NAME

sudoreplay — replay sudo session logs

SYNOPSIS

sudoreplay [**-h**] [**-d** *dir*] [**-f** *filter*] [**-m** *num*] [**-s** *num*] ID

sudoreplay [**-h**] [**-d** *dir*] **-l** [search e xpression]

DESCRIPTION

sudoreplay plays back or lists the output logs created by **sudo**. When replaying,**sudoreplay** can play the session back in real-time, or the playback speed may be adjusted (faster or slower) based on the command line options.

The *ID* should either be a six character sequence of digits and upper case letters, e.g. `0100A5`, or a pattern matching the *iolog_file* option in the *sudoers* file. When a command is run via **sudo** with *log_output* enabled in the *sudoers* file, a `TSID=ID` string is logged via syslog or to the **sudo** log file. The *ID* may also be determined using **sudoreplay**'s list mode.

In list mode, **sudoreplay** can be used to find the ID of a session based on a number of criteria such as the user, tty or command run.

In replay mode, if the standard output has not been redirected, **sudoreplay** will act on the following keys:

'`\n`' or '`\r`' Skip to the next replay event; useful for long pauses.