Global Information Assurance Certification Paper

Mark Strong
GSEC Practical Assignment (v.1.2e)

DEFENSE IN DEPTH ON A SOLARIS 2.X SYSTEM: A RESOURCE GUIDE

The purpose of this paper is to outline a defense in depth security structure for a Solaris 2.x system and offer resources to help implement and maintain security at each individual layer. The information contained in this document will provide a good systems administrative aid for a defense in depth implementation.

1.0 Physical Security - Layer 1

1.1 Environment

First check your hardware manuals for the environmental tolerances/requirements of your system such as temperature, humidity and power. Make sure the location you place the system meets these needs as well as has fire and power surge protection. It is also recommended that you supply your system with power failure protection with an UPS that features interface software to your system to enable a graceful shutdown when failures occur.

1.2 Access Control and Monitoring

In most cases your place of work will have existing policies mandating access control and monitoring requirements. Check these policies and locate your system accordingly. If further assistance is needed contact your site security office. The guiding factors regarding the extent of your security needs is going to depend on what the system is used for (i.e. the value of the data the system will host or be connected to) and the availability requirements of the system.

2.0 Operating Environment Installation and Configuration - Layer 2

2.1 Plan Ahead

One of the most important steps in setting up a defense in depth security scheme for a host is to execute the initial install and configuration with foresight regarding the implementation of the surrounding security layers. Good planning at this stage with not only lessen work to be done at later stages, it will help you get the system ready for adding the other layers that rely on this initial configuration and save rework.

2.2 Choosing an Operating Environment

It is important to note for clarification purposes that Solaris packages what it terms an "operating environment" which includes all its delivered software of which SunOS, which is the operating system, is included. The best way to start securing system software is to choose an operating environment version that has the best security features and of course meets your hardware and software compatibility requirements. Sun issues what they term "Trusted" versions of their

Solaris operating environments. The Trusted versions are designed for and evaluated against evolving security criteria. According to Trusted Solaris 8 Operating Environment: A Technical Overview: "Trusted Solaris 8 software is currently undergoing evaluation against the Common Criteria at the EAL4 level with the Labeled Security Protection Profile (LSPP -- equivalent to the Orange Book -- Trusted Computer System Evaluation Criteria (TCSEC) B1 class)." (1)

2.3 Operating Environment Installation

Place your system on an isolated network to execute the install so you can protect the system from hacking attempts during the installation process before your security measures are in place. For all your external requirements, use another active system to retrieve necessary information and software. Next, you will want to install your chosen operating environment in a minimized capacity such that you only install exactly what is needed for the system to function for its intended purpose(s). Solaris offers the "core" install as a selection to install a minimized operating environment if that suits your needs. When partitioning your system disk(s), a good idea is to create a separate partition for your log partition /var to avoid denial of service attacks flooding your logs and filling and crashing the root partition. After the installation is complete, you should obtain the latest vendor patch cluster for your version of Solaris from http://sunsolve.sun .com and install it. During the installation of the patch cluster, any patches that affect components that you did not install will fail with an error code of 8.

2.4 System Security Fine Tuning

After the operating environment installation is complete, you need to check/modify your system to further tighten the security. It is good idea at this point to set up a log book either in softcopy on another system or in a physical notebook to list all changes to a system for your benefit and that of your fellow systems administrators. The following sections will outline how to fine tune various areas of your operating environment.

2.4.1 Accounts and Authentication

Make sure your system is setup to use the /etc/shadow password file so that encrypted passwords are read-only to root. Remove any unnecessary accounts and groups. Restrict root logins by users to the system console by adding the line CONSOLE=/dev/console to the /etc/default/login file. An eeprom password can be setup, if desired, by changing your eeprom security mode to either "command" or "full" for added security from either the system prompt or PROM level "ok" prompt (Note: if your eeprom password is misplaced or forgotten, you will have to replace the eeprom to access the system). To help protect against trojans, make sure that all root startup scripts are under root control as well as the physical paths that are set for the PATH environmental variable in the scripts. Also, do not include "." (the current directory) in the default search paths. Set roots default umask to 077 or 027. Execute the "logins -p" command to check for existing accounts without passwords. Enable Solaris built in account control features such as password aging, disable old password reuse, and account expiration. For additional password management security control you can employ the use of other tools such as epasswd (http://www.nas.nasa.gov/Groups/Security/epasswd) or npasswd

(http://ftp.sunet.se/ftp/pub/security/tools/password/npasswd).

There are also tools available to delegate various levels of root access such as RBAC and sudo. Role-based access control (RBAC) enables custom accounts or roles to be configured to assign only the required system privileges to a user to perform their job duties. For additional information, download http://www.sun.com/software/whitepapers/wp-rbac/wp-rbac.pdf. Sudo allows the allocation of limited root privileges to users and logs their activities. For more information, go to http://www.courtesan.com/sudo.

Also integrated into Solaris 2.6 and above is The Pluggable Authentication Module (PAM) framework which enables a systems administrator to customize the authentication process on a per application basis. PAM acts similar to a wrapper in that it is an additional function that is transparent to the application and user.

2.4.2 Cron

An often overlooked area of risk is the cron facility which needs to be secured to avoid the abuse of its capabilities. Beyond malicious cron jobs being setup by a hacker, even a user can accidentally create a cron job that can have devastating effects on the system. For example, if a full backup of a large system is being run at a certain time and a user sets a cron job up that is very cpu and network intensive to run at the same time, a denial of service could occur. All unnecessary files in /var/spool/cron/crontabs should be removed and all remaining files should be under root control including any script files called in the crontab entries and so on. This does not necessarily mean that the non-root crontabs have to be owned by root, but special accounts can be set up by the systems administrator with passwords known only to the administrator(s) that run specific tasks required by users. With root control of crontabs, all cron additions can be verified prior to their implementation. This allows the system administrator to understand the system usage more intimately and control what types of processes are being run via cron and when. The /etc/cron.d/ allow and deny files should also be modified accordingly. For auditing purposes, cron logging should be enabled by adding CRONLOG=YES to the /etc/default/cron file.

2.4.3 Filesystems

All files and directories on your systems should be examined and permissions should be allocated appropriately to allow only required access. Use the "find" command to create a list of all files with SUID/SGID permissions and change permissions where needed. After you configure the system such that only necessary files have SUID/SGID permissions, create a new list and store this list on another system so that regular file checks can be run and compared against the list to show possible trojans. You can also disable SUID and SGID bits on mounted filesystems by using the "nosuid" option in the "mount" command (do not use this option on system partitions). Another important aspect of filesystem security is tracking change. Two tools that can help with filesystem security administration are Tripwire and AIDE. Tripwire is a is a semi-free tool that monitors various changes to your filesystem in detail and outputs its findings in easy to read reports (http://www.tripwire.com). AIDE is a free tool that was designed to encompass the

same capabilities as Tripwire and more (http://www.cs.tut.fi/~rammer/aide.html). Check out their associated web sites for more information.

2.4.4 Banners

In order to protect yourself and your organization you need to set up banners which are messages that appear when a user logs into the system. You have to inform the user about authorized access and monitoring rules/guidelines regarding your system. A banner should be configured for every access type. The /etc/issue file can be used to set up a banner for a basic system configurations but you may have to investigate how to set up a banner for specialized login services and graphical environments.

2.4.5 Network Services

Peruse the /etc/inetd.conf and /etc/services files and disable all unneeded services by commenting them out and also remove or disable all their associated startup scripts in the /etc/rc#.d directories (where # is the run level number). The so called "r" commands and ftp should be disabled since they can be replaced with ssh2 (or higher version) which contains secure encrypted transfer versions of these programs (for more information about ssh go to http://www.ssh.com/products/ssh). After completion, execute a kill -HUP of the inetd process to re-initialize the inetd daemon which controls these network services. Turn off IP forwarding by creating an empty /etc/notrouter file using the "touch" command (Solaris 2.6 and above). TCP Wrappers is a tool that provides additional network services security since it wraps TCP services or acts as a go between the inetd daemon and the service application. TCP Wrappers features include access control lists, logging facilities and address spoofing protection (ftp://ftp.porcupine.org/pub/security/index.html).

