Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Solaris

When configuring a Solaris system for production, a balance must exist between system manageability and security. It is necessary to determine the role the system will play in order to determine what services it needs to run. The objective is to keep things simple. By dedicating separate machines for different tasks, it is expected that only one or two services will run on a host. This methodology makes it easier to isolate applications, harden, and troubleshoot. This type of minimalist approach runs only what is absol...

Copyright SANS Institute
Author Retains Full Rights

AD

Securing Solaris

Angela Orebaugh

October 2, 2000

When configuring a Solaris system for production, a balance must exist between system manageability and security. It is necessary to determine the role the system will play in order to determine what services it needs to run. The objective is to keep things simple. By dedicating separate machines for different tasks, it is expected that only one or two services will run on a host. This methodology makes it easier to isolate applications, harden, and troubleshoot. This type of minimalist approach runs only what is absolutely necessary. Keeping a Solaris system secure is a daily task. This includes keeping up on exploits, patches, and reviewing log files. The following suggestions are just the beginning to securing your Solaris system. There are some additional steps that may need to be taken depending on the systems role in the organization, and some of the steps listed may not apply. Consulting the listed references for additional information is highly recommended.

1. Install the Operating System

   Securing a Solaris system starts with the installation. This consists of an "initial" install of the latest version of the Solaris operating system. With every new release, Sun incorporates improvements and additional features to enhance system security. Be sure that the system is disconnected from the network, or connected to an isolated network while performing the install and the subsequent hardening tasks. Attaching the system to a public network before it is secured can lead to a possible compromise. To get the necessary patches, use a second machine to download the files and burn them to CD-ROM, or connect to the isolated network to transfer them.

   Choosing the minimum "core" install increases security by reducing the amount of software and possible exploits. The core installation also decreases the amount of disk space needed for the install. Additional necessary packages can be added at a later time.

   The system will need to be partitioned to allocate disk space for system files, logging and applications. The four recommended partitions are /, /usr, /var and /opt. The /usr and /opt partitions are used for application installation. The size of these partitions varies according to available disk space and the size of the applications being installed. The /var partition is used for system logging and protects the root (/) partition from overfilling. The /swap partition is created automatically from the initial install.

2. Apply Patches

   Once the initial installation is complete and the system has rebooted, it is time to install the patches. Recommended Patch Clusters can be downloaded from Sun at http://www.sunsolve.sun.com. Maintenance Updates (MU) are also available to service contract customers. They should be applied before the Recommended Patch Clusters. If a patch fails with a "return code 8", then the patch applies to a package not installed on the system. A "return code 2" indicates that the patches have already been applied.

3. Secure the inetd

   The next step to securing Solaris is the removing unnecessary services from the inetd.conf file. This can be done by placing a pound sign (#) in front of the line that is not needed. It is ideal to comment out everything in the inetd.conf file and add them back as needed. Telnet and FTP will be replaced with SSH. Ideally, comment out ftp, tftp, systat, rexd, ypupdated, netstat, rstatd, rusersd, sprayd, walld, exec, talk, comsat, rquotad, name, uucp, sadmind, login, finger, chargen, echo, time, daytime, discard, telnet, imap, pop3, dtspc, fs, kcms, and all rpc services.

4. Secure the startup scripts

   The startup scripts reside in /etc/rc2.d and /etc/rc3.d. Many of the services here are not needed and pose potential security vulnerabilities. To stop a script from starting, replace the capital S with a lowercase s (or K with a lowercase k). Some example services that should be disabled are:

   Automounter /etc/rc2.d/S74autofs

   Sendmail /etc/rc2.d/S88sendmail and /etc/rc1.d/K57sendmail

   RPC /etc/rc2.d/S71rpc

   SNMP /etc/rc2.d/S76snmpdx

   NFS server */etc/rc3.d/S15nfs.server*

NFS client */etc/rc2.d/S73nfs.client*

5. Enable logging

The default Solaris system logging occurs in /var/adm. Enable additional logging by creating two additional logging files, /var/adm/sulog and /var/adm/loginlog. The sulog will log successful and unsuccessful su attempts. The loginlog will catch consecutive failed login attempts. Enable the files by:

#touch /var/adm/sulog

#touch /var/adm/loginlog

#chmod 600 /var/adm/sulog

#chmod 600 /var/adm/loginlog

#chown root /var/adm/sulog

#chown root /var/adm/loginlog

#chgrp sys /var/adm/sulog

#chgrp sys /var/adm/loginlog

Uncomment the following line in /etc/syslog.conf to log authentication messages:

#auth.notice ifdef(`LOGHOST', /var/log/authlog, @loghost)

Then perform the following to create the proper authlog file:

#touch /var/log/authlog

#chmod 600 /var/log/authlog

#chown root /var/log/authlog

6. Miscellaneous security tasks

Set the TCP initial sequence number generation parameters to protect against hijacking and spoofing.

In the file /etc/default/inetinit set TCP_STRONG_ISS=2

Protect against buffer overflow attacks by adding the following to /etc/system:

Set noexec_user_stack=1

Set noexec_user_stack_log=1

Ensure that root can only access the console by making sure the following line in /etc/default/login is not commented out:

CONSOLE=/dev/console

Remove, lock or comment out unnecessary accounts, including "sys", "uucp", "nuucp", "smtp" and "listen". The best way to disable them is to put "*LK*" in the password field of the */etc/shadow* file. The following command line options can also be used to remove or lock accounts:

Remove – #passmgmt –d *account*

Lock – #passwd –l *account*

Change the /etc/motd to contain warnings about inappropriate and unauthorized use of the system.

Remove sendmail packages – SUNWsndmr and SUNWsndmu

Remove group write permission of the /etc directory by performing the following:

```
chmod -R g-w /etc
```

Disable routing by performing the following:

```
#touch /etc/notrouter
```

Remove */etc/hosts.equiv, /.rhosts*

Disable the Stop-A abort sequence by changing the following in /etc/default/kbd:

```
KEYBOARD_ABORT=disabled
```

Enable EEPROM security:

```
#eeprom security-mode=full
```

New password: password

Retype new password: password

Do not make this password the same as root. Setting the security level to full requires a password to boot the system. "Command", instead of
"full", may be used to provide protection without the need of a boot password.

7. Installing SSH

   SSH is used for secure communications to the Solaris system. It encrypts all communications to the system. SSH has its own logging and access control, like TCP Wrapper, but is more secure since traffic cannot be sniffed. SSH can be obtained from http://www.ssh.com or http://openssh.com.

8. YASSP

   Another resource to consider using is YASSP – Yet Another Secure Solaris Package. It automates some of the changes above and incorporates additional functionality such as Tripwire, TCP Wrappers, and a version of SSH. It can be found at http://yassp.parc.xeorx.com. It is recommended to install YASSP, then perform steps 3 through 7 as a safety check.

Boran, Sean. "Hardening Solaris: Securely Installing a Firewall Bastion Host." 25 October 1999. http://securityportal.com/cover/coverstory19991025.html (25 Sept. 2000)

Carnegie Mellon University. "Installing and Securing Solaris 2.6 Servers." 14 June 2000. http://www.cert.org/security-improvement/implementations/i027.02.html (24 Sept. 2000)

Galvin, Peter. "The Solaris Security FAQ." 7 July 2000. http://www.sunworld.com/common/security-faq.html (23 Sept. 2000)

Noordergraaf, Alex and Watson, Keith. "Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology." December 1999. http://www.sun.com/blueprints/1299/minimization.pdf (23 Sept. 2000)

Noordergraaf, Alex and Watson, Keith. "Solaris™ Operating Environment Network Settings for Security." December 1999. http://www.sun.com/blueprints/1299/network.pdf (23 Sept. 2000)

Noordergraaf, Alex and Watson, Keith. "Solaris™ Operating Environment Security." January 2000. http://www.sun.com/blueprints/0100/security.pdf (23 Sept. 2000)

Spitzner, Lance. "Armoring Solaris." 27 August 2000. http://www.enteract.com/~lspitz/armoring.html (24 Sept. 2000)

Last Updated: November 27th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
HIMSS	**Boston, MAUS**	**Dec 01, 2015 - Dec 02, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Cyber Defence Delhi 2016	**Delhi, IN**	**Jan 11, 2016 - Jan 22, 2016**	**Live Event**
SANS Brussels Winter 2016	**Brussels, BE**	**Jan 18, 2016 - Jan 23, 2016**	**Live Event**
SANS Security East 2016	**New Orleans, LAUS**	**Jan 25, 2016 - Jan 30, 2016**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Alexandria, VAUS**	**Feb 03, 2016 - Feb 10, 2016**	**Live Event**
SANS Scottsdale 2016	**Scottsdale, AZUS**	**Feb 08, 2016 - Feb 13, 2016**	**Live Event**
SANS Secure Japan 2016	**Tokyo, JP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
ICS410 London 2015	**OnlineGB**	**Nov 30, 2015 - Dec 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**