Security Auditor

ADMINUX®

AdminUX accepts the status quo when installed and monitors changes to the status quo. This provides a healthy intrusion detection system. The daily security diary records changes to the system that may be of concern from the point of view of security.

The purpose of the AdminUX Security Auditor component is to compare the status quo on the system to industry standards and the operating system recommendations. Based upon this analysis, Security Auditor will suggest changes to improve the system's security.

The Security Auditor can be run on demand or can be configured to run on a regular schedule. The results of the audit will appear in the daily security diary.

The following is the list of audits performed. Any item or sub-item can be configured to be ignored. The fact that they are being ignored will appear in the daily security diary.

PASSWORD

- All users must have a password
- All passwords, except root's password, must be aged
- Report anomalies in "/etc/passwd":
  - Root entry is not the first entry
  - Duplicate logins
  - Duplicate UIDs
  - Login name is greater than 8 characters
  - Login name begins with a pound character ("#")
  - Contains a password (not allowed in /etc/passwd)
  - Group ID not in /etc/group
  - Invalid home directory
  - Invalid shell
  - Unexpected value for shell
  - Shell is Set UID
  - Shell is Set GID
  - Invalid number of fields
- Regular users cannot belong to GIDs 0-99
- System users must be in "/etc/ftpusers" ("anonymous" and "ftp" are exceptions)

SECURETTY

- Direct "root" login (UID = 0) is restricted to the physical console
- UIDs 1-99 (system users) are not allowed to log in

FILES

- "/tmp", "/usr/tmp", and "/var/tmp" directories must have sticky bit ("t") set
- Compares file access (owner, group, and permissions) to an industry standard access list and report files with different access.

SERVICES

- The following TCP and UDP services should be disabled:

bootps	chargen	daytime
discard	echo	finger
ftp	gopher	httpd
imap	link	linuxconf
named	netstat	ntalk
pop	rexec	rlogin
rshell	rusers	ststat
talk	tftp	time
uucp	xmd	

PAM

Pluggable Authentication Modules (PAM) are not part of some UNIX operating systems and will ignored.

- The use of the auth module "pam_permit" is not allowed
- The file "/etc/pam.d/other" must deny all authorizations.

RHOSTS

- List all .rhosts on the system

USER

- List all inactive users that can be removed.

SU

- Report where the list of all su attempts is stored.

WORLD

- Report where the list of all world writeable files is stored.

SUID

- Report where the list of all SUID files is stored.

SGID

- Report where the list of all SGID files is stored.