Руководство пользователя KDE su

Geert Jansen
Перевод на русский язык: Екатерина Пыжова
Перевод на русский язык: Олеся Герасименко
Рецензирование: Александр Яворский

Руководство пользователя KDE su

Оглавление

Аннотация

KDE su представляет собой графическую оболочку к UNIX®-команде **su**.

Глава 1

Введение

Добро пожаловать в KDE su! Эта программа представляет собой графическую оболочку к UNIX®-команде **su** для среды KDE. Позволяет запустить программу от имени другого пользователя при условии ввода пароля этого пользователя. KDE su — непривилегированная программа, она использует системную команду **su**.

KDE su предоставляет ещё одну дополнительную возможность — запоминание паролей. При использовании этой функции необходимо всего один раз ввести пароль для каждой команды. Подробные сведения и анализ безопасности: Раздел 3.4.

Программа предназначена для запуска из командной строки или файлов `.desktop`. Она запрашивает пароль пользователя `root`, используя графический интерфейс, но она, скорее, основана на слиянии командной строки и графического интерфейса, а не исключительно на графическом интерфейсе.

Так команда **kdesu** теперь установлена не в `$(kf5-config --prefix)`/bin, а в `kf5-config --path libexec`, следовательно, не в переменной среды `Path`, для запуска этой команды необходимо использовать `$(kf5-config --path libexec)kdesu`.

Глава 2

Использование KDE su

Использовать KDE su просто. Синтаксис следующий:

`kdesu` [`-c` *команда*] [`-d`] [`-f` *файл*] [`-i` *имя значка*] [`-n`] [`-p` *priority*] [`-r`] [`-s`] [`-t`] [`-u` *пользователь*] [`--noignorebutton`] [`--attach` *winid*]

`kdesu` [Типовые параметры KDE] [Типовые параметры Qt™]

Параметры командной строки описаны ниже.

`-c команда`

Этот параметр позволяет указать команду для запуска с правами root. Это должен быть один аргумент. Поэтому, если требуется запустить новый диспетчер файлов, следует ввести следующее: `$(kf5-config --path libexec)kdesu -c Dolphin`

`-d`

Этот параметр позволяет выводить информацию для отладки.

`-f файл`

Этот параметр позволяет эффективно использовать KDE su в файлах `.desktop`. При этом KDE su проверяет *файл*. Если он доступен для записи текущему пользователю, то KDE su запустит команду с правами этого пользователя. Иначе команда будет запущена с правами пользователя *пользователь* (root по умолчанию).

Параметр *файл* анализируется следующим образом: если он начинается с `/` , то считается абсолютным путем. Иначе — именем глобального файла конфигурации KDE.

`-i` *имя значка*

Этот параметр позволяет указать значок, который следует показывать в окне ввода пароля. Расширение указывать не обязательно.

Например, чтобы запустить браузер Konqueror в режиме диспетчера файлов и показать значок Konqueror в окне ввода пароля:

```
$(kf5-config --path libexec)kdesu  -i konqueror
-c "konqueror --profile filemanagement"
```

`-n`

Этот параметр отключает сохранение пароля. Он делает недоступным флажок **Сохранить пароль** в окне ввода пароля.

`-p` *приоритет*

Этот параметр задаёт значение приоритета. Приоритет — это любое число от 0 до 100, где 100 означает наивысший приоритет, а 0 — низший. По умолчанию: 50.

`-r`

Этот параметр задаёт использование приоритета реального времени.

`-s`

Этот параметр останавливает управляющую программу kdesu. Подробные сведения: Раздел 3.4.

`-t`

Этот параметр позволяет включить терминальный вывод, что делает невозможным запоминание паролей. Эта возможность в основном предназначена для отладки. Если требуется запустить обычное консольное приложение, используйте стандартную команду **sù**.

`-u` *`пользователь`*

Чаще всего этот параметр используется в KDE su для запуска команды от имени суперпользователя, но также можно ввести любое имя пользователя и соответствующий пароль.

Глава 3

Внутренние особенности

3.1 Авторизация X

Запускаемая программа будет работать с идентификатором пользователя root и, в общем случае, не будет иметь прав для доступа к X-дисплею. KDE su исправляет это, добавляя авторизационный cookie для дисплея во временный файл `.Xauthority`. После завершения команды файл удаляется.

Если система X cookie не используется, это будет обнаружено KDE su и новый cookie не будет добавлен, но в этом случае будет необходимо убедиться, что для пользователя root разрешён доступ к дисплею.

