Лабораторная работа №4.

Управление привилегиями и настройка безопасности в ОС “Альт”

*Цель работы:* Изучение методов управления привилегиями, особенностей ОС “Альт” с точки зрения безопасности, а также базовых аспектов настройки системы для повышения уровня безопасности.

1. Функционал control

Механизм *control* используется для переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда *control* доступна только для суперпользователя.

Запустив команду *control* без параметров можно увидеть полный список компонентов, управляемых командой вместе с их текущим состоянием и набором допустимых состояний.

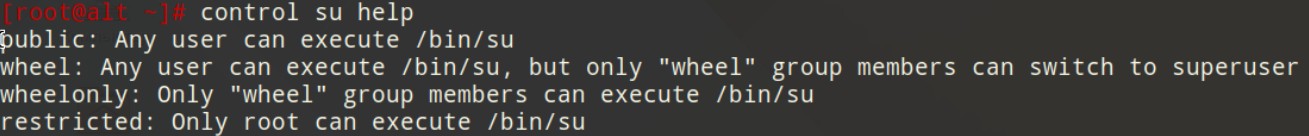
# control Описание вывода:

1-й столбец — компонент системы; 2-й столбец — текущее состояние;

3-й столбец — набор допустимых состояний;

Для того, чтобы посмотреть разрешения выполнения конкретным компонентов, надо запустить команду с ключом *help*.

Справка управления командой *su*:

# control su help

Команда *su* используется для смены пользователя в текущей сессии терминала.

Для управления командой *su* есть следующие политики:

public — любой пользователь может выполнить команду */bin/su*;

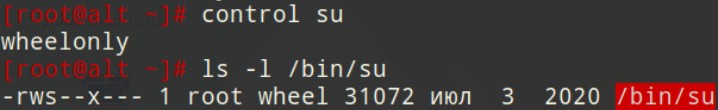
wheel — любой пользователь может выполнить команду *su*, но только пользователи, входящие в группу *wheel*, могут получить через нее права суперпользователя;

wheelonly — только пользователи, входящие в группу *wheel*, могут выполнить команду *su*;

restricted — только суперпользователь может выполнять команду *su*.

Теперь выведем текущую политику команды *su* и проверим права доступа к исполняемому файлу */bin/su*:

# control su # ls -l /bin/su

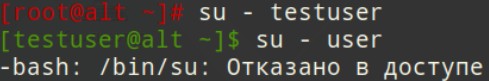


Создадим пользователя *testuser* с паролем *P@ssw0rd*: # useradd testuser

# passwd testuser

Зайдем под учетной записью *testuser* и попробуем с помощью команды

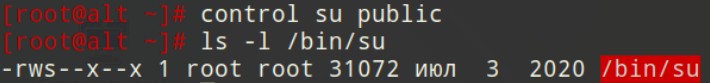
*su* войти в учетную запись *user*: # su - testuser

$ su - user

Поскольку пользователь *testuser* не входит в группу *wheel*, использовать команду *su* ему запрещено!

Изменим текущую политику команды *su* на *public* и проверим права доступа к исполняемому файлу */bin/su*:

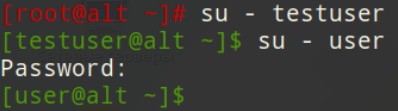
# control su public # ls -l /bin/su



Важно! Устанавливать разрешение *public* следует только в рамках учебной работы.

Еще раз зайдем под учетной записью *testuser* и попробуем с помощью команды *su* войти в учетную запись *user*:

# su - testuser

$ su - user

Для переключения состояния *control* вызывает соответствующий скрипт из каталога */etc/control.d/facilities/*:

# ls /etc/control.d/facilities

Зайдем под учетной записью *testuser* и проверим работу команды

*mount*:

# su - testuser

$ mount

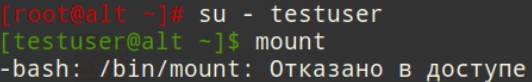
Команда *mount* предназначена для подключения файловых систем и переносных накопителей к конкретным точкам монтирования в дереве каталогов. При запуске без аргументов команда показывает все подключенные в данный момент файловые системы.

