HOSTS Test Matrix

Audit Series

Test	Description	Status	Discussion
Sol-ADT-1	Verify user account auditing thru inspection of files and subdirectories.	Partial: Login failures must be performed manually.	
Sol-ADT-2	Verify protection of audit data and processes thru inspection of files and subdirectories.	Complete	
Sol-ADT-3	Verify notification to trusted user of audit process abnormal behavior thru inspection of files and subdirectories.	Partial: Interactive APM interface testing must be performed manually. In addition, reception of generated e-mail by a human must be verified.	
Sol-ADT-4	Verify control of auditable events thru inspection of files and subdirectories.	Complete	
Sol-ADT-5	Verify separation of audit roles/functions among trusted users thru inspection of files and	Partial: Interactive testing of APM interface.	

Discretionary Access Control (DAC) Series

Test	Description	Status	Discussion
Sol-DAC	Verify functionality of Solaris protection schema.	Complete	
Sol-DAC	Verify functionality of Solaris chown ownership alteration utility.	Complete	
Sol-DAC-1	Verify controlling access to objects.	Partial: Some GUI testing is specified	
Sol-DAC-2	Controlling user access through grouping.	Partial: Some GUI testing is specified	
Sol-DAC-3	Verify the system will automatically logoff user session during periods of inactivity and screen-lock user session during periods of inactivity.	Defer: Interactive Inactivity and Deadman Test	
Sol-DAC-4	Enforce the principle of least privilege.	Partial: Some APM GUI testing is required.	
Sol-DAC-4-1	Searching local system partitions for world write enabled files and	Complete	
Sol-DAC-4-2	Searching local system partitions for SetUID and SetGID files and	Complete	
Sol-DAC-4-3	Searching local system partitions for C-Shell scripts.	Complete	

Identification and Authentication (IA) Series

Test	Description	Status	Discussion
Sol-IA-1	Account management per established system security policy parameters.	Partial: APM interface testing of account creation must be performed manually.	
Sol-IA-2	Password management per system security policy.	Partial: APM interface and interactive testing of password changing must be performed manually	
Sol-IA-3	Evaluate consecutive failed login attempts.	Partial: APM interface and interactive account lock-out testing must be performed manually.	
Sol-IA-4	User account management by a trusted user.	Partial: APM interface testing of account creation/modification/deletion must be performed manually.	

Miscellaneous (MISC) Series

Test	Description	Status	Discussion
Sol-Misc-1	Verify login banner is displayed and disallow an untrusted user access to authentication data.	Partial: GUI via observation.	
Sol-Misc-2	Verify the ability to control system processes exists.	Complete	
Sol-Misc-3	Verify unnecessary network services are disabled.	Complete	
Sol-Misc-4	Verify the COE kernel does not share any file systems by default.	Complete	
Sol-Misc-5	Verify object resuse as per C2 requirement.	Partial: See SunSHEILD documentation	

Operating System (OS) Series

Test	Description	Status	Discussion
Sol-OS-23	Verify the system provides an auditing function capable of acceptying application level audit logging requests and a standard audit format is provided for use in application level auditing.	Complete	
Sol-OS-24	Determine if an audit reduction capability exists. This capability can be either OS provided or an add-on product.	Complete	
Sol-OS-27	Verify the system provides a capability to archive audit data.	Complete	
Sol-OS-31	Verify Sendmail is configured to not allow piping into programs.	Complete	
Sol-OS-43	Verify .netrc files are disallowed (e.g., file not found in user home directory).	Complete	
Sol-OS-57	Verify the home directories and startup files for root and privileged user accounts are sufficiently protected. Also verify that the kernel Common Data Store files are adequately protected.	Complete	
Sol-OS-60	Verify the system is capable of restricting access to input/output (I/O) devices, such as floppy disks and tape drives, and the capability to specify which users may access I/O devices.	Complete	
Sol-OS-61	Verify the admind daemon is configured to use the correct security level.	Complete	

Operating System (OS) Series (Continued)

Test	Description	Status	Discussion
Sol-OS-65	Verify users cannot access functions, screens, or other objects for which authorization or access has not been granted, and that a user is permitted to grant or revoke access to an object only if the user has control permission to that object.	Complete	
Sol-OS-81	Verify the shell used on the system resets the Internal Field Seperator (IFS) when invoked.	Complete	
Sol-OS-86	Verify the system provides controls to limit the propagation of access rights (e.g., determine if users can give away files, and if so, if they can give away an SUID file to root).	Complete	
Sol-OS-88	Verify that all Berkeley R commands for R services that are disabled in the kernel have been restricted.	Complete	
Sol-OS-94	Verify the system provides the capability to selectively encrypt and decrypt data and files.	Complete	
Sol-OS-96	Verify the system provides the capability for a trusted user to monitor and analyze the configuration of the host.	Complete: Items tested may depend on software installed.	
Sol-OS-97	Verify I&A mechanisms are configured for secure operation.	Partial: login process checks must be performed manually.	
Sol-OS-98	Verify there are no accounts on the system that have not been used within a reasonable amount of time (e.g., one month).	Complete	

Operating System (OS) Series (Continued)

Test	Description	Status	Discussion
Sol-OS-106	Verify the installation provided UsewrIDs do not have the default password.	Defer: CRACK Utility.	
Sol-OS-117	Verify the appropriate entries are in the /etc/dfs/dfstab file under Solaris.	Partial: NFS server configuration will require additional human review of export definition files.	
Sol-OS-120	Verify NFS port monitoring is properly configured.	Complete	
Sol-OS-121	Verify that regular accounts do not have administrator priviliges.	Complete	
Sol-OS-122	Verify that the keyboard, mouse, console and audio devices are owned by user logged in.	Complete	
Sol-OS-129	Verify cron has been securely configured. Determine which form of cron is used on the system.	Partial: Defer executable tests to TIGER.	
Sol-OS-143	Determine if any development tools exist on the system. Verify that development tools such as compilers, linkers and debuggers are adequately protected and can only be accessed by authorized users.	Complete	
Sol-OS-151	Verify that the Solaris Basic Security Module and auditing have been enabled.	Complete	
Sol-OS-158	Verify the user environment is configured properly.	Complete	
Sol-OS-160	Verify the user is always prompted for a password when telneting into the host machine.	Complete	
Sol-OS-176	Verify HTTP client and server processes are not being run as root.	Complete	

Operating System (OS) Series (Continued)

Test	Description	Status	Discussion
Sol-OS-179	Verify the systems listed in xhosts are appropriate. Determine what release of X is used on the system.	Complete	
Sol-OS-183	Verify the system uses xauth mechanism for X server access control instead of the xhosts mechanism.	Complete	
Sol-OS-184	erify the single user boot or system firmware password is set, and the system is configured such that a password must be entered to boot to a single-user state.	Complete	
Sol-OS-189	Verify the system supports trusted facility management via segregation of authorized roles, requires users to reauthenticate prior to accessing a trustred role, supports sharing and dynamic assignment of role commands, and a GUI.	Defer: APM test via GUI.	
Sol-OS-260	Verify that permissions on the backup program(s) are set correctly.	Complete	
Sol-OS-271	Verify that the Operating System was designed to satisfy C2 level of trust as defined by the TCSEC.	Partial: Review of documentation / certification is also required.	
Sol-OS-271	Examining local partitions for files and directories with unassigned/unknown UID/GID values.	Complete	
Sol-OS-271	Examining local partitions for files and directories with suspicious names.	Complete	
Sol-OS-281	Verify that the crash program permissions are set correctly.	Complete	

Operating System (OS) Series (Continued)

Test	Description	Status	Discussion
Sol-OS-290	Verify that IP source routing has been disabled.	Complete	
Sol-OS-295	Verify that only appropriate envgironmental variable are set at system boot time.	Complete	
Sol-OS-306	Determine if the capability to generate reports of audit data is provided, and if the reports can be based on fields of event records or Boolean combinations of those fields, or on ranges of the system date and time that audit records were collected.	Complete	