



Compass Security

Hardening Solaris

March 8, 2001

Document name:	Hardening_Solaris_CSNC_V1.0.pdf
Version:	V 1.0
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:	March 8, 2001
Document state:	PUBLIC



CONTENT

1	INTRODUCTION.....	1
1.1	<i>Related documents</i>	1
1.2	<i>Version control</i>	2
1.3	<i>Reference</i>	3
1.4	<i>Author</i>	3
1.5	<i>Local - Network - Application Security</i>	4
1.6	<i>Monitoring / Alarming and Alerting</i>	6
2	HARDENING SOLARIS.....	7
2.1	<i>How to read the table</i>	7
2.2	<i>Installation</i>	7
2.3	<i>Auditing</i>	8
2.4	<i>System</i>	8
2.5	<i>User Management</i>	12
2.6	<i>Services started on request (inetd)</i>	17
2.7	<i>Services started at boot-time (rc.X)</i>	18
2.8	<i>Interface tuning and securing</i>	21
2.9	<i>File Permissions</i>	24
2.10	<i>Logging and Monitoring</i>	29
2.11	<i>General</i>	32
3	HARDENING APPLICATIONS.....	33
3.1	<i>Introduction</i>	33
3.2	<i>Application Security Considerations</i>	33
3.3	<i>Small Services</i>	36
3.3.1	<i>NFS Server</i>	36
3.3.2	<i>NIS NIS+</i>	37
3.3.3	<i>Mail Server</i>	39
3.3.4	<i>FTP Server</i>	41
3.3.5	<i>TELNET</i>	42
3.3.6	<i>X-Windows</i>	43
3.3.7	<i>RPC (remote procedure calls)</i>	44
4	APPENDIX.....	45
4.1	<i>Tools</i>	45
4.2	<i>Related articles</i>	47
4.3	<i>File Permissions</i>	49
4.3.1	<i>SUID</i>	49
4.3.2	<i>SGID</i>	50
4.3.3	<i>SUID & SGID Statement</i>	51
5	COMPASS APPENDIX.....	52
5.1	<i>Hardening Process</i>	52
5.1.1	<i>Iterativ TITAN usage</i>	52
5.1.2	<i>FILE_FIND_CSNC Script</i>	54
5.1.3	<i>PATCHDIAG_CSNC Script</i>	58

1 Introduction

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

- Network Security
- Local Security

aspects.

Even it is concentrated to Solaris, some of the recommendations are also need to other Unix derivates. This hardening article assumes you want to use Solaris as a DMZ (demilitarized-zone) host! If you just want to harden an internal Solaris machine, you don't have to perform all hardening steps. Which steps you want to apply is your own decision. I would recommend to walk trough this hardening article on your test-machine. This helps you to understand every single recommendation and gives you a basis for later decisions.

This document is not focused on "Application Security" aspects. But one single chapter was included, because you won't run Solaris without an application on it 8-). Pls. read chapter: 1.5 and 3 for further analysis.

1.1 Related documents

This document references to other documents. Especially:

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

These documents are in a draft status and available at <http://www.csnc.ch/> in the download section. The appendix refers to these tools as well. Check out chapter 4.1.

1.2 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
0.87	Ivan Bütler ivan.buetler@csnc.ch	More detailed discussion about 1020 (noshell) Solaris Fingerprinting System included to subject 1043 IP_Filter recommendation in 1064	Hardening_Solaris_CSNC_V0.87.pdf
1.0	Ivan Bütler ivan.buetler@csnc.ch	major change in document structure, intro-section and file-permission recommendations	Hardening_Solaris_CSNC_V1.0.pdf

[Ivan] I would like to proceeding improve the checklist in the future. 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.



1.3 Reference

I started writing this article when I was analyzing tools like TITAN, COPS and TIGER. Other Solaris Hardening tools such as YASSP is not part of this article. When I played around with YASSP, I was not very happy with the structure of the software (binary instead of scripts) and it was hard to understand what YASSP does in the very detail. I did not find any hardening task in YASSP, TITAN does not for me. The website of YASSP indicates in the FAQ section certain problems a Solaris won't startup again after applying the hardening. I will might reference to YASSP in the future....

1.4 Author

Ivan Buetler was doing security assessment at r3 security engineering Switzerland before the merge with Entrust Technologies. After the decision not becoming an Entrust PS employee and further analysis with my fellow Walter Sprenger we decided to found Compass Security Network Computing – or in short terms Compass Security. Since February 1999, we are doing penetration tests and security reviews for Swiss companies.

At the beginning of Compass, we formed our services to “Firewall Check” or “NT Security Check”. But eventually the more generic view of “Network Security”, “Local Security” and “Application Security” became popular to us. This helped us to explain tiger-team services to our clients and to identify appropriate modules and checks the client is really interested for. Therefore I included these “views” to this article. You will find the definition on the next page.

Thank you for reading this article.

Ivan

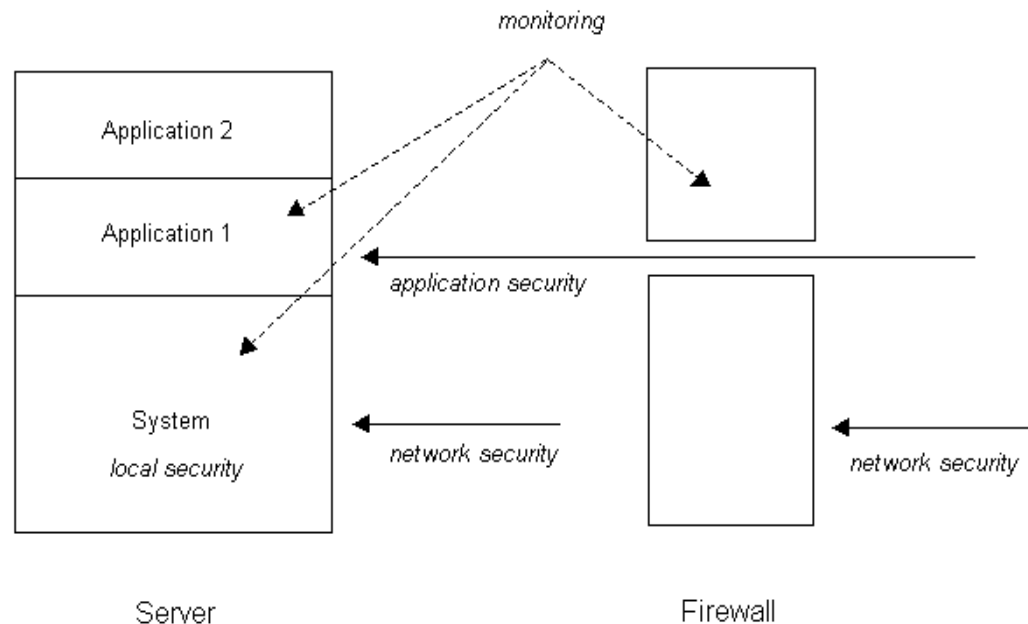
ivan.buetler@csnc.ch
www.csnc.ch

1.5 Local - Network - Application Security

Compass defined 3 levels of security views and 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 unused LISTEN (tcp) / Idle (udp) services (e.g. telnet) is discussed as network security aspect and not under application security terms. Application Security would be “Oracle Security”, “WebSphere Security” or “Apache Webserver Security” in this article.