По умолчанию для команды *mount* установлена политика *public*: # control mount

Изменим текущую политику команды *mount* на *restricted*: # control mount restricted

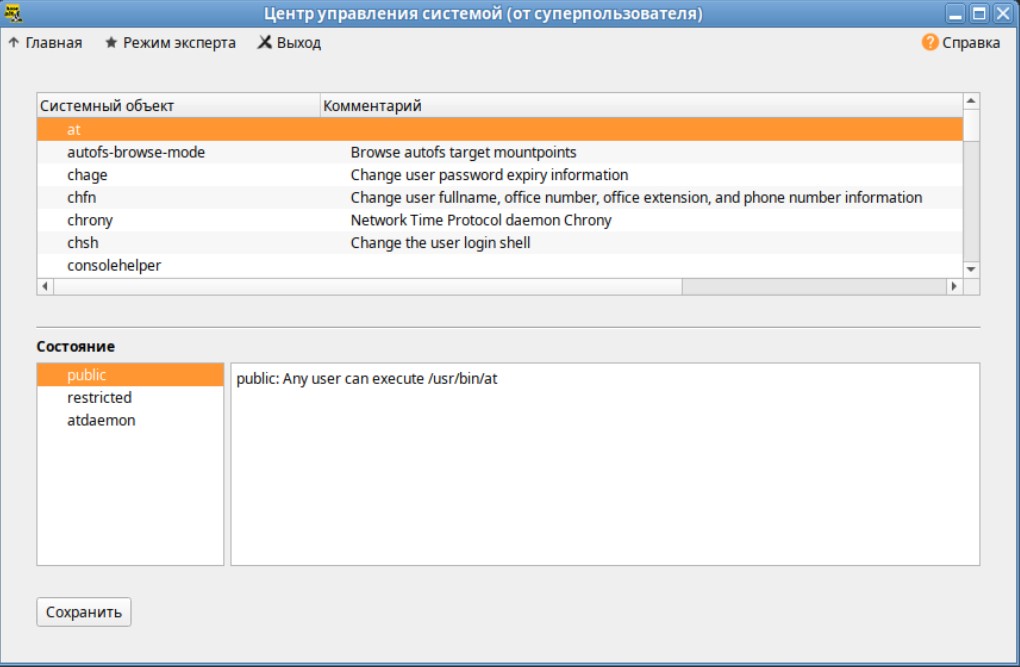
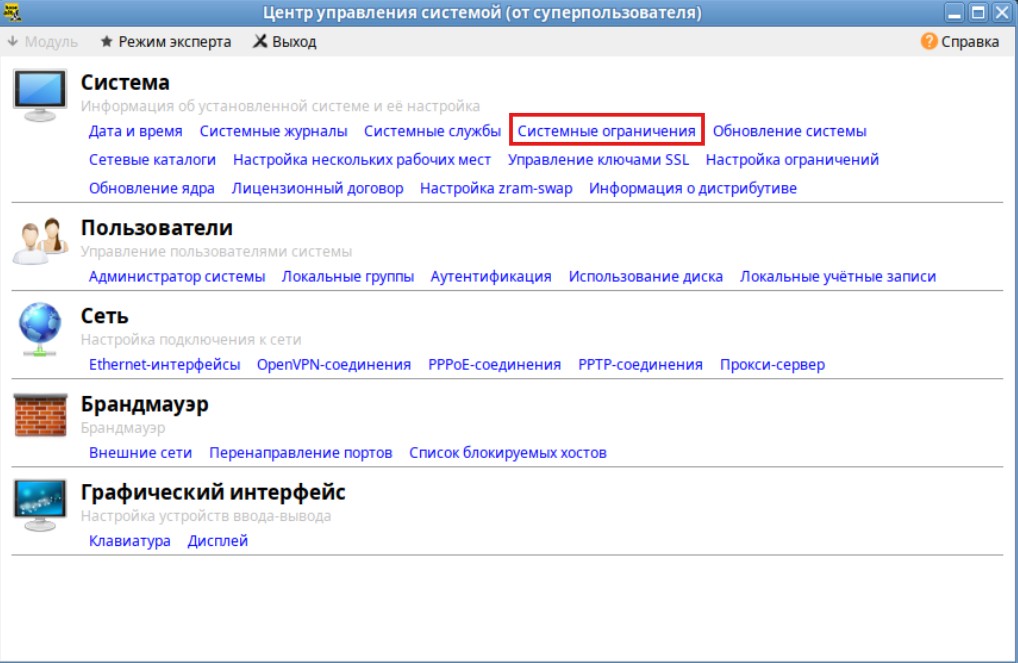
Еще раз зайдем под учетной записью *testuser* и проверим работу команды *mount*:

