Підручник KDE su

Geert Jansen
Переклад українською: Юрій Чорноіван

Підручник KDE su

Зміст

1 Вступ 5

2 Користування KDE su 6

3 Внутрішня частина роботи програми 8
- 3.1 Розпізнавання користувача у X . . . 8
- 3.2 Інтерфейс su . . . 8
- 3.3 Перевірка паролів . . . 8
- 3.4 Зберігання паролів . . . 9

4 Автор 10

Анотація

KDE su — це графічна оболонка до команди UNIX® su.

Розділ 1

Вступ

Ласкаво просимо до KDE su! KDE su — це графічний інтерфейс до команди UNIX® su для стільничного середовища KDE. Ця програма надає вам змогу виконувати команди від імені іншого користувача, якщо вам відомий пароль цього користувача. KDE su не є привілейованою командою (не запускається з підвищеними правами доступу) — для своєї роботи вона використовує права системної команди su.

KDE su має одну додаткову можливість: за вашого бажання, ця програма може запам'ятовувати введені вами паролі. Якщо ви використовуватимете цю можливість, для кожної з команд вам слід буде ввести пароль лише одного разу. Прочитайте розділ Розділ 3.4, щоб дізнатися більше про цю можливість і вивчити безпечність її використання.

Програму призначено для запуску інших програм з командного рядка або за допомогою файлів .desktop. Хоча програма показує запит на пароль користувача root за допомогою графічного діалогового вікна, вона є скоріше проміжною ланкою між командним рядком і графічним інтерфейсом, а не суто графічною програмою.

Оскільки kdesu встановлюється вже не до $(kf5-config --prefix)/bin, а до kf5-config --path libe xec, тому програми не буде у каталогах, описаних змінною PATH, вам слід використовувати для запуску kdesu команду $(kf5-config --path libexec)kdesu.

Розділ 2

Користування KDE su

Користуватися KDE su дуже просто. Синтаксис команди виглядає так:

kdesu [-скоманда] [-d] [-fфайл] [-іназва піктограми] [-n] [-ppriority] [-r] [-s] [-t] [-uкористувач] [--no ignorebutton] [--attachідентифікатор вікна]

kdesu [Загальні параметри KDE] [Загальні параметри Qt™]

Значення параметрів командного рядка пояснено нижче.

-c команда

Цей параметр визначає команду, яку слід виконати від імені користувача root. Команду для цієї програми слід передати у вигляді єдиного аргументу. Отже, якщо, наприклад, вам потрібно запустити нову програму для роботи з файлами, вам слід ввести до командного рядка таку команду: $(kf5-config --path libexec)kdesu -c Dolphin

-d

Показати інформацію, потрібну для налагоджування.

-f файл

Цей параметр надає вам змогу ефективно використовувати KDE su для файлів .desktop. За його допомогою можна повідомити KDE su про те, що слід обробити файл, вказаний аргументом файл. Якщо поточний користувач може вести запис до цього файла, KDE su виконає команду від імені поточного користувача. Якщо ж користувач не має права на запис до файла, команду буде виконано від імені користувача користувач (типово, від імені користувача root).

Обробка аргументу файл відбувається так: якщо файл починається з / , вважається, що надано абсолютний шлях до файла. У іншому випадку, вважається, що надано назву загального файла налаштувань KDE.

-i назва піктограма

Визначити піктограму, яку слід використовувати у діалозі запиту на пароль. Ви можете вказати лише назву файла, без суфікса, що визначає його тип.

Наприклад, щоб запустити програму Konqueror у режимі керування файлами і показати піктограму Konqueror у діалоговому вікні запиту на пароль, виконайте команду:

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

-n

Не зберігати пароль. Цей параметр знімає позначку з поля зберігати пароль у діалоговому вікні запиту на пароль.

-p пріоритет

Встановити значення пріоритету. Пріоритетом може бути довільне число між 0 і 100, де 100 означає найвищий пріоритет, а 0 — найнижчий. Типовим значенням є 50.

-r

Використовувати планування у режимі реального часу.

-s

Зупинити фонову службу kdesu. Прочитайте також Розділ 3.4.

-t

Увімкнути вивід до термінала. Цей параметр вимикає зберігання паролів. Параметр здебільшого призначено для налагоджування — якщо вам потрібно запустити програму, яка працює у термінальному режимі, скористайтеся звичайною командою su.

-u користувач

Хоча у звичайному режимі KDE su використовується для виконання команд від імені суперкористувача, ви можете використовувати програму і для виконання команд від імені інших користувачів, якщо вкажете правильний пароль.

Розділ 3

Внутрішня частина роботи програми

3.1 Розпізнавання користувача у X

Програму, яку ви накажете виконати, буде запущено з ідентифікатором користувача root, у загальному випадку ця програма не матиме дозволу для доступу до вашого дисплея X. KDE su обходить це обмеження додаванням ідентифікаційної куки (cookie) вашого дисплея до тимчасового файла .Xauthority. Після завершення роботи команди цей файл буде вилучено.

У випадку, якщо ви не використовуєте куки X, ви маєте самі усунути можливі проблеми. KDE su виявить неможливість використання кук і не буде додавати куку, але у такому випадку вам слід наперед переконатися, що користувачеві root дозволено доступ до вашого дисплея.

3.2 Інтерфейс su

Для отримання належних привілеїв KDE su використовує системну команду su. У цьому розділі детально пояснено, яким чином KDE su це робить.

Оскільки деякі з реалізацій команди su (наприклад реалізація цієї команди у Red Hat®) не бажають читати пароль з stdin, KDE su створює пару pty/tty і виконує команду su за допомогою її стандартних дескрипторів файлів, з'єднаних з tty.

Для виконання вказаної користувачем програми KDE su використовує аргумент параметра -c у сполученні з командою su замість інтерактивної оболонки. Цей аргумент розпізнається всіма відомими авторові оболонками і має без проблем працювати всюди. Команда su передає аргумент -c до оболонки призначення користувача, а оболонка виконує саму програму. Приклад команди: su root -c програма.

Замість виконання команди користувача безпосередньо за допомогою su, KDE su виконує невеличку проміжну програму з назвою kdesu_stub. Ця проміжна програма (запущена від імені визначеного користувача) надсилає запит на отримання деякої інформації від KDE su за допомогою каналу pty/tty (stdin і stdout проміжної програми), а потім виконує вказану програму. Інформація, яка передається за допомогою проміжної програми: назва дисплея X, кука розпізнавання X (якщо доступний), системна змінна PATH і команда, яку слід виконати. Причиною використання проміжної програми є те, що у куці X міститься особиста інформація, тому цю інформацію не можна передавати за допомогою командного рядка.

3.3 Перевірка паролів

KDE su перевірить введений вами пароль і повідомить вас про помилку, якщо цей пароль було вказано неправильно. Перевірка здійснюється за допомогою виконання програми перевірки: /bin/true. Якщо перевірку цією програмою пройдено, пароль вважається правильним.

3.4 Зберігання паролів

Для зручності у KDE su реалізовано можливість «збереження паролів». Якщо вам цікаво, чи безпечною є ця можливість, вам слід прочитати цей розділ.

Надання згоди на запам'ятовування паролів у KDE su відкриває (невеличку) дірку у системі безпеки вашого комп'ютера. Очевидно, що KDE su не дозволяє нікому з ідентифікатором відмінним від ідентифікатора користувача використовувати цей пароль, але, якщо бездумно користуватися цією можливістю, вона знижує рівень доступу до привілеїв користувача r oot до рівня звичайного (вашого) користувача. Зловмисник, якому вдалося зламати ваш обліковий запис, отримає доступ до прав виконання користувача root. KDE su намагається запобігти подібній ситуації. Схема убезпечення, що використовується програмою, принаймні на думку автора програми, достатньо надійна, нижче ви зможете з нею ознайомитися.

KDE su користується послугами фонової служби з назвою kdesud. Ця фонова служба очікує на команди у гнізді UNIX®, розташованому в теці /tmp. Режим доступу до гнізда визначено числом 0600, отже з гніздом може з'єднатися лише користувач з вашим ідентифікатором. Якщо увімкнено можливість зберігання паролів, KDE su виконує команди за допомогою цієї фонової служби. Програма записує команду і пароль користувача root до гнізда, а фонова служба виконує команду за допомогою su у спосіб, описаний вище. Після цього команда і пароль не викидаються — вони зберігаються певний час. Цей час визначається часом очікування модуля керування. Якщо протягом цього часу надійде ще один запит на ту саму команду, клієнтській програмі не слід буде вказувати пароль. Щоб запобігти викраденню паролів з фонової служби зловмисником, який зламав ваш обліковий запис (наприклад, за допомогою програми для налагоджування), фонову службу встановлено з ідентифікатором групи nogroup. Це запобігає спробам звичайних користувачів (зокрема, і вашого користувача) отримати паролі від процесу kdesud. Крім того, фонова служба встановлює системну змінну DISPLAY у значення, яке вона мала під час запуску. Все, що може зробити зловмисник, — це виконати програму на вашому дисплеї.

Єдиною слабкою ланкою цієї системи є те, що програми, які ви намагаєтеся виконати, не написано з врахуванням міркувань безпеки (наприклад програми з ідентифікатором користувача root). Це означає, що у них можуть бути помилки, що призводять до переповнення буфера, або інші помилки, які може використати зловмисник.

Використання можливості зберігання паролів є компромісом між міркуваннями безпеки і зручності. Автор радить вам добре все обдумати і вирішити, чи бажаєте ви користуватися цією можливістю, чи ні.

Розділ 4

Автор

KDE su

Автором KDE su є Geert Jansen. Код програми до певної міри засновано на коді Pietro Iglio для версії 0.3 KDE su. Pietro і Geert домовилися про те, що у майбутньому підтримку програми здійснюватиме Geert.

Зв'язатися з автором можна за допомогою електронної поштової скриньки з адресою g.t.jansen@stud.tue.nl. Будь ласка, повідомляйте йому про всі знайдені вади за цією адресою, щоб він міг виправити їх. Якщо у вас є якісь пропозиції, не вагайтесь і також повідомляйте про них за вказаною адресою.

Переклад українською: Юрій Чорноіван yurchor@ukr.net