NAME

aset – monitors or restricts accesses to system files and directories

SYNOPSIS

aset [**–p**] [**–d** *aset_dir*] [**–l** *sec_level*] [**–n** *user@host*] [**–u** *userlist_file*]

DESCRIPTION

The Automated Security Enhancement Tool (ASET) is a set of administrative utilities that can improve system security by allowing the system administrators to check the settings of system files, including both the attributes (permissions, ownership, etc.) and the contents of the system files. It warns the users of potential security problems and, where appropriate, sets the system files automatically according to the security level specified.

The security level for **aset** can be specified by setting the **–l** command line option or the **ASETSECLEVEL** environment variable to be one of 3 values: **low**, **med**, or **high**. All the functionality operates based on the value of the security level.

At the **low** level, **aset** does not alter any system behavior. It merely performs a number of checks and reports any potential security weaknesses.

At the **med** level, **aset** modifies some of the settings of system files and parameters, thus restricting system access, to reduce the risks from security attacks. Again it will report the security weaknesses and the modifications performed to restrict access. This does not affect the operations of system services. All the system applications and commands will maintain all of their original functionality.

At the **high** level, further restrictions are made to system access, rendering a very defensive system. Security practices which are not normally required are included. Many system files and parameters settings are modified to minimum access permissions. At this level, security is the foremost concern, higher than any other considerations that affect system behavior. The vast majority of system applications and commands will maintain their functionality, although there may be a few that exhibit behaviors that are not familiar in normal system environment.

More exact definitions of these levels (what exactly **aset** will do at each level) can be found in the administrator manual. The **asetenv**(4) file and the *master files* (see **asetmasters**(4)) determine to a large extent what **aset** performs at each level, and can be used by the experienced administrators to redefine the definitions of the levels to suit their particular needs. These files are provided by default to fit most security conscious environments and in most cases provide adequate security safeguards without modification. They are, however, designed in a way that can be easily edited by experienced administrators with specific needs.

aset can be periodically activated at the specified security level with default definitions using the **–p** option. **aset** will be automatically activated at a frequency specified by the administrator starting from a designated future time (see **asetenv**(4)). Without the **–p** option, **aset** will operate only once immediately.

OPTIONS

−p Schedule **aset** to be executed periodically. This adds an entry for **aset** in the **/etc/crontab** file. The **PERIODIC_SCHEDULE** environment variable in the **/usr/aset/asetenv** file is used to define the time for execution. See **crontab**(1) and **asetenv**(4). If a **crontab**(1) entry for **aset** already exists, a warning is produced in the execution log.

−d *aset_dir* Specify a working directory other than **/usr/aset** for ASET. **/usr/aset** is the default working directory. It is where ASET is installed, and is the *root* directory of all ASET utilities and data files. If another directory is to be used as the ASET working directory you can either define it with the −**d** option, or by setting the **ASETDIR** environment variable before invoking **aset**. The command line option, if specified, overwrites the environment variable.

−l *sec_level* Specify a security level (**low**, **med**, or **high**) for **aset** to operate at. The default level is **low**. Each security level is explained in detail above. The level can also be specified by setting the **ASETSECLEVEL** environment variable before invoking **aset**. The command line option, if specified, overwrites the environment variable.

−n *user@host* Notify *user* at machine *host*. Send the output of **aset** to *user* through e-mail. If this option is not specified, the output is sent to the standard output. Note that this is not the reports of ASET, but rather an execution log including error messages if there are any. This output is typically fairly brief. The actual reports of ASET are found in the **/usr/aset/reports/latest** directory. See the −**d** option.

−u *userlist_file* Specify a file containing a list of users. **aset** will perform environment checks (for example, **UMASK** and **PATH** variables) on these users. By default, **aset** only checks for **root**. *userlist_file* is an ASCII text file. Each entry in the file is a line that contains only one user name (login name).

USAGE

The following paragraphs discuss the features provided by ASET. Hereafter, each feature is referred to as a *task*. The first task, **tune**, is intended to be executed only once per installation of ASET. The other tasks are intended to be executed periodically at the specified frequency.

tune Task

This task is used to tighten system file permissions. In standard releases, system files or directories have permissions defined to maximize open information sharing. In a more security conscious environment, the administrator may want to redefine these permission settings to more restrictive values. **aset** allows resetting of these permissions, based on the specified security level. Generally, at the low level the permissions are set to what they should be as released. At the medium level the permissions are tightened to ensure reasonable security that is adequate for most environments. At the high level they are further tightened to very restrictive access. The system files affected and the respective restrictions at different levels are configurable, using the **tune.low**, **tune.med**, and **tune.high** files. See **asetmasters**(4).

cklist Task

System directories that contain relatively static files (that is, their contents and attributes do not change frequently) are examined and compared with a master description file. The **/usr/aset/masters/cklist.***level* files are automatically generated the first time the **cklist** task is executed. See **asetenv**(4). Any discrepancy found is reported. The directories and files are compared based on the following:

- owner and group
- permission bits
- size and checksum (if file)
- number of links
- last modification time

The lists of directories to check are defined in **asetenv**(4), based on the specified security level, and are configurable using the **CKLISTPATH_LOW**, **CKLISTPATH_MED**, and **CKLISTPATH_HIGH** environment variables. Typically, the lower level lists are subsets of the higher level lists.

usrgrp Task

aset checks the consistency and integrity of user accounts and groups as defined in the **passwd** and **group** databases, respectively. Any potential problems are reported. Potential problems for the **passwd** file include:

- **passwd** file entries are not in the correct format.
- User accounts without a password.
- Duplicate user names.
- Duplicate user IDs. Duplicate user IDs are reported unless allowed by the **uid_alias** file. See **asetmasters**(4)).
- Invalid login directories.
- If C2 is enabled, check C2 hidden **passwd** format.

Potential problems for the group file include:

- Group file entries not in the right format.
- Duplicate group names.
- Duplicate group IDs.
- Null group passwords.

aset checks the local **passwd** file. If the **YPCHECK** environment variable is set to **true**, **aset** also checks the NIS **passwd** files. See **asetenv**(4). Problems in the NIS passwd file are only reported and not corrected automatically. The checking is done for all three security levels except where noted.

sysconf Task

aset checks various system configuration tables, most of which are in the **/etc** directory. **aset** checks and makes appropriate corrections for each system table at all three levels except where noted. The following discussion assumes familiarity with the various system tables. See the manual pages for these tables for further details.

The operations for each system table are:

/etc/hosts.equiv
The default file contains a single "+" line, thus making every known host a trusted host, which is not advised for system security. **aset** performs the following operations:

Low Warns the administrators about the "+" line.

Medium
High Warns about and deletes that entry.

/etc/inetd.conf
The following entries for system daemons are checked for possible weaknesses.

tftp(1) does not do any authentication. **aset** ensures that **in.tftpd**(1M) is started in the right directory on the server and is not running on clients. At the low level, it gives warnings if the mentioned condition is not true. At the medium and high levels it gives warnings, and changes (if necessary) the **in.tftpd** entry to include the −**s /tftpboot** option after ensuring the directory **/tftpboot** exists.

ps(1) and **netstat**(1M) provide valuable information to potential system crackers. These are disabled when **aset** is executed at a high security level.

rexd is also known to have poor authentication mechanism. **aset** disables **rexd** for medium and high security levels by commenting out this entry. If **rexd** is activated with the −**s** (secure RPC) option, it is not disabled.

/etc/aliases
The decode alias of UUCP is a potential security weakness. **aset** disables the alias for medium and high security levels by commenting out this entry.

/etc/default/login
The **CONSOLE=** line is checked to allow root login only at a specific terminal depending on the security level:

Low No action taken.

Medium
High Adds the following line to the file:
CONSOLE=/dev/console

/etc/vfstab
aset checks for world-readable or writeable device files for mounted file systems.

/etc/dfs/dfstab
aset checks for file systems that are exported without any restrictions.

/etc/ftpusers	At high security level, **aset** ensures **root** is in **/etc/ftpusers** (create if necessary), thus disallowing **ftp**(1) to be used as root.
/var/adm/utmp **/var/adm/utmpx**	**aset** makes these files not world-writeable for the high level (some applications may not run properly with this setting.)
/.rhosts	The usage of a **.rhosts** file for the entire system is not advised. **aset** gives warnings for the low level and moves it to **/.rhosts.bak** for levels medium and high.

env Task

aset checks critical environment variables for **root** and users specified with the **−u** *userlist_file* option by parsing the **/.profile**, **/.login**, and **/.cshrc** files. This task checks the **PATH** variable to ensure that it does not contain '**.**' as a directory, which makes an easy target for *trojan horse* attacks. It also checks that the directories in the **PATH** variable are not world-writeable. Furthermore, it checks the **UMASK** variable to ensure files are not created as readable or writeable by world. Any problems found by these checks are reported.

eeprom Task

Newer versions of the EEPROM allow specification of a **secure** parameter. See **eeprom**(1M). **aset** recommends that the administrator sets the parameter to **command** for the medium level and to **full** for the high level. It gives warnings if it detects the parameter is not set adequately.

firewall Task

At the high security level, **aset** takes proper measures such that the system can be safely used as a firewall in a network. This mainly involves disabling IP packets forwarding and making routing information invisible. Firewalling provides protection against external access to the network.

ENVIRONMENT

ASETDIR	Specify ASET's working directory. Defaults to **/usr/aset**.
ASETSECLEVEL	Specify ASET's security level. Defaults to **low**.
TASKS	Specify the tasks to be executed by **aset**. Defaults to **all tasks**.

FILES

/usr/aset/reports	directory of ASET reports

SEE ALSO

crontab(1), **ftp**(1), **ps**(1), **tftp**(1), **eeprom**(1M), **in.tftpd**(1M), **netstat**(1M), **asetenv**(4), **asetmasters**(4)

System Administration Guide, Volume I