# su - testuser

$ mount

Управлять политиками *control* можно через ЦУС.

Для этого должен быть установлен пакет *alterator-control*.

Зайдем в ЦУС и в разделе “Система” откроем пункт “Системные ограничения”:

1. Концепция sudo

Команда sudo (сокращение от “superuser do”) используется для выполнения команд с привилегиями суперпользователя.

Перед выполнением команды *sudo* запрашивает пароль пользователя, а не пароль суперпользователя.

После выполнения *sudo* существует временной отрезок, в течение которого повторное выполнение команды *sudo* не требует пароль (удобно для взлома системы со стороны *rootkits* и хакерских атак).

С другой стороны, команда *sudo* удобна для распределения прав между несколькими администраторами системы, не предоставляя прав суперпользователя на все другие действия и не выдавая пользователю пароля суперпользователя.

В ОС “Альт Рабочая станция 10.2” команды *sudo* по умолчанию не установлен.

Предварительно установим пакет *sudo*:

# apt-get update

# apt-get install sudo

Команда *sudo* требует предварительной настройки, так как в */etc/sudoers*

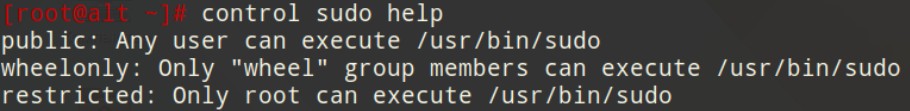
не описан ни один пользователь, включая суперпользователя. # cat /etc/sudoers

В дополнение к */etc/sudoers* могут использоваться отдельные файлы из каталога */etc/sudoers.d/*.

# ls /etc/sudoers.d

Для ограничения прав на выполнение самой команды *sudo* используется механизм *control*.

Справка управления командой *sudo*:

# control sudo help

На текущий момент существуют следующие политики у команды sudo: public — любой пользователь может получить доступ к команде

*/usr/bin/sudo*;

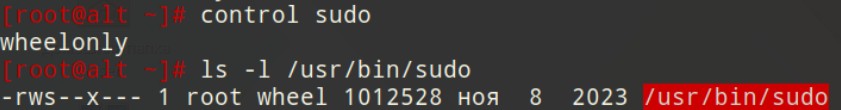
wheelonly — только пользователи из группы wheel имеют право получить доступ к команде */usr/bin/sudo*;

restricted — только суперпользователь имеет право выполнять команду

*/usr/bin/sudo*.

Теперь выведем текущую политику команды *su* и проверим права доступа к исполняемому файлу */bin/su*:

# control sudo

# ls -l /usr/bin/sudo

Пользователь из группы *wheel* имеет право запускать саму команду *sudo*, но это не означает, что он через sudo может выполнить какую-то команду с правами суперпользователя.