2.4.6 System Auditing/Logging

The first step in system logging configuration is to set up reliable timekeeping. This can be accomplished in numerous ways which vary in accuracy and reliability. Another possible variable in time configuration is if you are going to choose a remote log host (since you will need to keep accurate time on both your system and the remote log host). Some basic methods of setting your system time are using the "date" command or setting a cron job to run the "rdate" command that will synchronize your system to another system that keeps reliable time. A better approach is to configure and run Network Time Protocol (NTP). NTP is a standard feature of the Solaris 2.x operating environment. Sample server and client configuration files are also included. The next step in system logging configuration is to set up a logging facility. Syslog is a standard feature of the Solaris 2.x operating environment and will be enabled by default with the operating environment installation. You can fine tune syslog to meet your needs by editing the /etc/syslog.conf file including the configuration of a remote log server. You can also setup C2 (kernel based) auditing on a Solaris system if necessary. According to Software White Papers: Sun Solaris Security: "Solaris C2 auditing includes the Basic Security Mode (BSM) functionality,

which enables the logging of events down to the system call level." (2)

2.4.7 Miscellaneous

There are numerous other ways to boost your system security. A personal host based firewall such as one of the SunScreen products offered by Sun Microsystems can be useful (for more information go to http://www.sun.com/software/securenet). Solaris 2.x also has built in time and password dependent screenlocks for user protection. To help prevent stack overflows you can add the following lines to your /etc/system file:
set no_exec_user_stack=1
set no_exec_user_stack_log=1
After you add these lines you will need to reboot your system to have them take effect.
There are also tools available to help "harden" or further secure your operating system and save manual labor. Some of these tools are as follows:

Automated Security Enhancement Tool (ASET) is a standard feature of the Solaris 2.x operating environment and allows the administrator to set the system to one of three predefined security levels (low, medium or high). The tool automates the fixing of various security holes (for more information go to http://www.sun.com/software/white-papers/wp-security).

Solaris Security Toolkit: JASS is an innovative operating system hardening tool because the configuration is scripted and it has multiple levels of undo. JASS can also be run as part of a JumpStart installation. Another important point to keep in mind is your support contract when using various security tools. Be aware that it is possible that a tool could make a change to your system causing it to be unsupported. The JASS software itself is not supported by Sun but the changes it makes to your system are covered (for further information go to http://www.sun.com/security/jass).

Titan is a collection of Bourne shell scripts that can be used to harden an operating system and is designed in a modular fashion. This design makes it possible to add your own customized scripts to increase system security as you see fit and also help you to understand the workings of your system better (for more information go to http://www.fish.com/titan).

YASSP (Yet Another Solaris Security package) is a major innovation in system hardening. It not only saves hand modifications to secure a system, but it also bundles into its package TCP Wrappers (hardens TCP services), Tripwire (monitors files system integrity) and Fix-modes (enhances permission security of vital files and directories). For more information about YASSP go to http://www.yassp.org.

3.0 Vulnerability Analysis - Layer 3

After you have installed the operating environment and configured it to be as secure as your

knowledge permits, it comes time to analyze and test the configuration for vulnerabilities. Since you have already installed the recommended vendor patch cluster which includes the vendors suggested security patches, it is a good idea to check other sources for current lists of vulnerabilities that will affect your system and all of the add on software which you have installed.

If you have added on other non-system software for end users, you should check the web sites of those vendors for the latest patches for security or bugs and apply them if it makes sense. There is a web site (http://icat.nist.gov/icat.cfm) that has an actual vulnerability search engine available called "ICAT" that consists of a form where you can plug in refined information specific to your needs to search for vulnerabilities and related patch information. Some other good web sites to check are http://www.sans.org and http://www.securityfocus.com.