Hardening an application includes...:

- Limiting user rights
- Limiting rights of the process owner
- Checking file permissions of application specific files
- Restricting access to other system resources
- Minimizes application dependant suid/sgid files
- Activation of security features (if existing)
- Remove samples and other unused components

If an application is exploitable, 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 for authentication
- Secure dangerous network services (IP ACL)
- 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
- Minimize suid/sgid files
- Minimize rw-rw-rw files

Eventually people are aware in take advantage of firewall infrastructure before proceeding with e-business applications. But whatever you do to protect your DMZ hosts by a firewall, the application port need to be open for the outside world. That's why you have e-business! With this in mind, we defined the following hacking scenario:

- Hacker exploits the offered e-business application. In most cases by SSL, HTTP or IIOP (Corba). Let's assume the worst case, the hacker gains an interactive connection to this application by a shell.
- Most customers take advantage of three tier architectures. It's might needed (in the eyes of an attacker) to gain more privileges on the system, in order to read include files from the application (database definitions) or to set the network interface in promiscuous mode (sniffing the DMZ-LAN). The worst case in such a scenario would be, the attacker gains "root" or administrative privileges
- After the e-business tier is under full control of the hacker, he or she might wants to access confidential data's on a nearby database system. The hacker has fully access to all LISTEN or Idle services (not only to the application port, if we assume the DB belongs to the same DMZ segment).

You might ask yourself, why I did not write a "Hardening E-Business application" article, because this seems to be the first step a hacker has to take. You are right. I strongly believe in application security aspects. But various e-business applications are available out there and the hardening depends from application to application. Please checkout the hardening apache, IIS Security or Hardening WebSphere checklist. The latest article can be downloaded from our website, because we already helped clients in hardening WebSphere. Hardening Apache Checklists are available at www.apache.org and the Microsoft Checklists are available at www.microsoft.com/security. Currently I am working on a hardening Oracle checklist....coming soon.

Listen services such as telnet, ftp or rpcbind are not defined to be an application. But if you have a dedicated system to provide access to your mailboxes, the pop server is not only an unused service. In such a case the POP daemon is the application. If you read this article, please keep in mind the hardening tasks below described in the table only protect step 2 and step 3 of the hacking scenario above. We want to make sure, the hacker can't easy gain more privileges on your system and if you expect another DMZ host being hacked not being an easy hacking target. Don't trust your other DMZ hosts!!! This article might helps you to define your security policy, before new Solaris machines are rolled out in the Intra_NET.

1.6 Monitoring / Alarming and Alerting

Alarming and alerting is very need but also specific to your company. The tools described below 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?

Why not explain how Compass set up DMZ hosts? We have a couple of additional tools installed on our DMZ box. These are:

Installed Software	Description
Tripwire	<p>Tripwire provides cryptographic checksum functionality in order to create a reference. Compass runs tripwire in "verify-mode" every 6 hours. The output will be sent to an internal host by e-mail and checked against the reference. Especially binaries and important files in /etc are included to the integrity search path.</p> <p>Whenever a binary is replaced, changed (also when we update software), I will recognize this activities. This is a must to me!</p>
Swatch	<p>Simple watch daemon monitors log-files. This logfiles are typically /var/adm/messages or application specific logfiles. Swatch works with a rule-file. Whenever a pattern appears in the logfile, swatch will dispatch actions. We usually receive e-mails. But you can also start self-written programs. Our rule-file includes (for example) refused, connect, panic, invalid etc.</p>
Arpwatch	<p>Arpwatch monitors MAC addresses. The very first time you start arpwatch, it creates an arp.dat with containing all MAC addresses of your subnet. As soon as a new MAC address appears in the DMZ, Compass will be notified. This is a very powerful tool I like very much.</p>
Syslog	<p>By the way...you have to make sure syslog logs the information you want. In a standard environment, login tries to the SSH daemon are not logged in /var/adm/messages. You have to activate the related flag (auth) before your ssh logins will be logged.</p>
Snort	<p>The last tool we use (and you know already) is snort. Snort is a intrusion detection system providing enhanced pattern matching rules. We haven't installed swatch on every DMZ'host, but snort runs in stealth mode right after the ISP router. Snorts helps us to understand what is going on with back in mind, only specific patterns will be recognized.</p>



2 Hardening Solaris

2.1 How to read the table

H = Hardening

L = Task influences local security aspects

N = Task influences network security aspects

#	Description	How to fix	H		Reference
number	short brief description of the problem	discussion how to fix the problem	L	N	what script might automate this task

2.2 Installation

#	UPDATES	How to fix	L	N	Reference
1000	Apply latest patches	Check http://sunsolve.sun.com for the latest Solaris patches. Use SUNSOLVE patchdiag if 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	X		to be done by hand

		2) Insert special (small) disk and mount it to /var			
1002	Install minimal system	If you are in the position of installing a DMZ host out of the box, please don't install only the following packages: <lvan Input>	X	X	To do by hand

2.3 Auditing

#	AUDIT	How to fix	L	N	Reference
2000	Enable auditing	Auditing is a huge process you have to setup. There is no single recommendation we can make for every requirement. But this article contains possible monitoring and alerting mechanisms in chapter 2.10	X	X	Chapter: 2.10

2.4 System

#	SYSTEM	How to fix	L	N	Reference
3000	eeprom security	<p>"eeprom security-mode=command". The system will change the security level to command and ask you to set a password. Enter a password.</p> <p>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.</p> <p>The need of this hardening step has to be discussed, because everyone will be able to break a system, when physical access is granted. But if you activate eeprom</p>	X		To be done by hand. Pls. try it out on the ok prompt after change.

#	SYSTEM	How to fix	L	N	Reference
		security, the attacker needs to “steel” the box or harddisk, before the disk will be attackable. From this point of view, the hardening task is still a security improvement.			
3001	Set core size to zero	<p><u>Add the following line to the /etc/system file:</u></p> <pre>set sys:coredumpsize = 0</pre> <p>Apply the recommendation above make sense in environments where you won't recognize a panic. Let's assume you are in New York and your Solaris machine will reboot in Los Angeles at 11 pm. After the panic the system will boot again. Would you recognize the reboot?</p> <p>If yes, its might recommended to leave the coredumpsize > 0, because you are going to analyze the dump for sure. But if you belong to the group of Solaris administrators never get any information about reboots if the Solaris machine startup successfully, multiple panic could smash your filesystem with multiple dumps. In such a scenario, it is might recommended to set the coredumpsize to zero.</p> <p>It is might recommended to set the coredumpsize to zero if you are aware of the panic condition and you won't have a coredump at every panic. This value needs to be adapted to your needs</p>	X		<p>disable-core.sh</p> <p>[titan module]</p>
3002	Fix some stack errors [only for Solaris 2.6]	<p><u>Add the following lines into /etc/system:</u></p> <pre>set noexec_user_stack = 1 set noexec_user_stack_log = 1</pre> <p>Change file permission on /etc/passwd: chmod 644 /etc/system</p> <p>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</p>	X		<p>fix-stack.sol2.6.sh</p> <p>[titan module]</p>

#	SYSTEM	How to fix	L	N	Reference
		on the stack and logs it when it happens.			
3003	Allow Power Management only to be run by root [only on Solaris 2.6 and newer]	<u>Edit in the file /etc/default/sys-suspend the follow line:</u> Before: PERMS=console-owner after: PERMS=- and does: "/bin/chmod 0755 /usr/openwin/bin/sys-suspend" This recommendation should prevent from denial of service attacks.	X		powerd.sh [titan module]
3004	Set the sticky bit for the /tmp directory at boot time to mode 1777	<u>Create a file /etc/rc3.d/S79tmpfix file:</u> <pre> /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 </pre> <u>Change permission on S79tmpfix:</u> <pre> /usr/bin/chmod 755 /etc/rc3.d/S79tmpfix </pre> the sticky-bit influences the behaviour of the directory, so you are allowed to write to	X		psfix.sh [titan module]

#	SYSTEM	How to fix	L	N	Reference
		<p>the directory, but not allowed to delete any files. This is important if processes write .socket files into the /tmp directory and you want to prevent hackers being able to manipulate files within the /tmp directory. Don't mix the sticky-bit with the suid bit!</p> <p>Pls. check the /tmp directory before applying the above fix by the following command: ls -al / grep tmp</p> <p>Check out, if you have the "t" in the permissions rwxrwxrwt /tmp. This recommendation is only valid for Solaris 2.6.</p>			
3004	<p>Disable Keystroke stop-'A'</p> <p>[only on Solaris 2.6 and newer]</p>	<p>Change or add "KEYBOARD_ABORT=disable" into /etc/default/kbd.</p> <p>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 person 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.)</p>	X		<p>disable-L1-A.sh</p> <p>[titan module]</p>

2.5 User Management

#	USER MANAGEMENT	How to fix	L	N	Reference
4000	Disable all unused system accounts	<p>Edit /etc/passwd Make sure, the system accounts are locked and have no valid shell defined. Disabling an account could be done by entering NP instead of the * in /etc/passwd.</p> <p>Example: noaccess:x:60002:60002:No Access User:/:/sbin/noshell</p> <pre>cd \$TITAN_HOME/src1 gcc -o ./noshell ./noshell.c cp /sbin/noshell /sbin/noshell.solaris cp \$TITAN_HOME/src1/noshell /sbin/noshell</pre> <p>You can disable accounts by putting NP on the Password files for those users. This will disable those accounts</p> <p>Example: noaccess:NP:60002:60002:No Access User:/:/sbin/noshell</p> <p>A basic listing for SysV Unix: bin, daemon, adm, lp, smtp, sys, uucp, nuucp, nobody, noaccess</p> <p>PS: Compass recommends compiling the nosell.c from the TITAN distribution. This will add the feature of "error-messages to the /var/adm/messages", if someone tries to login to a locked or "no-access" account. The standard /bin/false shell does not provide additional information to /var/adm/messages and therefore attacks will not be detected.</p>	X		<p>to be done by hand</p> <p>to do by hand</p>

#	USER MANAGEMENT	How to fix	L	N	Reference
4001	usage of strong password library	<p>Compass recommends the usage of a strong password enforcer. Under Solaris the tool npasswd will work and compile perfectly.</p> <p>Npasswd will change the passwd libraries and has an extended config-file where you can define pw-length, aging, min-characters, and dictionaries. etc.</p> <p>You can find a special documentation in how to install and configure npasswd in "Installation npasswd".</p>		X	see Installation npasswd documentation
4002	Set default password parameters	<p>Add or edit /etc/default/passwd to match the following entries:</p> <p>PWMIN=1 # Minimum time period before the password can be changed.</p> <p>[only if you want to work with standard passwd functionality - without npasswd]</p>	X		defpwparams.sh [titan module]
4003	Set the Maximum valid time period for passwords	<p>Add or edit /etc/default/passwd to match the following entry:</p> <p>PWMAX=13 # Maximum time period that password is valid</p> <p>[only if you want to work with standard passwd functionality - without npasswd]</p>	X		defpwparams.sh [titan module]
4004	Set the time period where the system is starting to warn password expiration	<p>Add or edit /etc/default/passwd to match the following entry:</p> <p>PWWARN=4 # The number of days relative to MAX before the password expires to # start warning the user of the required change</p> <p>[only if you want to work with standard passwd functionality - without npasswd]</p>	X		defpwparams.sh [titan module]
4005	Set the minimum password length	<p>Add or edit /etc/default/passwd to match the following entry:</p> <p>PWLEN=8 # the following requires that all passwords must have min. length of 8</p>	X		defpwparams.sh (Titan sets PWLEN=6)

#	USER MANAGEMENT	How to fix	L	N	Reference
		[only if you want to work with standard passwd functionality - without npasswd]			[titan module]
4006	Prevent root to login from remote	Add or edit /etc/default/login to match the following entry: CONSOLE=/dev/console # If CONSOLE is set, root can only login on that device.	X		defloginparams.sh [titan module]
4007	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 SYSLOG=YES	X		defloginparams.sh [titan module]
4008	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. TIMEOUT=120	X		defloginparams.sh [titan module]
4009	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). UMASK=027 This will set a standard mask of 750. "rw--r-----" Apply this to the following files: /etc/.login /etc/profile /etc/skel/local.cshrc /etc/skel/local.login /etc/skel/local.profile	X		defloginparams.sh userumask.sh [titan module]
4010	Set UMASK for root	Assure root has a umask of 027 or 077 Check .profile of root	X		to do by hand

#	USER MANAGEMENT	How to fix	L	N	Reference
4011	Assure password prompt for login	Add or edit /etc/default/login to match the following entry: # PASSREQ determines if login requires a password. PASSREQ=YES	X		defloginparams.sh [titan module]
4012	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 ALTSHELL=YES	X		defloginparams.sh [titan module]
4013	Check whether every user has a password set	Check that every user has a password set in /etc/passwd or /etc/shadow user:IRs.8R9EfQXx.:11137:0:10000::: The encrypted Password is between the second and third ":"	X		passwd.sh (check only, no fix) [titan module]
4014	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 defexpire=	X		useraddset.sh [titan module]
4015	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	X		rootchk.sh [titan module]

#	USER MANAGEMENT	How to fix	L	N	Reference
		/etc/skel/local.login /etc/skel/local.profile /.profile /etc/profile			
4016	restrict su to the sugroup and add your users to this group	<p>create special group in /etc/group</p> <p>apply your admin accounts to this group (make them members)</p> <p>change permissions of /bin/su to have: r-sr-x 1 root sugroup</p> <p>chmod 550 /bin/su</p> <p>chmod +s /bin/su</p> <p>chown root:sugroup /bin/su</p> <p><u>ls -al /bin/su</u></p> <p>-r-sr-s--- 1 root sugroup 18360 Jan 15 1998 /bin/su</p> <p><u>grep sugroup /etc/group</u></p> <p>sugroup::600:root,httpadm,wsphere</p> <p>This means, that only the users of the sugroup are able to use the su command. There is no need for wasrun and wwwwrun to be able to su.</p> <p>Another possible and good solutions means take advantage of the sudo utility. Sudo is a wrapper around suid files, where you define in detail, which user is allowed to execute what suid file. Check out chapter: 4.1</p>	X		to do by hand

2.6 Services started on request (inetd)

#	INETD	How to fix	L	N	Reference
5000	Disable all inetd services	<p>Comment all entries in /etc/inetd.conf. (grep -v "^#" /etc/inetd.conf to check services started by inetd)</p> <p>Do only use inetd-services if really needed and protect them by tcpd (tcpwrapper).</p>		X	to do by hand
5001	Implement TCP Wrappers to inetd services.	<p>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:</p> <pre>ftp stream tcp nowait root /usr/local/bin/tcpd in.ftpd telnet stream tcp nowait root /usr/local/bin/tcpd in.telnetd</pre> <p>(We recommend using Wrappers in case inetd services are started for maintenance reasons.)</p> <p>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.</p>		X	to do by hand
5002	Secure inetd	<p>Check hosts.allow and hosts.deny. Make sure you have in</p> <pre>/etc/hosts.deny ALL:ALL</pre> <p>and do open your services in:</p> <pre>/etc/hosts.allow <service>:<source-ip></pre>		X	to do by hand

#	INETD	How to fix	L	N	Reference
5003	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

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

#	rc.X	How to fix	L	N	Reference
6000	Disable all unused Services	<p>This hardening task reflects to stop services started by the ordinary startup procedure.</p> <p><u>Rename not used services started in the rc.X directory.</u> Example: mv /etc/rc3.d/S92volmgt /etc/rc2.d/not_usedS92volmgt</p> <p><u>Titan convention</u> Titan renames the S?? to s??</p> <p><u>These services should be disabled: (you have to decide for yourself 8-)</u></p> <p>snmpdx autofd (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)</p>		X	to do by hand

#	rc.X	How to fix	L	N	Reference
		<p>Disable rpcbind if not used (Special purpose Servers like web servers, ftp servers, mail servers, etc can usually have rpc disabled. If you relay need rpcbind, please refer to chapter 3.3.7, where you enable rpcbind with Vietse Venemmas libwrap.a enabled rpcbind.</p> <p>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.</p>			
6001	Disable all DMI services	<p>Disable all dmi services with: <code>mv /etc/rc3.d/S??dmi /etc/rc3.d/D??dmi</code></p> <p>DMI Services started by <code>/etc/init.d/init.dmi</code> are: <code>/usr/lib/dmi/dmispd</code> <code>/usr/lib/dmi/snmpXdmid</code> <code>/etc/dmi/ciagent/ciinvoke</code></p> <p>Sun Solstice Enterprise Tools. Nobody knows exactly what it does and it's therefore not truthworth.</p>		X	<p>dmi-2.6.sh</p> <p>[titan module]</p>
6002	Disable mounting suid features as the default	<p>Add following lines to <code>/etc/rmmount.conf</code>:</p> <pre>mount hsfs -o nosuid mount ufs -o nosuid</pre>		X	<p>rmmount.sh</p> <p>[titan module]</p>
6003	Check all .rhosts file	<p>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.</p> <p>PS: cluster software might needs .rhosts etc. be carefully with removing trusts in such an environment.</p>		X	<p>rhosts.sh</p> <p>[titan module]</p>
6004	Disallow the use of rhosts authentication	<p>modify the <code>/etc/pam.conf</code> file removing the line: <code>login_auth sufficient /usr/lib/security/pam_rhosts_auth.so.1</code></p>		X	<p>pam-rhosts-2.6.sh</p>

#	rc.X	How to fix	L	N	Reference
	authentication	<pre>rlogin auth sufficient /usr/lib/security/pam_rhosts_auth.so.1</pre> <p>and changing the rsh line to read:</p> <pre>rsh auth required /usr/lib/security/pam_unix.so.1</pre>			[titan module]
6005	Checking Trust Relationship	<p>Check that the file /etc/hosts.equiv is empty.</p> <p>For more information type: man hosts.equiv</p>		X	<p>hosts.equiv.sh (check only, no fix)</p> <p>[titan module]</p>
6006	umask for startup files	<p>create a S00umask to every rc.X directory to make sure, the process has this umask</p> <pre>/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</pre> <pre>/etc/init.d/umask</pre>		X	<p>add-umask.sh</p> <p>[titan module]</p>

2.8 Interface tuning and securing

#	NETWORK SECURING	How to fix	L	N	Reference
7000	Shorten the period of time the ARP cache maintains entries	Add the following lines to the inet startup script /etc/rc2.d/S??inet nndd -set /dev/arp arp_cleanup_interval 60000 /* 1 min (default is 5 min*/		X	adjust-arp-timers.sh [titan module]
7001	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 nndd -set /dev/ip ip_ire_flush_interval 60000 /* 1 min (default is 20 min*/		X	adjust-arp-timers.sh [titan module]
7002	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 nndd -set /dev/ip ip_respond_to_echo_broadcast 0 # default is 1		X	disable-ping-echo.sh [titan module]
7003	Disable source routing at boot time	Add or modify the following line into the /etc/rc2.d/S??inet script nndd -set /dev/ip ip_forward_src_routed 0 # default is 1		X	disable_ip_holes.sh [titan module]
7004	Prevent System to forward ip packets at boot time	Add or modify the following line into the /etc/rc2.d/S??inet script nndd -set /dev/ip ip_forwarding 0 # default is 1		X	disable_ip_holes.sh [titan module]
7005	Prevent system to forward directed broadcast packets	Add or modify the following line into the /etc/rc2.d/S??inet script nndd -set /dev/ip ip_forward_directed_broadcasts 0 # default is 1		X	disable_ip_holes.sh [titan module]
7006	Set the system to ignore redirected ip packets	Add or modify the following line into the /etc/rc2.d/S??inet script nndd -set /dev/ip ip_ignore_redirect 1 # default is 0		X	disable_ip_holes.sh nnddconfig.sh (adds it into /etc/init.d/nddconfig)

#	NETWORK SECURING	How to fix	L	N	Reference
					/etc/init.d/nddconfig) [titan module]
7007	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) [titan module]
7008	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]
7009	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]
7010	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]
7011	Prevent system sending ICMP redirect messages	Add or modify the following line into the /etc/rc2.d/S??inet script		X	nddconfig.sh (adds it into /etc/init.d/nddconfig)

#	NETWORK SECURING	How to fix	L	N	Reference
		<pre>ndd -set /dev/ip ip_send_redirects=0 # default is 1</pre>			/etc/init.d/nddconfig) [titan module]
7012	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]
7013	Set in.routed to run in quiet mode	To build a wrapper starting routed -q (quiet mode) do following: <pre>mv /usr/sbin/in.routed to /usr/sbin/in.routed.orig</pre> Create a file /usr/sbin/in.routed with following content: <pre>#!/bin/sh /usr/sbin/in.routed.orig -q</pre> Change permission to this file: <pre>chmod 0755 /usr/sbin/in.routed</pre> # 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]
7014	Disable routing	Create an empty file called notrouter <pre>touch /etc/notrouter</pre>		X	disable_ip_holes.sh [titan module]
7015	Take advantage of ip filter	Suddenly I was in the situation, where multihomed Solaris boxes need rpcbind on hme0, but there is no reason to have rpcbind running on qfe0. I did some tests with ip_filter. This is a kernel module for Solaris, where you can build packet filtering rules.			

#	NETWORK SECURING	How to fix	L	N	Reference
		<p>I don't agree changing every Solaris box to a firewall would make sense. But in such a special scenario, the ip_filter was the only solution.</p> <p>Therefore I do also recommend to take advantage of ip_filter, whenever you can't see a solution to prevent services being visible on a specific interface. I recommend to have simple ip_filter rules to save processing time as well.</p>			

2.9 File Permissions

#	FILE PERMISSIONS	How to fix	L	N	Reference
8000	Remove not used suid files	<p>SUID files are the most risk to gain root privileges!. Check setuid files whether they should be run by someone else than root or not. Usually Solaris in a DMZ environment is not a "multi-user" operating system in the sense a lot of interactive connection by different users will appear. Most time, the amount of enabled non-root users is pretty small.</p> <p>Procedure:</p> <ol style="list-style-type: none"> 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 <p>If you want to see an example of the recommended steps, pls. refer to: 4.3.1.</p>	X		to do by hand

#	FILE PERMISSIONS	How to fix	L	N	Reference
		Compass included a detailed description of “hardening suid” files.			
8001	Remove not used sgid files	<p>Check setgid files whether they should be run by someone else than root or not</p> <ol style="list-style-type: none"> 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 <p>If you want to see an example of the recommended steps, pls. refer to: 4.3.2. Compass included a detailed description of “hardening sgid” files.</p>	X		to do by hand
8002	<p>Remove all group writeable files in /etc</p> <p>[If you want to check for group writeable files in “/”, pls. change the command to your needs]</p>	<p>Check group-write permission files in /etc</p> <pre>find /etc -type f \(-perm -20 \) -exec ls -al {} \;</pre> <pre>find /etc -type f \(-perm -20 \) -exec ls -al {} \; > search-4-group-writeable-in-etc.txt</pre> <p>No file in /etc needs group writeable.</p> <pre>find /etc -type f \(-perm -20 \) -exec chmod g-w {} \;</pre>	X		to do by hand
8003	<p>Remove all world writeable files in /etc</p> <p>[If you want to check for world writeable files in “/”, pls. change the command to your needs]</p>	<p>Check World-write permission files in /etc</p> <pre>find /etc -type f \(-perm -2 \) -exec xargs ls -als {} \;</pre> <pre>find /etc -type f \(-perm -2 \) -exec xargs ls -als {} \; > search-4-world-writeable.txt</pre> <p>No file in /etc needs world writeable. Remove permission with:</p>	X		to do by hand

#	FILE PERMISSIONS	How to fix	L	N	Reference
	needs]	find /etc -type f \(-perm -2 \) –exec xargs chmod w-w {} \;			
8004	change permissions of file with rw-rw-rw to rw-r--r--	<p>First list these files</p> <pre>find / -type f -perm 666 xargs ls -al > perm-666-before-change.txt</pre> <p>decide if one of these files are critical</p> <pre>find / -type f -perm 666 –exec chmod 644 {} \;</pre> <pre>find / -type f -perm 666 –exec xargs ls –al {} \; > perm-666-after-change.txt</pre>	X		to do by hand
8005	Change permissions of files with rwxrwx???	<p>First list these files</p> <pre>find / -type f -perm 777 –exec xargs ls -al {} \; > perm-777-before-change.txt</pre> <p>decide if one of these files are critical</p> <pre>find / -type f -perm 777 –exec xargs chmod 755 {} \;</pre> <pre>find / -type f -perm 777 –exec xargs ls -al {} \; > perm-777-after-change.txt</pre>	X		to do by hand
8006	find world writeable directories	<pre>find / -type d \(-perm 2 \) –print</pre> <pre>find / -type d \(-perm 2 \) –print > search-4-world-writeable-directories.txt</pre> <p>change permissions for your needs [check out the logfile after you did the command above]. Decide by yourself what permissions you can set more restrictive.</p> <p>If you want to check for group-writeable files as well, pls. use the following command:</p> <pre>find /etc -type f \(-perm -20 \) –print > search-4-group-writeable-dir.txt</pre>	X		to do by hand
8007	Make sure every script started by root belongs to root	<p>Check owner on all startup scripts</p> <pre>find /etc -type f -print grep rc egrep -v "skelltty mail snmp Mail" xargs ls -al > rc-files-before-change.txt</pre>		X	to do by hand

#	FILE PERMISSIONS	How to fix	L	N	Reference
	(these might influence the patching process and generate error messages)	<p>files-before-change.txt</p> <p>change owner on these files</p> <pre>find /etc -type f -print grep rc egrep -v "skel tty mail snmp Mail" xargs chown root:root</pre> <p>find /etc -type f -print grep rc egrep -v "skel tty mail snmp Mail" xargs ls -al > rc-files-after-change.txt</p> <pre>ls -al /etc/init.d > etc-init.d-before.change.txt</pre> <pre>chown root:root /etc/init.d</pre> <pre>ls -al /etc/init.d > etc-init.d-after-change.txt</pre> <p>(egrep -v tells not to show the files within the "" adapt these parameters for your need)</p> <p>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 = protection from Trojan horse"</p> <p>PS: If you install patches etc. you might get a warning. Pls. redo the tasks above after updating and patching.</p>			
8008	Check that all cron activities are logged	<p>Make sure there is the following entry in the /etc/default/cron:</p> <pre>CRONLOG=YES</pre>	X		<p>cronset.sh</p> <p>[titan module]</p>
8009	Check utmp, utmpx for world write permissions	<p>Check World-write permission files in /var/adm</p> <pre>find /var/adm -type f(-perm 2 \) xargs ls -las</pre>	X		<p>utmp.sh</p> <p>[titan module]</p>

#	FILE PERMISSIONS	How to fix	L	N	Reference
		Change file: chmod 644 /var/adm/utmp			
8010	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
8011	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
8012	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]

#	LOGGING & MONITORING	How to fix	L	N	Reference
		<p>this product</p> <p>SUN provides a tripwire similar tool called “sfpDB”. This means Solaris Fingerprinting System. Pls. refer to http://sunsolve.Sun.COM/pub-cgi/show.pl?target=content/content7 for detailed information.</p> <p>Solaris 2 is delivered with the ASET utility, allow scanning of the system for changes or weak configuration. Compass recommends tripwire instead of ASET.</p>			asset.sh]
9004	IDS (intrusion detection)	<p>Compass has installed snort on hostabc and hostdef in order to be able to monitor network attacks such as:</p> <ul style="list-style-type: none"> - cgi-scan - portscans - virus <p>Check out /root/config/snort.rules for your needs.</p>		X	to do by hand
9005	logfile watcher (swatch)	<p>Compass recommends using swatch in order to monitor your logfiles. You can have multiple swatch daemons running on your system to monitor for example:</p> <ul style="list-style-type: none"> - /var/adm/compass.messages - /var /adm/snort_portscan.log - /opt/AppServer/WebSphere/log/???? <p>Swatch bases on perl and a couple of PERL MODULES. This was installed in order to be able to run swatch successfully.</p> <p>Checkout the Compass documentation “Installation swatch”.</p>		X	to do by hand

#	LOGGING & MONITORING	How to fix	L	N	Reference
9006	BSM	<p>Sun deliver a "C2" level auditing system for both SunOS (Sunshield) and Solaris (Sunshield BSM). It is bundled with Solaris 2. The Solaris 2.4 BSM is discussed here. BSM allows the actions of specific users to be recorded and written to an audit file. However, the auditing is at the system call level, meaning huge logs may be generated by simple user actions. Performance is also affected. The standard analysis tools praudit and auditreduce offer no high level analysis of audit trails. Applications may also write to the audit trail.</p> <p>Reference documentation: "SunSHIELD Basic Security Module Guide" (Standard Solaris 2.x documentation). Man pages: audit(1m), audit_startup(1m), udit_warn(1m), auditconfig(1m), auditreduce(1m), bsmconv(1m).</p> <ul style="list-style-type: none"> - Audit only an absolute minimum of user actions. - Don't bother auditing if you don't have a system expert capable of interpreting the logs! - If you switch on auditing, then write a script which analyses the audit trail in real time and raise alerts when necessary. - Analysis of the audit trail should take into account existing processes analysing syslog or other system logs. - There is no way of auditing file access depending on the filename. E.g. all write attempts to /etc/passwd cannot be simply audited. Neither is it possible to trace use actions on a high level. - Ensure that the audit trail is stored on a partition with enough space, consider centralising audit trails of several machines via secure NFS and auditreduce. <p>See also Solaris C2/BSM security notes (sp/Solaris_bsm.html).</p>	X		<p>Copied from BORAN (www.boran.com)</p> <p>[titan checks the existence of BSM with the tool bsm.sh]</p>

#	LOGGING & MONITORING	How to fix	L	N	Reference
		[Ivan] I do not have much experience with BSM. If you feel like having good recommendations here, pls let me know!			

2.11 General

#	LOGGING & MONITORING	How to fix	L	N	Reference
10'000	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://www.titanproject.org/wiki/IssueBanner	X		create-issue.sh [titan module]

3 Hardening Applications

3.1 Introduction

As from our experience applications are not set up secure, I want to highlight some major considerations you might think about it. If you want a detailed description about hardening a specific application, please take a look at the vendor website or search through the Internet.

3.2 Application Security Considerations

Recommendations	Description
<p>Run your application by an unprivileged user (uid)</p>	<p>Try to run application processes with an unprivileged user-id. As far as I know, every application is able to do so. (under Unix!!!)</p> <p>If the hacker gains an interactive shell (worst case scenario you have to assume), he or she will firstly have permissions such as the application. Normally the hacker would be allowed to read configuration and might write to the log-file directories. But there is no need to write the configuratio.</p> <p>We recognized a difference between application with own user management such as the Oracle database and other applications using Solaris authentications. Having an application-owner user and application-running user in place makes sense for all applications without its own user management. But we strongly advice to take advantage of this concept if you run webservers, mailservers, etc.</p> <p>If you want to “see” a more detailed description of this concept, please refer to the “Hardening WebSphere” concept in http://www.csnc.ch/ download section.</p>
<p>Define an application owner. This UID owns all files (config, binaries, etc.)</p>	<p>Having an application-specific user in place, which does not run the application daemon but owns binaries and config files, you have the first improvement step in place.</p>