Для разрешения получения прав на выполнение конкретных команд с правами суперпользователя надо отредактировать настройки правил

*/etc/sudoers* при помощи специальной команды *visudo* (которая не портит права на файлы):

# visudo

Если раскомментировать (убрать # в начале строки) в */etc/sudoers* следующую строку, то это даст права выполнять через *sudo* любую команду с любого хоста (например, через ssh), пользователям, входящим в группу *wheel*, запрашивая их пароль:

WHEEL\_USERS ALL=(ALL) ALL

С точки зрения безопасности правильнее давать права на выполнение *sudo* не всей группе *wheel*, а конкретному пользователю, и не на все команды, а на те, которые ему необходимы для быстрого получения права суперпользователя.

Дадим пользователю *testuser* права на использование команды

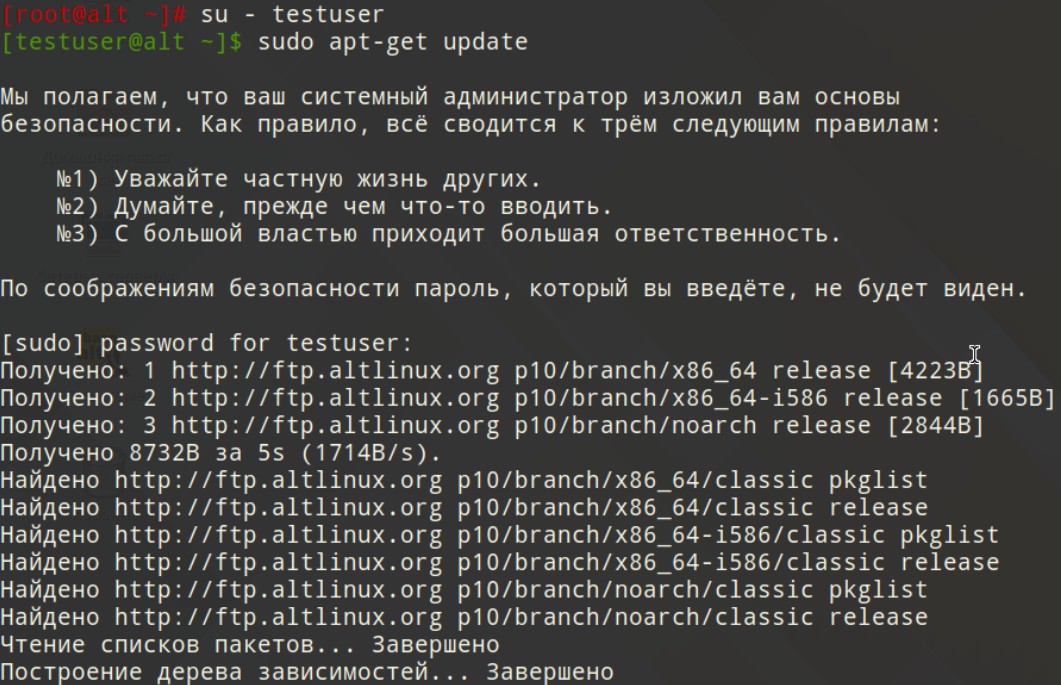
*/usr/bin/apt-ge*t:

testuser ALL=(ALL) /usr/bin/apt-get

Также не забудем добавить пользователя *testuser* в группу *wheel*: # usermod -aG wheel testuser

Зайдем под учетной записью и попробуем обновить систему: # su - testuser

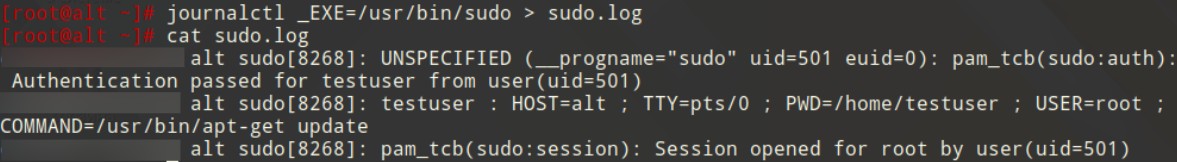
$ sudo apt-get update



Для просмотра и анализа логов *sudo* можно использовать команду

*journalctl*.

