Interested in learning more about securing Unix?

SANS Institute

Security Consensus Operational Readiness Evaluation

Unix Security Checklist

Auditing Unix (Solaris)

References:

Securing Solaris, Angela Orebaugh, October 2000
Secure Backups on Solaris Internet Servers, Richard Cove, November 2000
Central Logging Security, James Hunter, November 2000
An explanation of "TCP Wrappers" for the security manager, Rick Branicki, November 2000
Security Issues in NIS, James O'Brien, November 2000
Unix Logging and Security (Systems under siege), Chris Boyd, November 2000
An elementary introduction to Sendmail, Jay Coleson, August 2000
NFS Security, Samuel Sheinin, May 2000
Log Consolidation with syslog, Donald Pitts, December 2000
TCP Wrapper: A toll to help protect your data, Dan Gates, December 2000
Security and System maintenance automation, Ron Ryan, January 2001
TCP Wrappers – What are they?, Stacy Arruda, February 2001

Introduction

This checklist is to be used to audit a Unix (Solaris) environment. This checklist is of a technical nature and does not include manual procedures to be reviewed e.g. Reviewing the physical security of the Solaris server.

While all attempts have been made to make this checklist as comprehensive as possible, it can't be relied upon to be all-inclusive.

Elements to consider prior to applying this checklist:

- Other operating systems performing some of functions: This checklist needs to be tailored to the different circumstances of the network environment especially when there are other network operating systems within the architecture performing specific functions e.g. when an NT operating system performs the authentication of users and the application is hosted on the Solaris box.
- Other utilities: Where possible we have made mention of the various utilities to be used to enhance the operations and security of the Solaris box, however it is quite impossible to make mention of all freeware, shareware or commercial products. Thus, when the auditor is reviewing the security of the Solaris box, he must ascertain what utilities are being run on the Solaris system and ascertain the security impact of using such utilities. A good source to ascertain such security impacts is to review vendor documents accompanying commercial products or visit their sites (for freeware/shareware as well) and review security documents posted there.
- Findings and data sensitivity: When reporting any findings the auditor should take into account the risk element i.e. is the finding so substantial as to directly affect the availability, confidentiality and integrity of sensitive information. Thus, prior to performing the audit it is important to ascertain what data/applications are stored on the Solaris box. The risk committee/department can give the auditor indications of the risk pertaining to certain data. In some instances the finding may seem significant, however it may not be affect organisation due to the risk associated with that data e.g. To secure telephone extensions of the organisation.
  This step is fundamental to provide management with meaningful report.
- Mitigating Controls: The review of Solaris can't be done in a vacuum without considering database and application controls.

For example if an application calls the Solaris server using the root id. This seems to be a significant finding. However, the logical access controls for the application may be so granular that this risk is mitigated and thus this is not a significant finding. This is a mitigating control.
Weak security on the Solaris box may be mitigated by strong controls in either the database or the application.

- Peripheral Devices: This checklist has not made provision for environments where other devices like modems have been connected to the Solaris box.
- Practicality of checklist: The checklist highlights a list of security configurations to achieve the most secure configuration. However these are nice to haves and may not be feasible in the real world. Management may deem certain secure configurations to not be cost effective and thus may purposely omit them. The cost may not only relate to monetary terms but also to inefficiencies created by poor response times due to a particular configuration. The auditor must however, make certain that the omission of certain secure configurations are commensurate with the purpose and the risk associated with the Solaris server in question.

The most important item to ascertain before applying the checklist is the purpose of the server. What the server is used for directly affects how you would apply this checklist. Where possible we have indicated the controls where the purpose of the server is necessary to determine the most secure configuration e.g. The purpose of the server is important to determine what services are to be commented out in the inetd.conf file

Checklist

No.	Control
1.	Ascertain whether the latest patches of the operating system is installed. Determine procedures to update the patches: • If downloaded ascertain if downloaded from a secure site • Ascertain if patches are updated whenever there is a new vulnerability • Determine if the patch is tested in a test environment before being rolled out to the live environment • Ascertain whether the minimum core software is installed to reduce exploits.
2.	Ascertain the amount of space allocated to the various partitions. The amount of space allocated depends on the purpose of the server e.g. A logging server would have more space allocated to /var. /opt and /usr – application installation / - root partition

No.	Control
3.	Removing unnecessary services: Review the inetd.conf file to ascertain what services are enabled. Services are disabled by the pound sign (#) in front of the line. Again the auditor needs to ascertain the purpose of the server prior to ascertaining whether the necessary services have in fact been commented out. Depending on the function of the server comment out the following services: • ftp • tftp • systat • rexd • ypupdated • netstat • rstatd • rusersd • sprayd • walld • exec • talk • comsat • rquotad • name • uucp • telnet • imap • pop3 • dtspc • fs • kcms • all rpc services • sadmind • login • finger • chargen • echo • time • daytime • discard
4.	Startup scripts Review the /etc/rc2.d and /etc/rc3.d files to ensure that unnecessary startup scripts have been stopped from running (lowercase k or s stops a script). Again depending on the role ofthe server the following should be stopped: • automounter /etc/rc2.d/S74autofs • Sendmail /etc/rc2.d/S88sendmail and /etc/rc1.d/K57sendamil • RPC /etc/rc2.d/ S71rpc • SNMP /etc/rc2.d/S76snmpdx • NFS server /etc/rc3.d/S15nfs.server • NFS client /etc/rc2/S73nfs.client

No.	Control
5.	Logging In environments with multiple Solaris boxes, ensure that there is a central logging/syslog server. Review the /etc/hosts file on both the host to be logged and the syslog server to ensure that it contains the correct entries to the correct syslog/host servers. If using a central syslog server to log remote machine incidents, ensure that the traffic sent to the syslog server is encrypted using ppp rpm Ensure that sufficient space has been allocated to the /var file if the server is a syslog server or even if there is only one server in the environment in which case logging is performed locally. Ensure that the following items are being logged: • SU attempts • Failed login attempts • Last command – who logged in, when and from where • System events Review the /etc/syslog.conf file to ensure that at a minimum error priorities and above are logged on all the facilities. Ensure that the permissions on the/var/adm/loginlog are 600 and are owned by root and groupsys. Ensure that appropriate monitors are in place to notify system administrators of unauthorised activities. Tools such as Swatch and Logcheck can be used for this purpose and can forward alerts via e-mail. Ensure that the permissions on utmp are set to –rw-r- - r- - . Verify the existence of the wtmp file by using the ls - la command. Ensure that the permissions on wtmp is set to 644. Ensure that the btmp files exist.
6.	SSH: Review the /etc/hosts.allow and /etc/hosts.deny files to ensure that the authorised relationships are established. Ensure that the .ssh/identity file has permissions of 600 and owned by root. Ensure that all r programs have been removed and ssh has been configured to replace r programs. Review security procedures to maintain the security of the passphrases at the server and workstations.
7.	TCPWrapper Review the /etc/hosts.allow file to ensure that it is configured to disallow everyone and then allows the authorised hosts. Determine the process to change rules in TCP Wrapper and whether tools like tcpdchk (check configuration and reports problems) and tcpdmatch (what happens when rules are deployed) are used. Ensure that a TCP Wrapper banner message has been created with the appropriate legal wording. Ensure that the –DPARANOID option is turned on. Ensure that TCP Wrapper has been configured to query the client's IDENT server. Ensure that the Makefile has been edited to include the -DKILL_IP_OPTIONS. Ensure that the permissions for all TCP Wrapper files are read, read and execute only access (modes 755 &555).

No.	Control
8.	Backups Ensure that backups are performed frequently. A review of the cron file should give an indication of the frequency of backups. Ensure that not only the file system and data is backed up but also the configuration files e.g. Inetd.conf. If a remote server is being backed, ensure that SSH(refer to 6 above) to secure the trust relationship between the local and the remote machine. Ensure that the backups are tested regularly via restore procedures to ensure that they have been written to the offline me dia correctly.
9.	In the event that TCPWrapper is not used, ensure that a warning has been created in /etc/issue file and that it has been added to /etc/motd file.
10.	Ascertain how often vulnerability analysis are run using tools like SATAN, SAINT, ASET, ESM Omniguard and ISS System scanner. Determine if fixes to the vulnerabilities have been implemented and whether they were tested on in a test environment prior to rolling put in the live environment.
11.	NFS Security Ensure that the most recent NFS patches are installed. Ensure that sensitive files are exported read only Ensure that file systems are exported to a restricted set of hosts Ensure that NFS is configured to only accept requests from privileged system programs Ensure that the file system is not exported to an exporting server or to a netgroup which includes the exporting server Ensure that there is no reference to localhost in /etc/exports file Ensure that exports are to fully qualified domain names to prevent spoofing.. Ensure that all suid code is kept on one filesystem and is exported with no root access. Ensure that all other filesystems are mounted with nosuid. Ensure that the satmon directories are not world writable Ensure that the portmap/rpcbind program does not forward mount requests Ensure that the NIS netgroup does not contain empty host fields (treated as wildcards and grant access to any host via mountd daemon). Ensure that TCP and UDP ports 2049(nfs) & 111(portmap) are blocked on routers and firewalls Ascertain what authentication service is being used. If it is the Diffie-Hellman AUTH_DH, review procedures for the protection of keys To aid in auditing the security of NFS the following tools can be used: • Showmount – displays filenames exported by a given host • SATAN – examine remote hosts by probing services like NFS. • NFSWatch – monitor NFS requests to any given machine or to the entire local network • NFS tracer – to monitor NFS traffic • NFSbug – test hosts for well known NFS problems/bugs.
12.	Sendmail Security Ensure that local routers and firewalls restrict access to TCP port 25. Ensure that the most recent patch of sendmail is installed. Review SmtpGreetingMessage to ensure that the SMTP login message omits version information. Ensure that the proper ownerships and file permissions are applied to sendmail binary, configuration file, sendmail scripts and other sendmail directories and files.

No.	Control
13.	NIS Security Ensure that the latest NIS patches are applied. Ensure the use of compatibility mode for NIS. Ensure that the netgroup enfo rcement has been implemented to restrict user access to systems. Ensure that access to NIS maps is restricted by /var/yp/securenets. Ensure that access to the portmap service is restricted by the use of versions of portmap and rpcbind that support TCPWrappers. Ensure that encrypted passwords from the NIS maps are hidden by installing shadowing through the use of passwd.adjunct.
14.	SETUID and SETGID Ensure that the setuid/setgid is removed for services which the system is not using e.g. for UUCP the following should be removed: • /usr/bin/ct – used for managing dial in sessions on /dev/tty allocated for UUCP dial outs • /usr/bin/cu – UUCP , modem line to call out to another system. • /usr/bin/uucp – unix to unix copy command. Not required unless for UUCP dial up networking. Ensure that a master list of authorised setuid and setgid is created and procedures are in place to check that there are no unauthorised changes.
15.	Ensure that IPForwarding disabled.
16.	Tripwire Ascertain which version of Tripwire is being used. If earlier than 2, ensure that the database is stored to an off line medium. If version 2, don't worry about the off line media storage of the database. Determine how often rpm is run to determine changes to files, and steps taken if there is an unauthorised change.
17.	Security management: If rdist is being used to tighten security on multiple Solaris servers, then ensure that SSH is installed to encrypt transfers. Ensure that the latest patches for rdist are installed.
18.	Miscellaneous Review the /etc/default/inetinit file to ensure that the TCP initial sequence number generation parameters are set to TCP_STRONG_ISS=2. Review the /etc/system file to ensure that the following two lines have been included to protect against buffer overflow attacks: • Set noexec_user_stack=1 • Set noexec_user_stack_log=1 Ensure that root can only access the console by reviewing the /etc/default/login file to ensure that CONSOLE=/dev/console/ is not commented out. Review the /etc/shadow file to ensure that the sys, uucp, nuucp, smtp, and listen accounts are disabled (disabled if there is a LK in the password field for these accounts. Ensure that the sendmail packages of SUNWsndmr and SUNWsndmu are removed. Ensure that the group write permission of the /etc directory file is removed. Ensure that routing has been disabled. Ensure that the /etc/hosts.equiv,/.rhosts are removed. Ensure that the Stop-A abort sequence is disabled by reviewing the /etc/default/kbd. (KEYBOARD_ABORT=DISABLED) Ensure that EEPROM security is enabled.
19.	Ensure that shadowing is enabled.

20.	Ensure that the password aging is at least 45 days. Account Policy - /etc/default/passwd file – password aging.
21.	Ensure that the following accounts are locked “LK” in the encrypted password field in the /etc/shadow file: • adm • bin • daemon • listen • lp • nobody • noaccess • nuucp • smtp • sys • uucp These login accounts should not have login shells, they should be set to /dev/null.
22.	

Last Updated: May 1st, 2024

Upcoming SANS Training

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

SANS Rome May 2024	Rome, IT	May 06, 2024 - May 11, 2024	Live Event
SANS Security West 2024	San Diego, CAUS	May 09, 2024 - May 14, 2024	Live Event
SANS Dubai May 2024	Dubai, AE	May 11, 2024 - May 16, 2024	Live Event
SANS ICS Europe 2024 Munich	Munich, DE	May 12, 2024 - May 18, 2024	Live Event
SANS Cloud Singapore 2024	Singapore, SG	May 13, 2024 - May 24, 2024	Live Event
SANS Doha May 2024	Doha, QA	May 18, 2024 - May 23, 2024	Live Event
SANS Amsterdam May 2024	Amsterdam, NL	May 20, 2024 - Jun 01, 2024	Live Event
SANS Leadership & Cloud Security - Crystal City 2024	Arlington, VAUS	May 20, 2024 - May 24, 2024	Live Event
SANS SEC530 Canberra 2024	Canberra, ACT, AU	May 27, 2024 - Jun 01, 2024	Live Event
SANS Cyber Defence Thailand 2024	Bangkok, TH	May 27, 2024 - Jun 01, 2024	Live Event
SANS Philippines SEC504 2024	Manila, PH	May 27, 2024 - Jun 01, 2024	Live Event
SANS Muscat June 2024	Muscat, OM	Jun 01, 2024 - Jun 06, 2024	Live Event
SANS Summer Dunes 2024	Riyadh, SA	Jun 01, 2024 - Jun 06, 2024	Live Event
SANS Munich June 2024	Munich, DE	Jun 03, 2024 - Jun 08, 2024	Live Event
SANS Miami 2024	Coral Gables, FLUS	Jun 03, 2024 - Jun 15, 2024	Live Event
SANS Madrid June 2024	Madrid, ES	Jun 10, 2024 - Jun 15, 2024	Live Event
SANS Paris June 2024	Paris, FR	Jun 10, 2024 - Jun 15, 2024	Live Event
SANS ICS Security Summit & Training 2024	Orlando, FLUS	Jun 16, 2024 - Jun 24, 2024	Live Event
SANS Warsaw June 2024	Warsaw, PL	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Tbilisi June 2024	Tbilisi, GE	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Rocky Mountain Summer 2024	Denver, COUS	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Cyber Defence Japan 2024	Tokyo, JP	Jun 17, 2024 - Jun 29, 2024	Live Event
SANS Zurich June 2024	Zurich, CH	Jun 24, 2024 - Jun 29, 2024	Live Event
SANS Cyber Defence Australia 2024	Canberra, ACT, AU	Jun 24, 2024 - Jul 06, 2024	Live Event
SANS San Antonio 2024	San Antonio, TXUS	Jun 24, 2024 - Jun 29, 2024	Live Event
SANS London July 2024	London, GB	Jul 01, 2024 - Jul 06, 2024	Live Event
SANS Amsterdam July 2024	Amsterdam, NL	Jul 15, 2024 - Jul 20, 2024	Live Event
SANSFIRE 2024	Washington, DCUS	Jul 15, 2024 - Jul 20, 2024	Live Event
SANS Pen Test Hackfest Europe Summit & Training - Amsterdam 2024	Amsterdam, NL	Jul 21, 2024 - Jul 27, 2024	Live Event
SANS Security Awareness: Managing Human Risk Summit 2024	Norfolk, VAUS	Jul 29, 2024 - Aug 02, 2024	Live Event
SANS Malaysia FOR508 2024	Kuala Lumpur, MY	Jul 29, 2024 - Aug 03, 2024	Live Event
SANS New York City Summer 2024	New York City, NYUS	Jul 29, 2024 - Aug 03, 2024	Live Event
SANS Autumn Australia 2024	OnlineAU	May 06, 2024 - May 11, 2024	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced