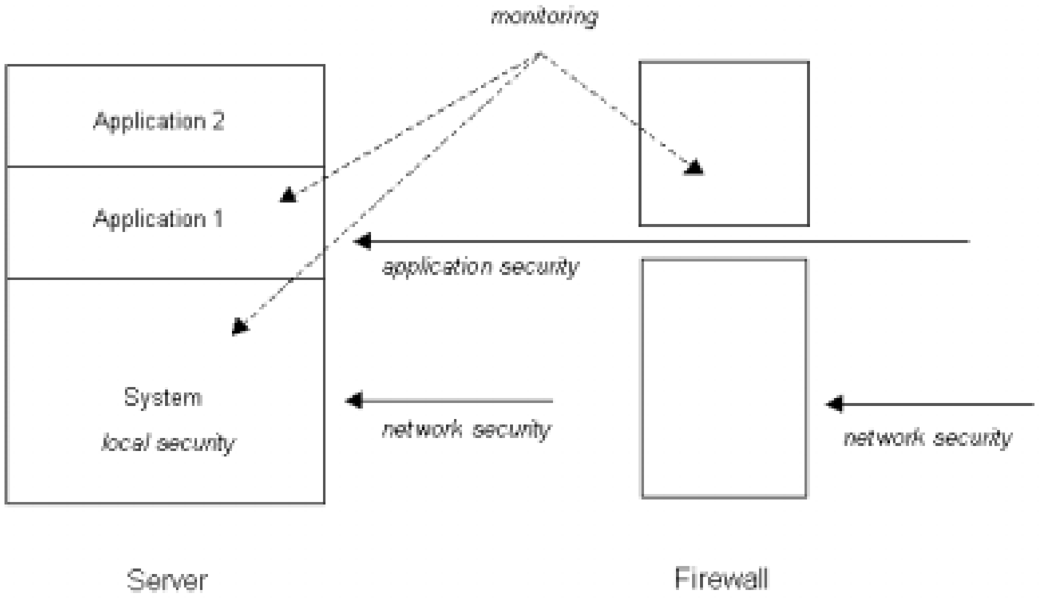
Sometimes a tool within the titan distribution does an automated hardening for you. If there is an existing tool or script, which does the hardening, you will find it in the reference row. This draft has a major lack according the permission recommendations. The final hardening document will also include these steps. 8-)

1.6 Local - Network - Application Security

Compass defined 3 levels of hardening tasks

local security hardening	[threat to local exploits]
network security hardening	[threat to LISTEN services - remote exploits]
application security hardening	[threat to application]
monitoring tasks	[attack detection / alarming and alerting]

All LISTEN services not used for the application (e.g. telnet) is discussed as network security aspect.



Hardening an application can be:

- Limiting user rights
- Limiting rights of process owner
- Checking file permissions of application specific files
- Restricting access to other system resources

If an application is exploiteable, the attacker should find a very unfriendly environment. That means it should be difficult for him to break the system or to attack other systems.

Hardening on network security level means:

- Use secure protocols for administration
- Disable unused network services
- Disable trust relations to other systems
- Disable unused accounts
- Enforce strong passwords
- Disable dangerous network services
- Restrict access to the required systems, persons

Hardening on local security level means:

- Restrict access to powerful commands
- Set correct file permissions
- Apply group and user concept
- Disable unused services

2 Tasklist

2.1 How to read the table

No.	Description	How to fix	H		Reference
number	short brief description of the problem	discussion how to fix the problem	Local	Network	what script might automate this task

2.2 Installation

	UPDATES		L	H	
1000	Apply latest patches	Check http://sunsolve.sun.com for the latest Solaris patches available showrev -p [list of installed patches]	X		to do by hand
1001	create /var partition	/var is the logfile partition. Protect yourself from logfile-spamming so the root partition won't be filled up with rubbish. You have to do the /var 1) At initial installation time 2) Insert special (small) disk and mount it to /var	X		to be done by hand

2.3 System

	SYSTEM		L	H	
1010	eeprom security	"eeprom security-mode=command". The system will change the security level to command and ask you to set a password. Enter a password. Every time the System is booted with Arguments it will prompt for a Password. For normal use (boot from disk), the password is not required. But if someone wants to boot from the CD-ROM, the password is needed. This should prevent you from attackers with physical access to the machine.	X		To be done by hand. Pls. try it out on the ok prompt after change.
1011	Set core size to zero	<u>Add the following line to the /etc/system file:</u> set sys:coredumpsize = 0 Compass recommends setting a coresize after you have multiple panics on your Solaris system. In such a case the vendor needs the core for analyses. The coresize setting to 0 prevents you from smashing your disk.	X		disable-core.sh [titan module]
1012	Fix some stack errors [only for Solaris 2.6]	<u>Add the following lines into /etc/system:</u> set noexec_user_stack = 1 set noexec_user_stack_log = 1 Change file permission on /etc/passwd: chmod 644 /etc/system Adds the following entry into /etc/system to force all users zero-fill-on-demand pages are marked rw- instead of rwx on the stack. This prevents attackers to executing code	X		fix-stack.sol2.6.sh [titan module]

	SYSTEM		L	H	
		on the stack and logs it when it happens.			
1013	Allow Power Management only to be run by root [only on Solaris 2.6 and newer]	Edit in the file /etc/default/sys-suspend the follow line: Before: PERMS=console-owner after: PERMS=- and does: “/bin/chmod 0755 /usr/openwin/bin/sys-suspend”	X		powerd.sh [titan module]
1014	Set the sticky bit for the /tmp directory at boot time to mode 1777	Create a file /etc/rc3.d/S79tmpfix file: /bin/cat << EOF >/etc/rc3.d/S79tmpfix #!/bin/sh #ident "@(#)tmpfix 1.0 95/09/14" if [-d /tmp] then /usr/bin/chmod g-s /tmp /usr/bin/chmod 1777 /tmp /usr/bin/chgrp sys /tmp /usr/bin/chown sys /tmp fi EOF Change permission on S79tmpfix: /usr/bin/chmod 755 /etc/rc3.d/S79tmpfix	X		psfix.sh [titan module]

	SYSTEM		L	H	
1015	Disable Keystroke stop-'A' [only on Solaris 2.6 and newer]	Change or add "KEYBOARD_ABORT=disable" into /etc/default/kbd. It will affect after reboot. This will prevent L1-A or Stop-A keyboard sequence. This might protects you from attacker with physical access to the machine-room. We assume this persion has its own hacker-cdrom with him. How can he/she boot from this device? He must do a "boot cdrom" from the OK-prompt. But if the stop-A sequence is disabled, the attacker can't gain the OK-prompt. (But he/she can still carry out the machine at home or remove the disks from the devices if we assume he/she has physical access.)	X		disable-L1-A.sh [titan module]

2.4 User Management

	USER MANAGEMENT		L	H	
1020	Disable all system accounts	Edit /etc/passwd so that all System Users don't have a shell. Example: noaccess:x:60002:60002:No Access User:/:/sbin/noshell cd $TITAN_HOME/src1 gcc -o ./noshell ./noshell.c cp /sbin/noshell /sbin/noshell.solaris cp $TITAN_HOME/src1/noshell /sbin/noshell Disable unnecessary accounts in the /etc/shadow. To do this put NP on the Password files for those users. This will disable those accounts A basic listing for SysV Unix: bin, daemon, adm, lp, smtp, sys, uucp, nuucp, nobody, noaccess	X		to be done by hand to do by hand

	USER MANAGEMENT		L	H	
		PS: Compass recommends compiling the nosell.c from the TITAN distribution in order to use as the noshell binary. On hostabc and hostdef the /sbin/noshell is already compiled and there. The /sbin/noshell.solaris is the original noshell script. You can find the noshell.c in $TITAN_HOME/src1 directory.			
1021	usage of strong password library	Compass recommends the usage of a strong password forcer. Under Solaris the tool npasswd will work and compile perfectly. Npasswd will change the passwd libraries and has an extended config-file where you can define pw-length, aging, min-characters, and dictionaries. etc. You can find a special documentation in how to install and configure npasswd in “Installation npasswd”.		X	see Installation npasswd documentation
1022	Set default password parameters	Add or edit /etc/default/passwd to match the following entries: PWMIN=1 # Minimum time period before the password can be changed. [only if you want to work with standard passwd functionality - without npasswd]	X		defpwparams.sh [titan module]
1023	Set the Maximum valid time period for passwords	Add or edit /etc/default/passwd to match the following entry: PWMAX=13 # Maximum time period that password is valid [only if you want to work with standard passwd functionality - without npasswd]	X		defpwparams.sh [titan module]
1024	Set the time period where the system is starting to warn password expiration	Add or edit /etc/default/passwd to match the following entry: PWWARN=4 # The number of days relative to MAX before the password expires to # start warning the user of the required change	X		defpwparams.sh [titan module]

	USER MANAGEMENT		L	H	
		[only if you want to work with standard passwd functionality - without npasswd]			
1025	Set the minimum password length	Add or edit /etc/default/passwd to match the following entry: PWLEN=8 # the following requires that all passwords must have min. length of 8 [only if you want to work with standard passwd functionality - without npasswd]	X		defpwparams.sh (Titan sets PWLEN=6) [titan module]
1026	Prevent root to login from remote	Add or edit /etc/default/login to match the following entry: LCONSOLE=/dev/console # If CONSOLE is set, root can only login on that device.	X		defloginparams.sh [titan module]

1027	Log all root login attempts	Add or edit /etc/default/login to match the following entry:
		# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
		# to log all root logins at level LOG_NOTICE and multiple failed login
		# attempts at LOG_C
		LSYSLOG=YES
			X		defloginparams.sh
					[titan module]

1028	Set a timeout for a session	Add or edit /etc/default/login to match the following entry:
		# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
		# abandoning a login session.
		LTIMEOUT=120
			X		defloginparams.sh
					[titan module]

1029	Set a default UMASK	Add or edit /etc/default/login to match the following entry:
		# UMASK sets the initial shell file creation mode mask. See umask(1).
		LUMASK=027
		This will set a standard mask of 750. “rwx-rw------“
			X		defloginparams.sh
					userumask.sh
					[titan module]

	USER MANAGEMENT		L	H	
		Apply this to the following files: /etc/.login /etc/profile /etc/skel/local.cshrc /etc/skel/local.login /etc/skel/local.profile			
1030	Set UMASK for root	Assure root has a umask of 027 or 077 Check .profile of root	X		to do by hand

1031	Assure password prompt for login	Add or edit /etc/default/login to match the following entry:
		
		# PASSREQ determines if login requires a password.
		LPASSREQ=YES
			X		defloginparams.sh
					
					[titan module]

1032	Set the SHELL environment variable	Add or edit /etc/default/login to match the following entry:
		
		# ALTSHELL determines if the SHELL environment variable should be set
		LALTSHELL=YES
			X		defloginparams.sh
					
					[titan module]

1033	Check whether every user has a password set	Check that every user has a password set in /etc/passwd or /etc/shadow user:lRs.8R9EfQXx.:11137:0:10000:::: The encrypted Password is between the second and third ":"	X		passwd.sh (check only, no fix) [titan module]
1034	Edit useradd defaults to match your password policy	Edit /usr/sadm/defadduser according to your password policy Example: defgroup=15 defgname=users defparent=/export/home defskel=/etc/skel defshell=/usr/bin/ksh definact=30	X		useraddset.sh [titan module]

	USER MANAGEMENT		L	H	
		defexpire=			
1035	Remove all “.” in search path variables.	Remove all “.” of search path variables of default startup scripts and root startup scripts. /.login /etc/.login /etc/default/login /.cshrc /etc/skel/local.cshrc /etc/skel/local.login /etc/skel/local.profile /.profile /etc/profile	X		rootchk.sh [titan module]
1036	restrict su to the sugroup and add your users to this group	create special group in /etc/group apply your admin accounts to this group (make they members) change permissions of /bin/su to have: r-sr-sr-x 1 root sugroup chmod 550 /bin/su chmod +s /bin/su chown root:sugroup /bin/su ls -al /bin/su -r-sr-s--- 1 root sugroup 18360 Jan 15 1998 /bin/su grep sugroup /etc/group sugroup::600:root,httpadm,wsphere This means, that only the users of the sugroup are able to use the su command. There is no need for wasrun and wwwrun to be able to su.	X		to do by hand

2.5 Services started on request (inetd)

	INETD		L	H	
1040	Disable all inetd services	Comment all entries in /etc/inetd.conf. (grep –v “^#” /etc/inetd.conf to check services started by inetd) Do only use inetd-services if really needed and protect them by tcpd (tcpwrapper).		X	to do by hand
1041	Implement TCP Wrappers to inetd services.	Compile and then install tcpd into /usr/local/bin (see document “How to install TCP Wrappers for further details). Edit the services inetd.conf that have to be wrapped: ftp stream tcp nowait root /usr/local/bin/tcpd in.ftpd telnet stream tcp nowait root /usr/local/bin/tcpd in.telnetd (We recommend using Wrappers in case inetd services are started for maintenance reasons.) Compass wrote a little compilation and installation guide in order to make tcpwrapper up and running. This document is called “Installation tcpwrapper”. Check it out for your convenience.		X	to do by hand
1042	Secure inetd	Check hosts.allow and hosts.deny. Make sure you have in /etc/hosts.deny ALL:ALL and do open your services in: /etc/hosts.allow <service>:<source-ip>		X	to do by hand

	INETD		L	H	
1043	xinetd	Inetd (even with tcpwrapper) has no option to restrict inetd services from binding to specific interfaces. Xinetd has the ability to restrict specific inetd services to the interface you want. There is also a script to transform /etc/inetd.conf in /etc/xinetd.conf	X		to do by hand

2.6 Services started at boot-time (rc.X)

	rc.X		L	H	
1043	Disable all unused Services	This hardening task reflects to stop services started by the ordinary startup procedure. Rename not used services started in the rc.X directory. Example: mv /etc/rc3.d/S92volmgt /etc/rc2.d/not_usedS92volmgt These services should be disabled: (you have to decide for yourself 8-) snmpdx autofs (Automounter) volmgt (Volume Deamon) lpsched (LP print service) nscd (Name Service Cache Daemon) Sendmail keyserv (Keyserv Deamon is only used if NIS+ or NFS are installed, if used start with –d option so that the defaults "nobody" key is not allowed) Disable rpcbind if not used (Special purpose Servers like web servers, ftp servers, mail servers, etc can usually have rpc disabled.		X	to do by hand

	rc.X		L	H	
		The list might not adapt all needs and services. Please go through the rc.X directories and decide by yourself weather you want to start or disable these services.			
1044	Disable all DMI services	Disable all dmi services with: mv /etc/rc3.d/S??dmi /etc/rc3.d/D??dmi DMI Services started by /etc/init.d/init.dmi are: /usr/lib/dmi/dmispd /usr/lib/dmi/snmpXdmid /etc/dmi/ciagent/ciinvoke Sun Solstice Enterprise Tools. Nobody knows exactly what it does and it's therefore not truthworth.		X	dmi-2.6.sh [titan module]
1045	Disable mounting suid features as the default	Add following lines to /etc/rmmount.conf: mount hsfs -o nosuid mount ufs -o nosuid		X	rmmount.sh [titan module]
1046	Check all .rhosts file	The .rhosts file allows User or machines to log from remote without providing a password. This can be a major security issue if one of the remote hosts can be compromised. We recommend disallowing all .rhosts. PS: cluster software might needs .rhosts etc. be carefully with removing trusts in such an environment.		X	rhosts.sh [titan module]
1047	Disallow the use of rhosts authentication	modify the /etc/pam.conf file removing the line: rlogin auth sufficient /usr/lib/security/pam_rhosts_auth.so.1 and changing the rsh line to read:		X	pam-rhosts-2.6.sh [titan module]

	rc.X		L	H	
		rsh auth required /usr/lib/security/pam_unix.so.1			
1048	Checking Trust Relationship	Check that the file /etc/hosts.equiv is empty. For more information type: man hosts.equiv		X	hosts.equiv.sh (check only, no fix) [titan module]
1049	umask for startup files	create a S00umask to very rc.X directory to make sure, the process has this umask /etc/rc0.d/S00umask.sh /etc/rc1.d/S00umask.sh /etc/rc2.d/S00umask.sh /etc/rc3.d/S00umask.sh /etc/rcS.d/S00umask.sh /etc/init.d/umask		X	add-umask.sh [titan module]

2.7 Interface tuning and securing

	Network Tuning and Securing		L	H	
1049	Shorten the period of time the ARP cache maintains entries	Add the following lines to the inet startup script /etc/rc2.d/S??inet ndd -set /dev/arp arp_cleanup_interval 60000 /* 1 min (default is 5 min*/		X	adjust-arp-timers.sh [titan module]
1050	Shorten the time a specific entry is kept in the arp-table	Add the following lines to the inet startup script /etc/rc2.d/S??inet		X	adjust-arp-timers.sh

	Network Tuning and Securing		L	H	
		ndd -set /dev/ip ip_ire_flush_interval 60000 /* 1 min (default is 20 min*/			[titan module]
1051	Disable respond to echo Broadcast to prevent some specific ping crashes	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_respond_to_echo_broadcast 0 # default is 1		X	disable-ping-echo.sh [titan module]
1052	Disable source routing at boot time	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_forward_src_routed 0 # default is 1		X	disable_ip_holes.sh [titan module]
1053	Prevent System to forward ip packets at boot time	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_forwarding 0 # default is 1		X	disable_ip_holes.sh [titan module]
1054	Prevent system to forward directed broadcast packets	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_forward_directed_broadcasts 0 # default is 1		X	disable_ip_holes.sh [titan module]
1055	Set the system to ignore redirected ip packets	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_ignore_redirect 1 # default is 0		X	disable_ip_holes.sh nddconfig.sh (adds it into /etc/init.d/nddconfig) [titan module]
1056	Set the system to do strict multihoming	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_strict_dst_multihoming 1 # default is 0		X	disable_ip_holes.sh nddconfig.sh (adds it into /etc/init.d/nddconfig)

	Network Tuning and Securing		L	H	
					[titan module]
1057	Reassure the system doesn't respond to ICMP netmask requests	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_respond_to_address_mask_broadcast=0 # default is 0		X	nddconfig.sh (adds it into /etc/init.d/nddconfig) [titan module]
1058	Prevent System responding to ICMP timestamp requests	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_ip_respond_to_timestamp=0 # default is 1		X	nddconfig.sh (adds it into /etc/init.d/nddconfig) [titan module]
1059	Prevent System responding to ICMP timestamp Broadcast	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_ip_respond_to_timestamp_broadcast=0 # default is 1		X	nddconfig.sh (adds it into /etc/init.d/nddconfig) [titan module]
1060	Prevent system sending ICMP redirect messages	Add or modify the following line into the /etc/rc2.d/S??inet script ndd -set /dev/ip ip_send_redirects=0 # default is 1		X	nddconfig.sh (adds it into /etc/init.d/nddconfig) [titan module]
1061	Changes the TCP initial sequence number generation parameters	Change the entry in /etc/default/inetinit to: TCP_STRONG_ISS=2		X	tcp-squence.sh [titan module]

	Network Tuning and Securing		L	H	
1062	Set in.routed to run in quiet mode	To build a wrapper starting routed -q (quiet mode) do following: mv /usr/sbin/in.routed to /usr/sbin/in.routed.orig Create a file /usr/sbin/in.routed with following content: #! /bin/sh /usr/sbin/in.routed.orig –q Change permission to this file: chmod 0755 /usr/sbin/in.routed # Dynamic route receiving daemons are vulnerable to receive incorrect routes. Consider to use static routes (routes added via the route commands in startup files) rather than the routing daemons		X	routed.sh [titan module]
1063	Disable routing	Create an empty file called notrouter touch /etc/notrouter		X	disable_ip_holes.sh [titan module]

2.8 Small Services

2.8.1 NFS

	NFS		L	H	
1070	Removing NFS	We recommend not running NFS in a DMZ. Therefore NFS should be deactivated if is running. Steps to do so: Remove all Shares defined in /etc/dfs/dfstab Kill the NFS daemons: lockd, nfsd, statd, mountd Rename NFS starting scripts: /etc/rc3.d/S??nfs.server and /etc/rc2.d/S??nfs.client (Rename to something like “not_usedS??[scriptname]”)		X	to do by hand
1071	Setting NFS privileged port for tcp	perform the following command: ndd -set /dev/tcp tcp_extra_priv_ports_add 2049		X	disable-NFS-2.6.sh [titan module]
1072	Setting NFS privileged port for udp	perform the following command: ndd -set /dev/udp udp_extra_priv_ports_add 2049		X	disable-NFS-2.6.sh [titan module]
1073	Enables NFS port monitoring	Add following lines to /etc/system: set nfssrv:nfs_portmon = 1 set nfs:nfs_portmon = 1 Make sure permission on /etc/system are set to 644: chmod 644 /etc/system		X	nfs-portmon.sh [titan module]

	NFS		L	H	
1074		nfsd mountd rpc.boot in.rarpd rpld		X	

2.8.2 NIS NIS+

	NIS, NIS+		L	H	
1080	Removing NIS, NIS+	We recommend not running NIS or NIS+ in a DMZ. Therefore it should be deactivated if is running. Steps to do so: Remove domainname entries in the /etc/domainname You could also consider to remove NIS in general: - pkginfo |grep NIS - pkgrm <NIS-Package> system SUNWypr NIS Server for Solaris (root) system SUNWypu NIS Server for Solaris (usr)		X	to do by hand
1081	Remove NIS, NIS+ and DNS lookups	Edit /etc/nsswitch.conf to match following: passwd: files group: files hosts: files		X	nsswitch.sh [titan module]

	NIS, NIS+		L	H	
		networks: files protocols: files rpc: files ethers: files netmasks: files bootparams: files publickey: files netgroup: files automount: files aliases: files services: files sendmailvars: files If you need dns you'll have to edit nsswitch.con accordingly			

2.8.3 Mail

	MAIL		L	H	
1190	stop sendmail from binding to port 25	Sendmail could be used as local transport provider (used by swatch, tripwire and other tools) in order to inform the maintenance and monitoring group to receive online information about the status of the system. This means, sendmail could be still there and installed, but not started as a daemon. You can restrict users to use sendmail with the trusted user entry within sendmail.cf	X		by hand

	MAIL		L	H	
		mv /etc/rc2.d/S88sendmail /etc/rc2.d/not_usedS88sendmail			
1191	Comment all piped aliases for mail out	check /etc/aliases for any programs that mail is piped "|" to and comment "#" them out		X	decode.sh [titan module]
1092	Restricting expn and vrfy on sendmail to gather information	This flag stops nosey persons from connecting to port 25 and using expn and vrfy to gather in /etc/mail/sendmail.cf # O PrivacyOptions=authwarnings,goaway Opgoaway # O PrivacyOptions=noexpn, novrfy, authwarnings O LogLevel=5		X	sendmail.cf [titan module]
1093	Hiding Version on SMTP Banner	Look for the smtp banner line in /etc/mail/sendmail.cf Change it to something like: # SMTP login message De Mail Server Ready		X	smtp-banner.sh [titan module]
1094	disable mail forwarding	User cannot choose by them to have a forwarder. But root controls the forwards in /usr/local/forward/.forward.$u The script adapts /etc/mail/sendmail.cf with the entry: O ForwardPath=/usr/local/forward/.forward.$u		X	sendmail-forward.sh [titan module]

	MAIL		L	H	
		and creates plus permission the /usr/local/forward directory			
1095	accept e-mail	if you really plan to accept external e-mails on your machine (listen to port 25), Compass recommends to use smap or smtpd/smtpfwdd in order to have a secure incoming mail-server (plus anti-spam, secure configuration)	X		to do by hand

2.8.4 FTP

	FTP		L	H	
1100	Securing FTP	Changes or creates /etc/default/ftpd file to add in a umask and ftp banner. UMASK=077 BANNER="`/bin/cat /etc/ftp-banner`" Change permission on /etc/default/ftpd with: chmod 644 /etc/default/ftpd		X	ftp-2.6_secure.sh [titan module]
1101	Create a FTP Banner	Create a Banner /etc/ftp-banner file with content: Example: This system is for authorized users only. Monitoring may occur Change permission on /etc/ftp-banner with: chmod 644 /etc/ftp-banner		X	ftp-2.6_secure.sh [titan module]

	FTP		L	H	
1102	Create a ftpuser file	create a file /etc/ftpusers add all system users to that file Example of system users: root daemon sys bin adm lp smtp uucp nuucp listen nobody noaccess news ingres audit admin sync nobody4 Change permission to 644 chmod 644 /etc/ftpusers		X	ftp-2.6_secure.sh [titan module]

2.8.5 TELNET

	TELNET		L	H	
1110	Prevent display information on telnet banner	Remove the Banner in /etc/default/telnetd to: Banner=”” If /etc/default/telnetd doesn’t exist do following: touch /etc/default/telnetd echo "BANNER=\"\"" >> /etc/default/telnetd chmod 444 /etc/default/telnetd		X	telnet-banner.sh [titan module]

2.9 X-Windows

	X-WINDOW		L	H	
1120	Set CDE to not accept XDMCP login connections from anyone	Replace the Xaccess file with a minimal one If /usr/dt/config/Xaccess exists perform following tasks: cat << EOF >/usr/dt/config/Xaccess # disable all XDMCP connections !* EOF If /etc/dt/config/Xaccess exists perform following tasks: cat << EOF > /etc/dt/config/Xaccess		X	cde.sh [titan module]

	X-WINDOW		L	H	
		# disable all XDMCP connections !* EOF			

2.10 File Permissions

	FILEPERMISSION		L	H	
1030	Remove not used suid files	Many setuid files on Solaris are used only by root. Check setuid files whether they should be run by someone else than root or not Procedure: 1) Find all suid files -> output to suid-files-before-change 2) create backup directory structure (e.g.: /opt/backup/usr/local/bin) 3) save suid files in backup directory structure 4) tar backup structure (find does not find suid files in backup structure) 5) remove backup directory structure 6) remove suid flag for all founded suid-files 7) enable the only needed suid (passwd, su,) 8) do a find again for suid - output to suid-files-after-change important commands: find / -type f\(-perm -4000 \) |xargs ls -a find / -type f\(-perm -4000 \) |xargs chmod -s	X		to do by hand

	FILEPERMISSION		L	H	
1031	Remove not used sgid files	Many setgid files on Solaris are used only by root. Check setgid files whether they should be run by someone else than root or not 1) Find all suid files -> output to sgid-files-before-change 2) create backup directory structure (e.g.: /opt/backup/usr/local/bin) 3) save suid files in backup directory structure 4) tar backup structure (find does not find suid files in backup structure) 5) remove backup directory structure 6) remove sgid flag for all founded suid-files 7) enable the only needed sgid (passwd, su,) 8) do a find again for suid -> output to sgid-files-after-change important commands: find / -type f\(-perm -2000 \) |xargs ls -a find / -type f\(-perm -2000 \) |xargs chmod -s	X		to do by hand
1032	Remove all group writeable files in /etc	Check group-write permission files in /etc find /etc -type f\(-perm 20 \) | xargs ls –las No file in /etc needs group writeable. Remove permission with: find /etc -type f\(-perm 2 \) | xargs chmod g-w	X		to do by hand
1032	Remove all world writeable files in /etc	Check World-write permission files in /etc find /etc -type f\(-perm 2 \) | xargs ls –las	X		to do by hand

	FILEPERMISSION		L	H	
		No file in /etc needs world writeable. Remove permission with: find /etc -type f\(-perm 2 \) | xargs chmod w-w			
1033	change permissions of file with rw-rw-rw to rw-r--r--	First list these files find / -type f -perm 666 |xargs ls -al > perm-666-before-change.txt decide if one of these files are critical find / -type f -perm 666 |xargs chmod 644 find / -type f -perm 666 |xargs ls -al > perm-666-after-change.txt	X		to do by hand
1034	Change permissions of files with rwxrwx???	First list these files find / -type f -perm 777 |xargs ls -al perm-777-before-change.txt decide if one of these files are critical find / -type f -perm 777 |xargs chmod 755 find / -type f -perm 777 |xargs ls -al > perm-777-after-change.txt	X		to do by hand
1035	find world writeable directories	find / -type d\(-perm 2 \) change permissions for your needs	X		to do by hand
1036	Make sure every script started by root belongs to root (these might influence the patching process and	Check owner on all startup scripts find /etc -type f -print | grep rc | egrep -v "skel|tty|mail|snmp|Mail" | xargs ls -al > rc-files-before-change.txt change owner on these files		X	to do by hand

<table>
<tr><th></th><th>FILEPERMISSION</th><th></th><th>L</th><th>H</th><th></th></tr>
<tr><td></td><td>generate error messages)</td><td>find /etc -type f -print | grep rc | egrep -v "skel|tty|mail|snmp|Mail" | xargs chown root:root

find /etc -type f -print | grep rc | egrep -v "skel|tty|mail|snmp|Mail" | xargs ls -al > rc-files-after-change.txt

ls -al /etc/init.d > etc-init.d-before.change.txt
chown root:root /etc/init.d
ls -al /etc/init.d > etc-init.d-after-change.txt

(egrep –v tells not to show the files within the “”
adapt these parameters for your need)

After these changes, all rc.X belong to user root and group root and all files in /etc/init.d belong to user root and group root. This is, because the statement: “what root starts should belong to the user group = protetction from Trojan horse”

PS: If you install patches etc. you might get a warning. Pls. redo the tasks above after updating and patching.</td><td></td><td></td><td></td></tr>
<tr><td>1037</td><td>Check that all cron activities are logged</td><td>Make sure there is the following entry in the /etc/default/cron:

CRONLOG=YES</td><td>X</td><td></td><td>cronset.sh

[titan module]</td></tr>
<tr><td>1038</td><td>Check utmp, utmpx for world write permissions</td><td>Check World-write permission files in /var/adm

find /var/adm -type f\(-perm 2 \) | xargs ls -las

Change file:</td><td>X</td><td></td><td>utmp.sh

[titan module]</td></tr>
</table>

	FILEPERMISSION		L	H	
		chmod 644 /var/adm/utmp			
1039	Find files where no user is associated with	find / -type f –nouser Compass recommends to do 1) find / -type f -nouser > files-nouser-before-change 2) find / -type f -nouser | xargs chwon nobody:nobody 3) find / -type f -nouser > files-nouser-after-change	X		to do by hand
1040	Find files where no group is associated with	find / -type f –nogroup Compass recommends to do 1) find / -type f -nogroup > files-nogroup-before-change 2) find / -type f -nogroup | xargs chgrp nobody 3) find / -type f -nogroup > files-nogroup-after-change	X		to do by hand
1041	Check file permission on /var/cron	Change the permission and owner on /var/cron if not set to 700 and owner is root:sys chmod 700 /var/cron && chown root /var/cron && chgrp sys /var/cron	X		cronset.sh [titan module]

2.11 Logging and Monitoring

	LOGGING & MONITORING		L	H	
1040	Set the limit of cron logfiles to 2 MB before it is rotated.	Edit or add the following entry into /etc/cron.d/logchecker LIMIT=4096	X		cronset.sh [titan module]
1041	Log all inetd services	Edit /etc/init.d/inetsvc so that there are just those following entries /usr/sbin/ifconfig –au netmask + broadcast + /usr/sbin/inetd -s –t Note: If you are running named (DNS server) DHCP, or multicast, you will have to modify this.	X		inetsvc.sh [titan module]
1042	modify syslog.conf	edit syslog.conf to log more information insert the line: *.debug /var/adm/compass.messages This will log debug messages (in the first phase) to this message file.		X	to do by hand
1043	install tripwire	Tripwire is a Trojan horse detector. It works with a reference database, which includes a cryptographic checksum over binaries, and what you configure. Compass recommends to start tripwire (on a productive environment) every 6 hours, because no changes should appear and the output should always be zero. Check the Compass documentation “Installation tripwire” in order to install, configure		X	to do by hand

	LOGGING & MONITORING		L	H	
		this product			
1044	IDS (intrusion detection)	Compass has installed snort on hostabc and hostdef in order to be able to monitor network attacks such as: - cgi-scan - portscans - virus Check out /root/config/snort.rules for your needs.		X	to do by hand
1045	logfile watcher (swatch)	Compass recommends using swatch in order to monitor your logfiles. You can have multiple swatch daemons running on your system to monitor for example: - /var/adm/compass.messages - /var /adm/snort_portscan.log - /opt/AppServer/WebSphere/log/???? Swatch bases on perl and a couple of PERL MODULES. This was installed in order to be able to run swatch successfully. Checkout the Compass documentation “Installation swatch”.		X	to do by hand

2.12 General

	GENERAL		L	H	
1150	Set a boot up Banner	Create a file /etc/issue with a Warning Banner according to your policy Good examples can be found here: http	X		create-issue.sh [titan module]

3 Appendix

3.1 Tools

Tool	Description	URL
Titan	Titan is a very powerful local security analyst. As I went through all modules I have a deep trust to it.	http://www.fish.com/titan/
xinetd	powerful inetd daemon which has the tcpd implemented and the power to bind specific services to specific interfaces (not binding the services to all interfaces)	http://www.synack.net/xinetd/
smtpd/smtpfwdd	smtpd is a tiny little tool as a frontend to sendmail on unix boxes which runs in a chroot enviroment and secures your sendmail.	http://www.obtuse.com/smtpd.html

3.2 Compass script

The following script helps to find the following files within a Solaris box.

- suid files
- sgid files
- group writeable files
- world writeable files
- group writeable directories
- world writeable directories
- nouser files
- nogroup files

Pls. note the grep commands at the end of the script. The following directories and files are not monitores by this script

- /usr/openwin
- /dt/appconfig
- /local/C
- /dt/share/include

To prevent iterative search by XFN, pls. configure the filesystems within the variable fs. The script will only walk and search through the configured filesystems there.

```
#! /bin/csh -f
set fs={/,/usr,/var,/opt};
set report=/opt/compass/scripts/report-find-file.txt
set report1=/opt/compass/scripts/report-find-dir.txt

set i=1
echo "===================================" > $report
echo "search for suid-files" >> $report
echo "===================================" >> $report
```

```
while ( $i <= $#fs )
            /bin/find $fs[$i] -mount -type f \( -perm -4000 \) -print -exec ls -al {} \; >>& $report
            @ i = $i + 1
end

set i=1
echo "========================================" >> $report
echo "search for sgid-files" >> $report
echo "========================================" >> $report
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type f \( -perm -2000 \) -print -exec ls -al {} \; >>& $report
        @ i = $i + 1
end


set i=1
echo "========================================" >> $report
echo "search for group-writeable files" >> $report
echo "========================================" >> $report
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type f \( -perm -20 \) -print -exec ls -al {} \; >>& $report
        @ i = $i + 1
end


set i=1
echo "========================================" >> $report
echo "search for world-writeable files" >> $report
echo "========================================" >> $report
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type f \( -perm -2 \) -print -exec ls -al {} \; >>& $report
        @ i = $i + 1
end
```

```
set i=1
echo "==================================" > $report1
echo "search for group-writeable directories" >> $report1
echo "==================================" >> $report1
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type d \( -perm -20 \) -print  >>& $report1
        @ i = $i + 1
end


set i=1
echo "==================================" >> $report1
echo "search for world-writeable directories" >> $report1
echo "==================================" >> $report1
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type d \( -perm -2 \) -print  >>& $report1
        @ i = $i + 1
end


set i=1
echo "==================================" >> $report
echo "search for nouser files" >> $report
echo "==================================" >> $report
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type f -nouser -print -exec ls -al {} \; >>& $report
        @ i = $i + 1
end


set i=1
echo "==================================" >> $report
echo "search for nogroup files" >> $report
echo "===================================" >> $report
while ( $i <= $#fs )
        /bin/find $fs[$i] -mount -type f -nogroup -print -exec ls -al {} \; >>& $report
        @ i = $i + 1
end

/bin/grep -v "\/usr\/openwin" $report > report-sum1
/bin/grep -v Titan report-sum1 > report-sum2
/bin/grep -v "\/dt\/appconfig" report-sum2 > report-sum3
/bin/grep -v "\/locale\/C" report-sum3 > report-sum4
/bin/grep -v "\/dt\/share\/include" report-sum4 > report-sum5
/bin/grep -v '^/' report-sum5 > report-sum6
```