Найдем в журнале информацию о выполнении предыдущей команды. Отфильтруем логи *sudo* и сохраним в файл *sudo.log*:

# journalctl \_EXE=/usr/bin/sudo > sudo.log # cat sudo.log

1. Схема Tcb

*Trusted Computing Base (tcb)* — механизм управления теневыми паролями, выступающего в роли альтернативы традиционной схемы

*/etc/shadow*.

Ключевым отличием *tcb* от */etc/shadow* является уход от использования общего файла со всеми хэшами паролей в пользу разнесения хэшей паролей по отдельным каталогам и файлам. При подобной организации хранения операции с паролями можно выполнять без повышения прав, а процесс, осуществляющий обработку учетных данных, ограничен учетной записью отдельного пользователя.

Обработчик */etc/shadow* всегда получает доступ сразу ко всем хэшам паролей, т.е. уязвимость в утилите *passwd* позволяет изменить любой пароль. В *tcb* каждый файл включает только хэш одного пользователя и размещается в

каталоге, принадлежащем этому пользователю, что позволяет обойтись без повышения привилегий при запуске утилиты *passwd*.

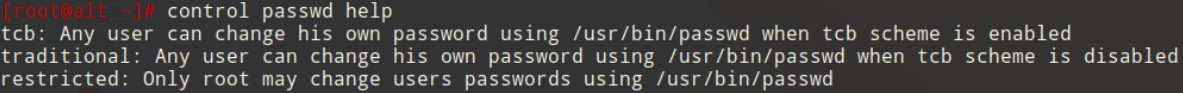
В ОС “Альт Рабочая станция” все теневые файлы пользователей располагаются в каталоге */etc/tcb*.

# ls /etc/tcb

Для совместимости с другими схемами входное имя может содержать только латинские буквы, цифры и символ подчеркивания.

Переключение между схемой хранения паролей *tcb*, классической схемой (с единым файлом */etc/shadow*) и строгой схемой (классическая, при которой команду *passwd* имеет право запускать только суперпользователь) управляется командой *control passwd* с параметрами *tcb*, *traditional* и *restricted* соответственно.

Справка управления командой *passwd*:

# control passwd help

По умолчанию в ОС “Альт Рабочая Станция” установлена схема хранения паролей *tcb*:

# control passwd

1. Основы Linux Login

Аутентификация пользователя выполняется с помощью файла теневого пароля. Файл теневого пароля настраивается с помощью конфигурационного файла */etc/login.defs*.

Команды *useradd*, *usermod*, *userdel* и *groupadd*, а также другие утилиты для пользователей и групп берут значения по умолчанию из этого файла. Каждая строка состоит из имени директивы и связанного с ней значения.

# cat /etc/login.defs

Приведем список основных директив */etc/login.defs*: MAIL\_DIR — расположение почтовых ящиков пользователей;

UID\_MIN, UID\_MAX — минимальное и максимальное значения для автоматического выбора UID (от 1000 до 60000);

GID\_MIN, GID\_MAX — минимальное и максимальное значения для автоматического выбора GID (от 1000 до 60000);

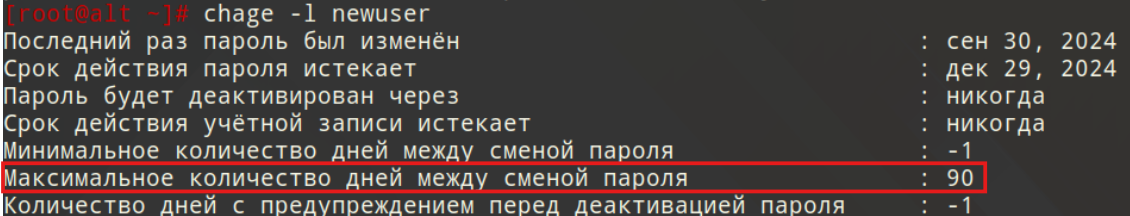
CREATE\_HOME — создание домашних директорий при добавлении нового пользователя;

UMASK — пользовательская маска *umask*.