Once you have found and fixed all the vulnerabilities that you researched, you should now run automated tools to scan your system for holes much like a hacker would but without exploiting them. As you would probably imagine, there are a tremendous amount of scanning tools available for this purpose. SARA and Nmap are two popular vulnerability scanners. Security Auditor's Research Assistant (SARA) is a derivative of SAINT and SATAN (http://www-arc.com/sara). Network Mapper (Nmap) is an open source tool for network mapping and vulnerability analysis (http://www.insecure.org/nmap). Before scanning your system with these tools make sure the system is either located on an isolated network and/or you have written permission to run the scans and load the software on another system. If any vulnerabilities are discovered during your scans, research and remove them.

4.0 Configuration Management - Layer 4

At this point your system should be in a good state that is ideal for an initial snapshot of the systems configuration. You should determine a location that is not on the system to store the system snapshot. One method is to upload the snapshot to an intranet systems administration web site (which is backup up regularly) so that subsequent snapshots and reports can be uploaded and stored by system name and date. You can create a snapshot using various system commands such as "pkginfo" (lists installed software package information) and tools you may have installed such as Tripwire to all append all the information you want collected to one or more files named appropriately (including the date). You should now make a full backup of the system and store it in a safe place for use as an initial system configuration baseline. Move your system to the network in which it is supposed to reside. Automate the snapshot process so periodic snapshots can be created and uploaded to your the web site via cron. In addition to normal backups you should create periodic baseline backups after any significant system changes and log those changes as well as any other changes made between the baseline backups in your systems administration log book or file to aid in disaster recovery.

5.0 Social Engineering - Layer 5

If policies and procedures do not already exist that encompass the system you have just configured, then they must be created. Create policies that outline the areas you want users to be

aware of and follow regarding your system. Some possible topics to be outlined are password policies, configuration changes, disk usage and problem reporting. Implement these policies in procedures. Educate system users of the policies and procedures and locate them for easy user access. Maintain the policies and procedures to keep them current. An additional suggestion would be to get written permission to run the crack on your passwd/shadow file to keep your password expiration policies/procedures current.

6.0 Maintenance - Layer 6

Now that your system is ready for use, you need to maintain your system security. Maintaining a secure system configuration is a never ending process. The first step is to create a backup strategy based on your needs and the needs of your users and implement it according your environment and budget. Develop a regular and in depth system auditing procedure and try to automate the process as much as possible. Keep your system patches up to date by periodically checking the sunsolve web site (http://sunsolve.sun.com) where you can also subscribe to the Sun Security Alert mail list (http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec). If a patch management tool would fit the needs of your environment, you can obtain Sun Management Center software which contains a patch management tool plug in (For more information go to http://www.sun.com/solaris/sunmanagementcenter/overview.html). Finally, regularly check the aforementioned vulnerability web sites to keep up on needed changes and sign up for security notification mailing lists where available and appropriate for your needs.

References:

(1) Unknown. "Trusted Solaris 8 Operating Environment White Paper: Trusted Solaris 8 Operating Environment: A Technical Overview." 2001. URL: http://www.sun.com/software/white-papers/wp-ts8 (24 Jun. 2001)

(2) Unknown. "Software White Papers: Sun Solaris Security." 2001. URL: http://www.sun.com/software/white-papers/wp-security (24 Jun. 2001)

(3) Spitzner, Lance. "Armoring Solaris: Preparing Solaris for a Firewall." 22 Oct. 2000. URL: http://www.enteract.com/~lspitz/armoring.html (24 Jun. 2001).

(4) Vandenberg, Paul D. J., and Susan D. Wyess. "Securing Solaris Servers: A Checklist Approach." 26 Nov. 1998. URL: http://www.usenix.org/sage/sysadmins/solaris/index.html (24 Jun. 2001).

(5) Galvin, Peter Baer. "The Solaris Security FAQ: Answer All of Your Questions Here." SunWorld Jul. 7 2000. URL: http://secinf.net/info/unix/security-faq.html (24 Jun. 2001)

(6) Garfinkel, Simson, and Gene Spafford. Practical UNIX & Internet Security, 2nd Edition.

Sebastopol: O'Reilly & Associates, Inc., 1996.

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor