SECURITY REVIEW - UNIX PLATFORMS

TRACKING INFORMATION

Review Date:

System/DNS Name:

System Location:

IP Address(s) of System:

Hardware Type and OS Level:

System Administrator	Telephone Number	E-mail Address
System Administrator	Telephone Number	E-mail Address
System Administrator	Telephone Number	E-mail Address
Application Administrator	Telephone Number	E-Mail Address

Person(s) conducting review

Sysguard Installed, y or n

SecurID Installed, y or n

Trust Level

List area code and telephone numbers of any modems associated with system:

List names of applications running on this system:

(Instructions for completing a review follow the checklist)

SW908 Section	Security Area/Requirement	Yes	No
	TO BE COMPLETED BY THE SYSADMIN'S SUPERVISOR		
4.08	1. Security Admin Responsibilities: System security functions have been assigned and appropriately documented for System Administration, User Administration, etc. Tool: Job Description, Departmental Responsibility Agreement, etc.		
4.08	2. Security Admin Training: Security administrator has completed available training on security and platform requirements (SW908, UNIX System Administration, UNIX Security) Tool: Completed Training Records, Diplomas		
4.08	3. Security Admin Registration: System/Security Administrator is registered with the Corporate Information Systems sysadmin database representative, 314 235-3150. Tool: SW908 Appendix 1, Page 1		
5.01	4. Physical Access: Physical access to the system and its components are securely controlled. Tool: SW 007-590-905		
7.15	5. Trust Level Verification: The trust level of this system has been verified. Tool: SW 007-590-908, 7.15 through 7.17		
	6. Advisory Receipt: CERT (Computer Emergency Response Team), Bellcore, and Vendor security advisories are received on a regular basis.		
9.02	7. Contingency Plans: Recovery plans have been documented in application/site recovery manuals.		

SW908 Section	Security Area/Requirement	Yes	No
	TO BE COMPLETED BY THE SYSADMIN		
5.07	8. Software Backups: Backup process has been documented and reviewed for compliance. Tool: SW 007-590-904, OP47		
5.08	9. Authorizing Software: Any software resident on system has been authorized, appropriately licensed, and stored (security software source code stored off line).		
	10. Security Tools: Bellcore's SysGuard or other security monitoring tool(s), e.g. COPS, TIGER, etc. are installed on the system to provide ongoing detective controls.		
	11. Patch Application: All appropriate patches have been applied. Tool: See applicable platform specific appendix		
6.05	12. User Authorization: All non-administrative, non-application user ids are in the SUITS format (2 initials, last four numbers of the SSN). Official SUITS ID's are obtained from the PHONE data base. Tool: /etc/passwd PHONE SUITS		
6.06	13. Authorization: An authorized paper or electronic record of access allowance is available for each non-administrative, non-application user ID present in the password file. Tool: SW908, Appendix 11		
6.09	14. Validation: All non-administrative, non-application user ids are re-verified as an active employee or an authorized contractor on a monthly basis. Tool: get_phoneids, available from MASS representative Receipt of weekly employee deletion lists, available from 314 235-3032		
6.10	15. Deactivation: Valid user ids with no activity for 90 days are deactivated or deleted. Tool: pwexpire(Sysguard) lastlogin log		
6.05a	16. Uniqueness: User ids and UID numbers are unique. Tool: unique(Sysguard) pwdck		
6.05a	17. Uniqueness: Group ids and GID numbers are unique. Duplicated. Tool: groupck(Sysguard) grpck		
	18. Uniqueness: All users are assigned to a group that does		

SW908 Section	Security Area/Requirement	Yes	No
	not exceed the scope of their authority. Tool: groupck(Sysguard) grpck		
6.08	19. Sharing: User ids are not shared. If application requirements require the use of a single id by multiple personnel, a single individual has been designated as responsible for that account. Individuals using the group ID access the system with their personal ID and su to the group ID.		
	20. One-Time Password: SECURID is completely installed and operational. (Completely installed means both securid shell and secure ftp are installed and is being used by all non-administrative and non-application ID's).		
6.12	21. Password: Password complexity guidelines are followed (6-8 char, 1 special character and 1 numeric, no more than 2 sequential alphas or numerics in a row) Tool: trypw(Sysguard) passwd(Sysguard) npasswd(freeware)		
6.12a	22. Procedures have been implemented to periodically check the potential of an individual password being cracked. Tool: checker(Sysguard) Crack		
6.12b	23. The password field for each id in the password and/or shadow file is populated. A blank space does not exist in the password field of any ID. Tool: /etc/passwd loginck(Sysguard)		
6.13	24. Password Aging: Both minimum and maximum aging parameters have been set. Minimum aging is no less than 7 days and maximum aging is no greater than 30 days. Aging is not necessary if SecurID is fully installed and functional. Tool: pwexpire(Sysguard) Standard UNIX aging procedures		
6.14	25. Password Reuse: Security software, if installed, disallows reuse of a password for 6 months. Tool: passwd(Sysguard)		
6.15	26. If the operating system provides or allows it, password shadowing is used. Tool: pwconv(Sysguard) pwunconv(Sysguard) Standard UNIX shadowing		
6.15	27. The /etc/passwd file is owned by root and set to mode 444.		

SW908 Section	Security Area/Requirement	Yes	No
6.15	28. If utilized, the /etc/shadow file is owned by root and set to mode 400.		
6.12d	29. Clear text passwords are not imbedded in known connectivity scripts or programmed into the console's PF keys.		
6.21	30. Default Passwords: System installation or maintenance passwords supplied by vendors have been changed or disabled. Tool: checker(Sysguard)		
6.12f	31. The chsh and chfn commands are disabled or removed Tool: chmod 000 chsh chfn chown root chsh chfn		
	32. The rdist command has either been patched or had the suid bit removed. Tool: See applicable system specific appendix chmod u-s /usr/bin/rdist		
6.12e7	33. Privileged Logins: Most accounts with a UID number of less than 100 and are never used as login accounts (e.g. bin, sys, daemon) have been locked. Tool: /etc/passwd /etc/shadow		
6.17	34. Last Logon Information: Date and time of last login session is displayed to user after successful authentication.		
	35. ELM mailer: Versions of elm prior to 2.4 PL25 have several security vulnerabilities. Elm 2.4 PL25 is installed. Tool: elm -v		
5.06a	36. Directory and File Protection: Operating system directories and files are not readable or writable by anyone except authorized accounts. Tool: copstools(Sysguard) COPS		
5.06a	37. A permanent listing of critical files and directories, including SETUID/SETGID programs, containing recommended ownerships and permissions, is maintained and compared on a daily basis to existing system files. Tool: permck(Sysguard) look(Sysguard) tripwire		
5.06b	38. Duplicate system commands, such as login, etc., and unknown to the security administrator, do not reside outside of proper system directories. Tool: clash(Sysguard) find		
5.06c	39. Device files reside in the /dev, /devices directory. Disk,		

SW908 Section	Security Area/Requirement	Yes	No
	tape and network devices are owned by root and set to mode 600. Memory devices are not readable by others and owned by root and set to mode 440. Tool: find / \(-type c -o -type b \) -print | grep -v "^/dev/"		
5.06d	40. The network interface(s) are not in a promiscuous mode. Tool: cpm(CERT) for SUN 4.x ifconfig -a pfstat for ULTRIX lsof		
	41. Filenames containing special characters and thus hidden from the output of the ls command are found and investigated. Tool: find / \(-name " *" -o -name "..*" -o -name "*[!?^ -~]*" \) -print | cat -vt findHidden(Sysguard)		
	42. Files and directories without legitimate owners and groups are found and investigated. Tool: find / -nouser -o -nogroup -print findorphan		
5.06e	43. Crontab and at directories and files are not readable or writable by anyone other than the owner. Scripts and programs that run out of cron are checked for integrity. Tool: ls -l /usr/spool/cron/crontabs copstools(Sysguard)		
5.12a	44. Default Protection: The default system umask is set to 066 for new files and directories. Creation of files and directories restricts read and write access to the creator/owner of the file or directory. Tool: umaskck(Sysguard) umask		
5.12b	45. The default system PATH variable and any user's PATH does not list the current directory (: or .) prior to any system directories in the search path. Even better, the current directory is nowhere in the search path. Tool: pathck(Sysguard) find / -name *profile -print -exec grep PATH {} \;		
5.12c	46. The system default mesg(1) command is set to n.		
5.12d	47. The permissions of users home directories and files (especially .files) are not too wide open and have the proper owner and group. .forward files have been examined for potential trojan code. Tool: loginck(Sysguard) cut -d: -f6 /etc/passwd | xargs -i ls -ld {} {}/.profile find . -name .forward -exec cat {} \;		

SW908 Section	Security Area/Requirement	Yes	No
5.12a	48. Each user's "umask" is set to grant no more permission than what is necessary to "do the job". Tool: umaskck(Sysguard) find / -name *profile -print -exec grep -i umask {} \;		
6.03b	49. Procedures are utilized that audit the use or attempted use of switching user (su) to root. Tool: su(Sysguard) /usr/adm/sulog		
6.03c	50. Direct access to the root login is limited to the system console. Tool: scfmgr(Sysguard) "rootaccess" parameter /etc/ttytab /etc/securetty		
6.19	51. Concurrent Sessions: Simultaneous access by the SAME userid is only permitted for business needs. Each user is notified in real time that the id is in use. Tool: scfmgr(Sysguard) "concurrent sessions" parameter /etc/sw-limit-login		
6.22	52. Warning Message: The access warning banner is displayed at the point of initial entry. Tool: /etc/issue /etc/motd TCPWRAPPER telbanner		
6.23	53. Access Tracking: Invalid attempts to login to a system are logged and maintained for a minimum of 90 days. The system or security administrator reviews administrative reports or utilizes administrative tools to monitor user activities. Tool: auditlog(Sysguard) acctcom /var/spool/adm/messages		
6.25	54. Accounting process turned on Tool: /etc/rc adm's cron		
	55. /etc/utmp is owned by root and set to mode 644 Tool: ls -l /etc/utmp		
6.24	56. Terminating Logon Session: Following OP 113 standards in disconnecting session if invalid userid/password is used (e.g., after a maximum of 3 consecutive invalid attempts). Tool: login(Sysguard) scfmgr(Sysguard) MAXTRYS (/bin/login)		

SW908 Section	Security Area/Requirement	Yes	No
6.25	57. System Log: System logs and or reports (su logs, cron logs, uucp logs, accounting output, etc.)are reviewed regularly and protected from unauthorized access. Tool: audrep(Sysguard) acctcom(1)		
6.26a	58. SUIDPERL/SPERL: Any suidperl or sperl commands are found and the suid and sgid bits are removed. Tool: find / -xdev -type f -user root \(-name 'sperl[0-9], [0-9][0-9][0-9]' -o -name 'suidperl' \) -perm -04000 -print -ok chmod ug-s '{}' \; Installation of perl version 5.003		
7.01	59. Terminal Timeout: Terminals screen blank(passworded) and/or lock and disconnect after a reasonable (15 minutes) of inactivity. Tool: hangup(Sysguard)		
7.03	60. Single User Mode: A system that does not reside in a secure computer room or data center environment is password protected before access to the single user mode is given. Tool: rootpass(Sysguard)		
	61. UUCP Security: UUCP directories and files restrict access to authorized users and systems. Tool: uucpck(Sysguard)		
7.05a	62. The HoneyDanBer version of UUCP is running on the system.		
7.05b	63. Each system that is communicated with via uucp has a unique and distinct login ID and password.		
7.05c	64. The files /usr/lib/uucp/Systems and /usr/lib/uucp/Permissions are set to mode 400 and owned by uucp.		
7.05e	65. General access to files is restricted to /usr/spool/uucppublic. Tool: uucpck(Sysguard) uucheck -v		
7.07	66. FTP Security: All login names corresponding to the reserved user ids (1-100) reside in the file /etc/ftpusers and the file /etc/shells contains a list a valid system login shells.		
7.07d	67. The use of .netrc files is securely administered. The $HOME/.netrc file is owned by root or the $HOME owner and is set to mode 600. Tool: find . -name .netrc -exec ls -la {} \;		
7.07e	68. TFTP Security: The tftp function is commented out or is running in a secure mode. Inspect /etc/inetd.conf, /usr/etc/tlid.conf, /etc/rc.d or "system" equivalent for		

SW908 Section	Security Area/Requirement	Yes	No
	unauthorized additions or changes, such as entries that execute /bin/sh. Tool: /etc/inetd.conf CERT Advisory 91:18		
7.08	69. Trusted Host: The /etc/hosts.equiv file does not contain any hosts names or IP addresses that are not under your direct administrative control.		
7.08a	70. The file /etc/hosts.equiv is set to mode 400 and owned by root.		
7.08b	71. The file /etc/hosts.equiv does not contain any user names.		
7.08c	72. The file /etc/hosts.equiv does not contain a plus (+), minus (-), or pound (#) sign. Tool: rcmdck(Sysguard) CERT Advisory 91:12		
7.09	73. Trusted User: Administrative id's .rhosts do not contain any host names, IP addresses, or user ID's from systems that are not under your direct administrative control. Individual user's .rhosts are strictly limited and securely administered. No .rhosts file grants access to a user not previously authorized on this system or establishes a shared ID scenario. Tool: rcmdck(Sysguard) find / -name .rhosts -exec cat {} \;		
7.09b	74. The file $HOME/.rhosts is set to mode 400 and owned by the login id.		
7.10	75. Sendmail Security: If the system is running sendmail, the latest SWBT version*(8.8.4) has been obtained and applied. The files /etc/aliases or /usr/lib/aliases do not contain the "uudecode" alias. Tool: Latest freeware version "Eric Allman's" 8.8.5 Latest patch from bedrock, 8.8.x (314 235-3419) grep uudecode /etc/aliases CERT CA:95-08, 95:13, 96:20 and others		
7.11	76. NFS & NIS Security: Disk resources are not exported to the world but are restricted to limited and authorized systems. If necessary, a patched portmapper and/or rpcbind has been applied. Tool: showmount -e nfschk(Sysguard) CERT CA:94-15		
	77. TCP & UDP protocol Security: Rexd, finger, rusersd, rstatd, sprayd, uucp, routed, rwalld, rwhod, chargen, echo, etc. and other unnecessary and possibly insecure processes		

SW908 Section	Security Area/Requirement	Yes	No
	are not running. Only necessary protocols are being provided. Tool: rpcinfo -p		
7.21	78. Dial ups have been installed in accordance with OP118. Dial up passwords are in place to provide a second level of security.		
7.13	79. If this system is connected to the network and running TCP/IP, a program to wrap and log the TCP suite of protocols has been installed and is functional. Tool: TCP WRAPPER TAMU's netlog		
7.12	80. X-WINDOW: X services can not be obtained except by authorized clients and access control is enabled. The binary program xterm is not setuid or setgid and logging has been disabled. Tool: xhost xhost + <system name(s) xhost - ls -l <directory>/xterm Appendix 10-Securing X-Services		
7.12a	81. XDM: Direct root access from a X-terminal is disallowed by configuring the Xstartup file to deny direct root login capability, e.g. Tool: if [$USER = root] ; then exit 1 fi		
7.14	82. HTTPD: If a home page has been built using NCSA's HTTP daemon, it is version 1.5.2 or higher, or if APACHE's HTTP daemon, it is a version 1.1.2 or higher. The JAVA functionality of NetScape has been disabled. There are no interpreters, e.g., perl, sh, etc. located in the cgi-bin directory. The query strings in the scripts contained in the cgi-bin are loosely quoted, e.g., QUERY_STRING = "$QUERY_STRING" CONTENT_TYPE = "$CONTENT_TYPE" Tool: CIAC Security Advisory G-20 CERT Advisory 96:05 CERT Advisory 96:11		
	83. The "10-point" checklist which searches for known hacker activity or methods of operation has been performed on this system. Tool: SW908, Appendix 12		

1. REQUIREMENT FOR A REVIEW: To comply with OP113, SW 007-590-908 (SW908), Section 8, requires an annual review of each computer system's environment, hardware, software, operating procedures, and documentation. A proper review **SHOULD** provide direction on how to maintain and/or increase the level of information protection on a system and document current problems and concerns.

2. PERFORMING THE REVIEW: The annual review should be coordinated by the system administrator responsible for security administration; assisted by other Information Systems and client department personnel (e.g., Project Manager , User Administrator, etc.). SW908 defines these functions and jobs in Section 4. In most cases, a single checklist should be filled out for each system/complex.

3. ITEMS TO BE REVIEWED: The preceding pages include the SW908 requirements to be covered in each review (with a reference to SW908 under "SW908 Sect"), a brief summary expression (e.g., Sec Admin Responsibilities), a SW908 reference (e.g., [SW908 4.05-08]), and a brief description in terms of UNIX based operations. Any concerns or issues unique to a given application **MUST** be referred to the application's support staff for resolution. Perform the checklist by completing:

- TRACKING INFORMATION: Complete the Tracking Information form included as page 1 of Appendix 1.
- COMPLIANCE STATUS: the status of each question - "Yes" (in compliance) or "No" (not in compliance requires an explanation)
- ATTACHMENTS: Explanations for each "No" reply.

4. DOCUMENTING DEVIATIONS: Exceptions or deviations **MUST** be fully documented and resolved as soon as practicable (see SW908, Section 8.02). If a requirement is considered unnecessary, unreasonable, or not possible, review it with the Information Systems ISF representative. For significant exceptions, a written exception and plan for correction **MUST** be approved by the departmental division manager, retained for the life of the system (i.e., available for audit reviews), and a copy sent to the ISF Chairperson for review.

ISF Chairperson
Computer Security Administration Group
One Bell Center, Room 32-U-07
St. Louis, MO 63101