Recommendations	Description
	<p>You are also able to divide certain roles within the Solaris environment. It's not absolutely required the system administrator is also the webserver administrator.</p> <p>Example: Webserver</p> <p>Create a user in /etc/passwd called wwwadm Create a user in /etc/passwd called wwwrun</p> <p>Enforce the webserver administrator to login to the Solaris machine (by ssh hopefully) with the username wwwadm. This user is able to reconfigure and change the behaviour of the application. But the wwwrun only runs the process. ps -ef shows up wwwrun being the process owner.</p>
Samples	<p>Most e-business applications are delivered with samples. We strongly recommend to remove samples from your productive system. Samples mostly have powerful features. I want to refer to the stronghold showstatus sample tool, which shows detailed information in the log file. Compass recognized strong authentication to the application (very long session / seed) without being able to guess the session number in a short time period. But with being able to use the showstatus sample, everybody was in the Internet was able to "see" the session written to the logfile. Doing session hijacking this way is peace of cake!</p>
chroot	<p>Changing the root directory of a process is another step increasing application security. We have chroot'ed ssh daemon, sendmail, apache and other applications. In most cases enabling chroot for an application is hard work. Additional utilities like "truss" under Solaris or "strace" under Linux help understand what files are required by the application. As you might know, every single file needed by the applicatin needs to be in the chroot.</p> <p>Why chroot?. In the early stage of Compass Security, the ISP was hosting our website. We had an interactive shell to this machine as well. But there were about 100 other website hosted on this machine. Doing little investigation by the try to change into these directories failed because file permission settings. So we wrote our own little dirty scripts, moved into the /cgi-bin directory and suddenly the webserver-daemon did the investigation for us. If the ISP would have chroot'ed every single client to it's own jail, this would not have been able.</p>

Recommendations	Description
	If external resources are doing administrative tasks of your e-business application, why not chroot'ing the ssh-daemon to the webserver root-directory? If I recognize the need of publishing our "chrooting ssh" article at a certain time (because you really read this article), I will do it immediately.
Application specific recommendations	I have to stop here with my recommendations, because I would have to start with webserver-considerations, WebSphere considerations, Oracle-considerations and so one. Please don't ever trust your vendor recommendations if they try to explain the service only runs with "root" privileges. This is not true!!!! Unix makes it possible!!

3.3 Small Services

As introduced during the application security considerations, I understand NFS being an application, if the goal of the machine is to provide NFS shares. But if the major goal of a Solaris server intends to be an Oracle server, the NFS service is called “small service”, which need to be disabled.

If you can't stop NFS from being started even the Solaris machine is an Oracle e-business server, please refer to the little dirty recommendations below. Don't assume this would make small services secure, but it might helps you to apply little security improvements.

3.3.1 NFS Server

#	NFS	How to fix	L	N	Reference
10'100	Removing NFS	We strongly 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
10'101	Setting NFS privileged port for tcp	perform the following command: ndd -set /dev/tcp tcp_extra_priv_ports_add 2049 (only necessary, if you really can't stop the nfs daemon)		X	disable-NFS-2.6.sh [titan module]
10'102	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]

#	NFS	How to fix	L	N	Reference
		(only necessary, if you really can't stop the nfs daemon)			
10'103	Enables NFS port monitoring	Add following lines to /etc/system: <pre>set nfssrv:nfs_portmon = 1 set nfs:nfs_portmon = 1</pre> Make sure permission on /etc/system are set to 644: <pre>chmod 644 /etc/system</pre>		X	nfs-portmon.sh [titan module]

3.3.2 NIS NIS+

#	NIS, NIS+	How to fix	L	N	Reference
10'200	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 SUNWypyr NIS Server for Solaris (root) system SUNWypu NIS Server for Solaris (usr)		X	to do by hand
10'201	Remove NIS, NIS+ and DNS	Edit /etc/nsswitch.conf to match following:		X	nsswitch.sh

#	NIS, NIS+	How to fix	L	N	Reference
	lookups	passwd: files group: files hosts: files 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.conf accordingly			[titan module]
10'202	If NIS is required, please take advantage of NIS+	If you really need NIS in your DMZ environment, for example in a cluster environment, please take advantage of NIS+. This would require to start keyserv again.		N	to do by hand

3.3.3 Mail Server

#	MAIL	How to fix	L	N	Reference
10'300	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 mv /etc/rc2.d/S88sendmail /etc/rc2.d/not_usedS88sendmail	X		by hand
10'301	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]
10'302	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 O goaway # O PrivacyOptions=noexpn, novrfy, authwarnings O LogLevel=5		X	sendmail.cf [titan module]
10'303	Hiding Version on SMTP Banner	Look for the smtp banner line in /etc/mail/sendmail.cf Change it to something like: # SMTP login message		X	smtp-banner.sh [titan module]

#	MAIL	How to fix	L	N	Reference
		De Mail Server Ready			
10'304	disable mail forwarding	<p>User cannot choose by them to have a forwarder. But root controls the forwards in /usr/local/forward/.forward.\$u</p> <p>The script adapts /etc/mail/sendmail.cf with the entry:</p> <pre>O ForwardPath=/usr/local/forward/.forward.\$u</pre> <p>and creates plus permission the /usr/local/forward directory</p>		X	sendmail-forward.sh [titan module]
10'305	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/smtpfwd in order to have a secure incoming mail-server (plus anti-spam, secure configuration)	X		to do by hand
10'306	if sendmail (as service) is required, take advantage of smtpd or smap	<p>smtpd and smap are tiny small services running in a chroot environment to accept incoming mails. Compass strongly recommends not let sendmail being the service LISTEN to the port 25, instead using smtpd or smap to do so.</p> <p>If required, Compass could publish a "SMTPD/SMTPFWDD concept" article, which describes in detail what we are talking about here. If you take advantage of smtpd or smap, you are not attackable from sendmail network exploits by malformed string exploits and similar.</p>		X	to do by hand

3.3.4 FTP Server

#	FTP	How to fix	L	N	Reference
10'400	Stop FTP from being started	<p>Compass strongly recommends take advantage of SSH as the best solutions to access Solaris machines in an FTP-style manner. SSH 2.0 clients from www.ssh.com include a graphical interface to scp (secure copy). You won't recognize any difference between ftp and the scp client. Needless to say, ftp provides plaintext authentication, which is very simple to sniff on the network. There are specific hacker tools only waiting for unencrypted authentication packets (dsniff). Dsniff is able to decrypt more protocols you would expect!!!! (VNC, PCAnywhere, BasicAuth,....)</p> <p>The following recommendations only need to be applied, if you can't live without FTP up and running.</p>		X	think about it
10'401	Securing FTP	<p>Changes or creates /etc/default/ftpd file to add in a umask and ftp banner.</p> <pre>UMASK=077 BANNER="/bin/cat /etc/ftp-banner`"</pre> <p>Change permission on /etc/default/ftpd with:</p> <pre>chmod 644 /etc/default/ftpd</pre>		X	ftp-2.6_secure.sh [titan module]
10'402	Create a FTP Banner	<p>Create a Banner /etc/ftp-banner file with content:</p> <p>Example: This system is for authorized users only. Monitoring may occur</p> <p>Change permission on /etc/ftp-banner with:</p> <pre>chmod 644 /etc/ftp-banner</pre>		X	ftp-2.6_secure.sh [titan module]

#	FTP	How to fix	L	N	Reference
10'403	Create a ftpuser file	<p>create a file /etc/ftpusers</p> <p>add all system users to that file</p> <p>Example of system users: root daemon sys bin adm lp smtp uucp nuucp listen nobody noaccess news ingres audit admin sync nobody4</p> <p>Change permission to 644</p> <p>chmod 644 /etc/ftpusers</p>		X	ftp-2.6_secure.sh [titan module]

3.3.5 TELNET

#	TELNET	How to fix	L	N	Reference
10'500	Stop TELNET from being started	<p>Compass strongly recommends take advantage of SSH as the best solutions to access Solaris machines in an TELNET-style manner. SSH 2.0 clients from www.ssh.com include a graphical interface similar to the TELNET client. You won't recognize any difference between telnet and the ssh client. Needless to say, telnet provides plaintext authentication, which is very simple to sniff on the network. There are specific hacker tools only waiting for unencrypted authentication packets (dsniff). Dsniff is able to decrypt more protocols you would expect!!!! (VNC, PCAnywhere, BasicAuth,...)</p> <p>The following recommendations only need to be applied, if you can't live without TELNET up and running.</p>		X	think about it
10'501	Prevent display information on telnet banner	Remove the Banner in /etc/default/telnetd to:		X	telnet-banner.sh

#	TELNET	How to fix	L	N	Reference
		Banner="" If /etc/default/telnetd doesn't exist do following: <pre>touch /etc/default/telnetd echo "BANNER=\"\" >> /etc/default/telnetd chmod 444 /etc/default/telnetd</pre>			[titan module]

3.3.6 X-Windows

#	X-WINDOW	How to fix	L	N	Reference
10'600	Stop X Windows Server from being started	Compass strongly recommends take advantage of SSH as the best solutions to access Solaris machines in an X11-style manner. SSH 2.0 clients from www.ssh.com include X11 port forwarding feature. You won't recognize any difference between direct X11 connections and the ssh-tunneled X11 connections (beside of speed) Needless to say, X11 provides plaintext authentication (even with the magic-cookie), which is very simple to sniff on the network. There are specific hacker tools only waiting for unencrypted authentication packets (dsniff). Dsniff is able to decrypt more protocols you would expect!!!! (VNC, PCAnywhere, BasicAuth,...)		X	think about it
10'601	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: <pre>cat << EOF >/usr/dt/config/Xaccess # disable all XDMCP connections !* EOF</pre>		X	cde.sh [titan module]

#	X-WINDOW	How to fix	L	N	Reference
		<pre>If /etc/dt/config/Xaccess exists perform following tasks: cat << EOF > /etc/dt/config/Xaccess # disable all XDMCP connections !* EOF</pre>			

3.3.7 RPC (remote procedure calls)

#	RPC	How to fix	L	N	Reference
10'700	Take advantage of libwrap.a from tcpwrapper to enable IP based access control to your rpcbind or portmapper	Compass strongly recommends to exchange the standard Solaris rpcbind to the libwrap.a enabled rpcbind from Vietse Venemma. The rpcbind from Vietse enables same IP access control features like tcpwrapper. You can control what IP address is allowed to access the portmapper by /etc/hosts.allow		X	think about it

4 Appendix

4.1 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. It's the free implementation of smap from TIS firewall toolkit (TISFWTK).	http://www.obtuse.com/smtpd.html
COPS	CERT provides a system security checker called COPS. It checks your permissions, searches .rhosts etc.	COPS 1.04 is also archived at ftp://ftp.cert.org/pub/tools/cops/ Merlin provides a graphical front-end to COPS and other security software
TIGER	Tiger is another system security checker.	ARC's TARA - Tiger Analytical Research Assistant also provides security checking similar to COPS. Commercial ("PRO") and free versions. It is based on TAMU's Tiger software.
tcpwrapper	IP based ACL for inetd services. Usage of /etc/hosts.allow and /etc/hosts.deny	ftp://ftp.porcupine.org/pub/security/index.html

Tool	Description	URL
	/etc/hosts.deny	
ipfilter	IP Filter is a TCP/IP packet filter, suitable for use in a firewall environment. To use, it can either be used as a loadable kernel module or incorporated into your UNIX kernel; use as a loadable kernel module where possible is highly recommended. Scripts are provided to install and patch system files, as required.	http://coombs.anu.edu.au/ipfilter/ http://www.obfuscation.org/ipf/
snort	flexible packet sniffer/logger that detects attacks Snort is a libpcap-based packet sniffer/logger which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has a real-time alerting capability, with alerts being sent to syslog, a separate "alert" file, or even to a Windows computer via Samba.	http://www.snort.org
tripwire	A file and directory integrity checker. Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.	http://www.tripwire.com/
swatch	Swatch was originally written to actively monitor messages as they were written to a log file via the UNIX syslog utility. It has multiple methods of alarming, both visually and by triggering events. The perfect tools for a master loghost. This is a beta release of version 3.0, so please use it with caution. The code is still slightly ahead of the documentation, but examples exist. NOTE: Works flawlessly on Linux (RH5), BSDI and Solaris 2.6 (patched).	http://www.stanford.edu/~atkins/swatch/
arpwatch	a tool that monitors ethernet activity and keeps a database of ethernet/ip address pairings. It also reports certain changes via email.	ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/arpwatch/

Tool	Description	URL
	address pairings. It also reports certain changes via email.	watch/
ssh	Secure Shell. Replacement for TELNET, FTP. Tunneling feature for X11 traffic.	www.ssh.com www.openssh.org
npasswd	<i>Npasswd</i> is a replacement for the <i>passwd</i> command for UNIX. New passwords are stringently screened to decrease the chance of having passwords vulnerable to guessing by programs such as Crack. In addition <i>npasswd</i> addresses other deficiencies found in many vendor-supplied <i>passwd</i> programs.	http://www.utexas.edu/cc/unix/software/npasswd/
sudo	sudo (Super User Do) is a very useful program that allows a system administrator to give certain users the ability to run some (or all) commands as root	http://www.courtesan.com/sudo/ . http://www.kempston.net/solaris/sudo.html
rpcbind from Vietse Venemma	rpcbind and portmapper including IP ACL bases on tcpwrapperr of Vietse Venemma	ftp://ftp.porcupine.org/pub/security/index.html
lsof	analyze which process binds what port. This gives you more information about LISTEN or Idle services	ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/

4.2 Related articles

WWW Link	Description
www.boran.com	BORAN consulting in Switzerland
www.sunworld.com/common/security-faq.html	Solaris Security FAQ
ftp.porcupine.org/pub/security/index.html	Vietse Venema articles (libwrap.a author)

4.3 File Permissions

4.3.1 SUID

The following procedure shows how you might eliminate unused suid files. Especially on DMZ hosts, most of the suid files are not required:

ENUMERATE suid FILES on your SYSTEM

```
find / -type f \( -perm -4000 \) -exec ls -al {} \;  
find / -type f \( -perm -4000 \) -exec ls -al {} \; > $HOME/search-4-suid-files.txt
```

Check out the logfile and you are wondering, how many suid files are in place!!!

BACKUP suid FILES first:

```
mkdir /opt/backup/suid  
find / -type f \( -perm -4000 \) -print |cpio -pudm /opt/backup/suid
```

The command above will make a copy with corresponding permissions to /opt/backup/suid. After the command has finished successfully, you will have (for example) a copy of the suid passwd command in /opt/backup/suid/usr/bin/passwd

TAR the suid directory before removing the suid FLAG. This is your backup. Don't remove the suid-files.tar!!

```
cd /opt/backup; tar -cvpf suid-files.tar /opt/backup/suid/*  
rm -r /opt/backup/suid
```

You will have a TAR archive with all suid-files in it.

REMOVE suid FLAG from suid FILES

```
find / -type f \( -perm -4000 \) -exec chmod -s {} \;
```

Check again, if you still have suid-files in place.

```
find / -type f \( -perm -4000 \) -exec ls -al {} \;
```

ENABLE suid FLAG for well-known FILES

```
chmod u+s /usr/bin/su      (if you login by unprivileged user and do su -> good solution)
chmod u+s /usr/bin/passwd (if you want users to change their password)
chmod u+s /usr/bin/ps     (if you want unprivileged user to view the process list)
```

Doing suid-hardening in that way is might a bit "hard". But it follows the concept of "enabling" what you need and not disabling what you "don't need". The enable-way needs more knowledge, but considering the most risky part of gaining root privileges goes through suid files. At least from our experience.

You have to enable suid files and other files as well (Oracle-Listener, etc.). Pls. use the hardening steps above with care. Make sure you have a working backup before the magic command.

4.3.2 SGID

The following procedure shows how you might eliminate unused suid files. Especially on DMZ hosts, most of the suid files are not required:

ENUMERATE sgid FILES on your SYSTEM

```
find / -type f \( -perm -2000 \) -exec ls -al {} \;
find / -type f \( -perm -2000 \) -exec ls -al {} \; > $HOME/search-4-sgid-files.txt
```

Check out the logfile and you are wondering, how many sgid files are in place!!!