3.2 Взаимодействие с su

KDE su использует системную команду **su**, чтобы получить привилегированный доступ. В этом разделе подробно объясняется то, как KDE su это делает.

Так как некоторые реализации команды **su** (например, в Red Hat®) не позволяют вводить пароль, используя `stdin`, KDE su создаёт пару терминалов pty/tty и запускает **su** с его стандартными файловыми дескрипторами, настроенными на такой tty.

Чтобы выполнить программу, которую выбрал пользователь, а не запустить оболочку интерактивно, для команды **su** используется аргумент `-c`. Этот аргумент понимается всеми оболочками, соответственно, он должен быть переносимым. Команда **su** передаёт аргумент `-c` оболочке пользователя, которая и запускает программу на исполнение. Пример: **su** `root -c программа`.

Вместо прямого запуска команды пользователя через **su**, KDE su запускает небольшую программу, называемую kdesu_stub. Она (запущенная с правами требуемого пользователя) запрашивает определённую информацию от KDE su через канал pty/tty (stdin и stdout для этой программы), а затем уже выполняет программу пользователя. Передаваемая информация: номер X-дисплея, авторизационный X cookie (если доступен), переменная `PATH` и команда для запуска. Такая вспомогательная программа нужна, потому что X cookie содержит секретную информацию и поэтому не может быть передан в командной строке.

3.3 Проверка пароля

KDE su проверяет введённый пароль и выдаёт сообщение об ошибке, если он не верен. Проверка организована с помощью выполнения программы-теста `/bin/true`. Если проверка пройдена успешно, пароль считается правильным.

3.4 Хранение паролей

Для удобства пользователя в KDE su реализован механизм хранения паролей. В этом разделе освещены вопросы безопасности.

Запоминание паролей в KDE su создаёт небольшую брешь в системе безопасности. Очевидно, что KDE su позволяет пользоваться этими паролями только пользователю с вашим идентификатором. Но если это реализовать без предосторожностей, системный уровень безопасности `root` понизится до уровня обычного пользователя (вас). И человек, который получит доступ к вашей учётной записи, получит доступ уровня `root`. KDE su пытается не допустить этого. Схема безопасности, используемая программой, обеспечивает достаточный уровень безопасности. Описание этой схемы приведено далее.

KDE su использует управляющую программу, которая называется kdesud. Эта управляющая программа ожидает команды с UNIX®-сокета, расположенного в `/tmp`. Режим его доступа равен 0600, то есть только пользователь с вашим идентификатором может соединиться с ним. Если хранение паролей включено, KDE su выполняет команды через эту управляющую программу. Программа пишет команды и пароль пользователя `root` в сокет, и управляющая программа выполняет команду **su**, как описано выше. После этого команда и пароль не удаляются, а хранятся в течение указанного времени (устанавливается в модуле настройки). Если другой запрос на запуск такой же команды приходит в течение этого периода времени, клиент может не предоставлять пароль. Чтобы не дать человеку, получившему доступ к вашей учётной записи, украсть у управляющей программы пароль (например, запуском отладчика), длясgid сервиса (группа при запуске) установлено значение nogroup. Это не даёт обычным пользователям, в том числе и вам, получать пароли от процесса kdesud. Также эта управляющая программа устанавливает переменную окружения `DISPLAY` в значение при запуске. Всё, что сможет сделать взломщик, — это запустить на вашем дисплее приложение.

Слабое место в этой схеме в том, что запускаемые программы могут быть написаны без соблюдения правил защиты (например, программы с setuid `root`). Это означает, что они могут вызвать переполнение буферов или другие проблемы, а взломщик может использовать это.

Использование хранения паролей — это компромисс между безопасностью и удобством. Подумайте и определите, что имеет приоритетное значение, и, соответственно, следует ли пользоваться этой возможностью программы.

Глава 4

Автор

KDE su

Программа KDE su написана Geert Jansen. Она частично основана на KDE su, версии 0.3, написанной Pietro Iglio. По договорённости между авторами дальнейшую поддержку этой программы будет выполнять Geert Jansen.

С автором можно связаться по адресу g.t.jansen@stud.tue.nl. Пожалуйста, сообщайте о всех встреченных ошибках, чтобы автор мог их исправить. Также приветствуются любые предложения и комментарии.

Олеся Герасименкоgammaray@basealt.ru