Table of co

7.9.

PDF

7.9.1. C

The aud or disable auditing of TTY input for specified users. When the audited user logs in, `pam_tty_audit` records the exact keystrokes the user makes into the `/var/log/audit/audit.log` file. The module works with the `auditd` daemon, so make sure it is enabled before configuring `pam_tty_audit`. See Section 7.4, "Starting the `audit` Service" for more information.

When you want to specify user names for TTY auditing, modify the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` files using the `disable` and `enable` options in the following format:

```
session required pam_tty_audit.so disable=username,username2 enable=username
```

You can specify one or more user names separated by commas in the options. Any `disable` or `enable` option overrides the previous opposite option which matches the same user name. When TTY auditing is enabled, it is inherited by all processes started by that user. In particular, daemons restarted by a user will still have TTY auditing enabled, and will audit TTY input even by other users,

unless auditing for these users is explicitly disabled. Therefore, it is recommended to use `disable=*` as the first option for most daemons using PAM.

Important

By default, `pam_tty_audit` does **NOT** log keystrokes when the TTY is in password entry mode. Logging can be re-enabled by adding the `log_passwd` option along with the other options in the following way:

```
session required pam_tty_audit.so disable=username,username2 enable=username log_passwd
```

When you enable the module, the input is logged in the `/var/log/audit/audit.log` file, written by the `auditd` daemon. Note that the input is not logged immediately, because TTY auditing first stores the keystrokes in a buffer and writes the record periodically, or once the audited user logs out. The `audit.log` file contains *all* keystrokes entered by the specified user, including backspaces, delete and return keys, the control key and others. Although the contents of `audit.log` are human-readable it might be easier to use the **aureport** utility, which provides a TTY report in a format which is easy to read. You can use the following command as root:

```
~]# aureport --tty
```

The following is an example of how to configure `pam_tty_audit` to track the actions of the `root` user across all terminals and then review the input.

Example 7.8. Configuring pam_tty_audit to log root actions

Enter the following line in the `session` section of the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` files:

```
session    required     pam_tty_audit.so disable=* enable=root
```

Use the `aureport --tty` command to view the log. If the `root` user has logged in a TTY console at around 11:00 o'clock and tried to issue the `pwd` command, but then deleted it and issued `ls` instead, the report will look like this:

```
~]# aureport --tty -ts today | tail
40. 08/28/2014 11:00:27 901 0 ? 76 bash "pwd",<backspace>,<backspace><backspace>,"ls",<ret>
41. 08/28/2014 11:00:29 903 0 ? 76 bash <^D>
```

For more information, see the `pam_tty_audit(8)` manual page.

Previous

Next