BACKUP sgid FILES first:

```
mkdir /opt/backup/sgid
find / -type f \( -perm -2000 \) -print |cpio -pudm /opt/backup/sgid
```

The command above will make a copy with corresponding permissions to /opt/backup/sgid. After the command has finished successfully, you will have (for example) a copy of the ssgid /usr/bin/adb command in /opt/backup/sgid/usr/bin/adb

TAR the sgid directory before removing the sgid FLAG. This is your backup. Don't remove the sgid-files.tar!!

```
cd /opt/backup; tar -cvpf sgid-files.tar /opt/backup/sgid/*
rm -r /opt/backup/sgid
```

You will have a TAR archive with all sgid-files in it.

REMOVE sgid FLAG from sgid FILES

```
find / -type f \( -perm -2000 \) -exec chmod -s {} \;
```

Check again, if you still have suid-files in place.

```
find / -type f \( -perm -2000 \) -exec ls -al {} \;
```

ENABLE suid FLAG for well-known FILES

Doing sgid-hardening in that way is might a bit "hard". But it follows the concept of "enabling" what you need and not disabling what you "don't need". The enable-way needs more knowledge, but considering the most risky part of gaining root privileges goes through suid files. At least from our experience.

You have to enable sgid files and other files as well. Pls. use the hardening steps above with care. Make sure you have a working backup before the magic command.

4.3.3 SUID & SGID Statement

I was removing the suid and sgid files from a SUN SOLARIS 2.7. I can absolutely make sure the system successfully boots after these steps, but you need to enable the suid or sgid files you want. If you want to use ipcs for example after the hardening as an unprivileged user, you will get a "permission denied" error message. For emergency reasons you have still the "original" files in your /opt/backup directory. Check out the tar file for further analysis.



5 Compass Appendix

5.1 Hardening Process

This section might help you to perform the hardening/auditing steps mentioned above. I usually get TITAN up and running and to a “verify” check. See the raw output below:

5.1.1 Iterativ TITAN usage

create your audit directory. In this case it was:

```
/opt/compass/download
```

copy sources of titan in /opt/compass/download

```
gzip -d titan.tar.gz
```

```
tar -xvf titan.tar
```

```
cd titan
```

Configure titan

```
./Titan-Config -i
```

(answer the question about shadow)

Run Titan in verify-mode

```
./Titan -v
```

After Titan did his job, I usually go to the log-file directory. This directory contains logs for all checks. I do a grep for “FAILS” and “PASS” within this log directory. Afterwards I know, what Titan identified to be a “weakness”.

```
corro:Titan,v4.0ALPHA-9# uname -a
```

```
SunOS corro 5.7 Generic_106541-06 sun4u sparc SUNW,Ultra-5_10
```

```
cd /opt/compass/download/titan/Titan,v4.0ALPHA-9/logs/modules
```

```
corro:modules# grep FAILS *
aset.sh.V.162520:ASET not installed - FAILS CHECK
disable-accounts.sh.V.162520:root1 shell = /sbin/sh - FAILS CHECK
disable-services.sh.V.162520:Service S??rpc still active in /etc/rc2.d - FAILS CHECK
disable-services.sh.V.162520:Service S??nfs.server still active in /etc/rc3.d - FAILS CHECK
eeprom.sh.V.162520:eeprom security-mode is currently NOT SET! - FAILS CHECK
fix-cronpath.sh.V.162520:      No cron.allow file - FAILS CHECK
keyserv.sh.V.162520:File /etc/rc2.d/S71rpc keyserv ; user nobody enabled - FAILS CHECK
nuke-powerd.sh.V.162520:File /etc/rc2.d/S85power exists.- FAILS CHECK
nuke-rpc.sh.V.162520:File /etc/rc2.d/S71rpc exists.- FAILS CHECK
passwd.sh.V.162520:The above accounts have no password - FAILS CHECK
rootchk.sh.V.162520:      /etc/skel/local.cshrc - Contains . - FAILS CHECK
rootchk.sh.V.162520:      /etc/skel/local.profile - Contains . - FAILS CHECK
rootchk.sh.V.162520:      /opt/compass/download/titan/Titan,v4.0ALPHA-9/bin/lib is NOT owned by root. FAILS CHECK.
sendmail.sh.V.162520:smrsh not found in /sbin - FAILS CHECK
snmpdx-2.6.sh.V.162520:Snmpdx daemon is enabled: FAILS CHECK
syslog.sh.V.162520:you define loghost to be a remote system - FAILS CHECK
```

Perform the hardening tasks

You can tell Titan to do the hardening for you. Let's assume the script rhosts.sh FAILS, this means titan identified some rhosts files, you can create a single file within the titan home directory.

```
echo "rhosts.sh -v" > rhosts.verify.conf
```

```
echo "rhosts.sh -f" > rhosts.fix.conf
```

You can firstly check (verify) this module by: `./Titan -f ./rhosts.verify.conf`

This will create a single logfile within the log directory

Afterwards you are going to apply this module by `./Titan -f ./rhosts.fix.conf`

The "-f" flag turns titan into fix-mode. The script rhosts.sh will fix the problem for you.

I would recommend to do a `./Titan -f ./rhosts.verify.conf` after you applied the fix to make sure, the program really did what it should do and to understand its behaviour.

Eventually, if you feel more comfortable with titan, you can add more modules to a single config-file. For example add:


```
# START Configuration Section
#
# define fs please
# define path of logfiles please
# -----
set fs={/, /opt, /var};
set report=/opt/compass/download/scripts/report-find-file.txt
set report1=/opt/compass/download/scripts/report-find-dir.txt

# END Configuration Section
# -----
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\VC" report-sum3 > report-sum4
/bin/grep -v "\dt\share\include" report-sum4 > report-sum5
/bin/grep -v '^' report-sum5 > report-sum6
```

Have you recognized the creation of report-sum?. You should edit this grep commands to your needs. The files in \$report contain full content of the search command.

5.1.3 PATCHDIAG_CSNC Script

patchdiag_CSNC_V1.0.sh (Download the script)

This script is included in: http://www.csnc.ch/download/sources/scripts_hardening_CSNC_V1.0.tar.gz

If you have SunSolve, you will use standard SUN patchdiag to apply recommended patches. Don't read further.... But if you download the patches from the Internet, the following procedure might helps you to identify installed and uninstalled recommended patches.

```
download recommended patches from http://sunsolve.sun.com. This example assumes, the downloaded file is named as "7_Recommended.zip"
cd /opt/compass/download
mkdir /opt/compass/download/patches
cp 7_Recommended.zip /opt/compass/download/patches
unzip /opt/compass/download/patches/7_Recommended.zip
cd /opt/compass/download/patches/7_Recommended
cp patchdiag_CSNC_V1.0.sh /opt/compass/download/patches/7_Recommended
Now you can take the patchdiag_csnc.sh to identify already installed patches. The script will create a file "already-installed-patch.txt" within the directory. You have to make sure, you have copied the script to the patch directory. Otherwise the script won't work.
```

```
#!/bin/csh -f
#
# Author:    Ivan Buetler
# Goal:     patchdiag by hand
#
#####33
setenv PATH /usr/bin
set installed=on.txt
showrev -p | awk '{print $2}' > $installed

set patchcluster=`ls -al|grep drwx|awk '{print $9}' | grep -v "\."`
set x=1
```

```
while ($x <= $#patchcluster)
  grep $patchcluster[$x] $installed >> temp.txt
  @ x = $x + 1
end

sort temp.txt > temp2.txt
cat temp2.txt | awk '{print "already installed patch "$1}' > already-installed-patch.txt

rm $installed
rm temp.txt
rm temp2.txt
```

The patchdiag_csnc.sh is a quick and dirty script as well.