Изменим директиву PASS\_MAX\_DAYS, которая отвечает за максимальное количество дней, в течение которых пароль может оставаться действительным. Для этого отредактируем следующую строку в файле

*/etc/login.defs* (также необходимо раскомментировать строку): PASS\_MAX\_DAYS 90

Теперь создадим пользователя *newuser* с паролем *P@ssw0rd* и проверим информацию о его пароле:

# useradd newuser # passwd newuser # chage -l newuser

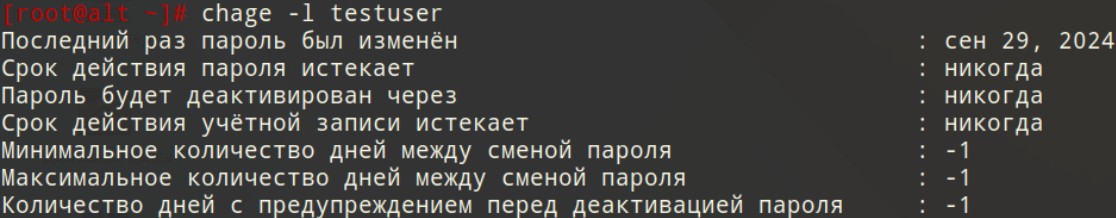
1. Управление паролями

Команда *chage* используется для управления сроком действия паролей пользователей.

Синтаксис команды *chage*:

*chage* [options] [username]

Опция -l отображает информацию о пароле указанного пользователя. Выведем информацию о пароле пользователя *testuser*:

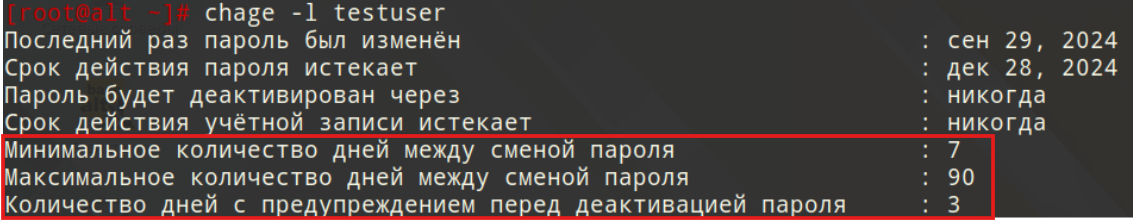
# chage -l testuser

Справка команды *chage*:

# chage --help

Установим для пароля пользователя *testuser* следующие параметры: Минимальный срок действия пароля — 7 дней;

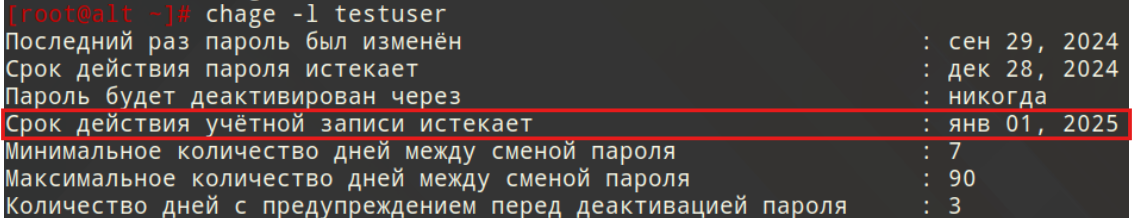
Максимальный срок действия пароля — 90 дней; Предупреждение до истечения срока действия пароля — 3 дня. # chage -m 7 -M 90 -W 3 testuser

Теперь еще раз выведем информацию о пароле пользователя *testuser*: # chage -l testuser

Также установим дату истечения срока действия учетной записи

*testuser*:

# chage -E ‘2025-01-01’ testuser

Проверим применение настроек: # chage -l testuser