МИНИСТЕСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Факультет информационных технологий и робототехники

Отчет по лабораторной работе № 1.4

на тему «Основы администрирования системы Linux»

по дисциплине «Системное программирование»

Кафедра программного обеспечения информационных систем и технологий

Выполнили

Студенты группы 10701322 Н.В. Тимощенко

Д.Е. Кудрявец

Проверил Галай В.В

Минск 2024

**Цель работы:**

Закрепить на практике основы администрирования системы Linux, изучить атрибуты файлов и права доступа к ним, освоить работу с файлами и каталогами.

**Выполнение работы:**

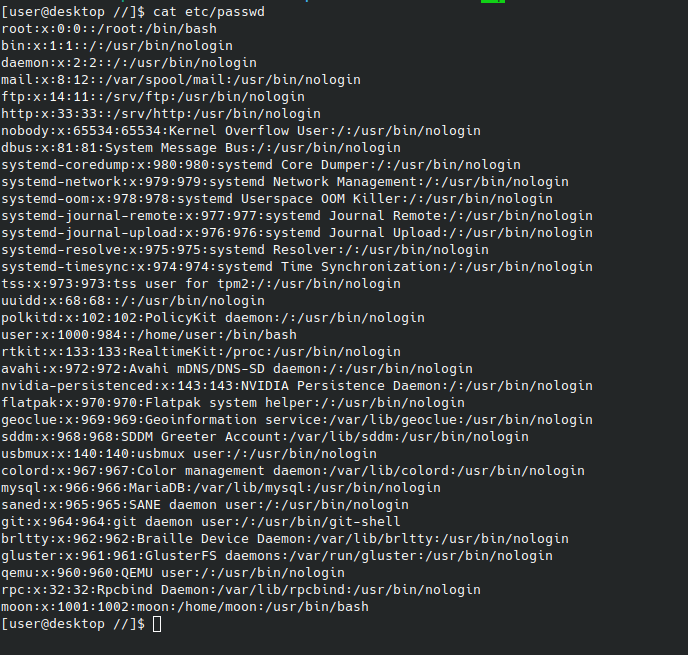
**Задание 1. Создание пользователей:**

Создайте стандартного пользователя с помощью GUI. Пользователю присвойте имя члена вашей команды, но в имени должен присутствовать суффикс \*GUI. Это нужно для проведения экспериментов. При присвоении имен действуйте по принципу: «Относитесь к именам переменных, как к именам детей своих». Пароль пользователя должен быть простым, например «123».

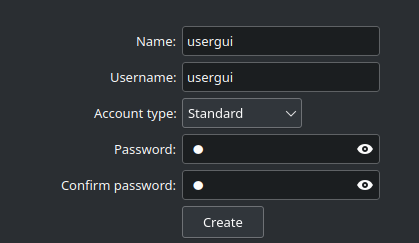
Просмотрите содержимое файла /etc/passwd, сравните атрибуты реальных пользователей и пользователя root. Результат подтвердите скриншотом. Дайте пояснения.

Создайте несколько стандартных пользователей (аккаунтов) посредством командной строки. При этом пользователям присвойте имена членов вашей команды, но в имени должен присутствовать суффикс \*CL или \*CLI. Это нужно для того, чтобы отличить пользователей созданных при помощи графического и консольного интерфейсов. Создайте двух пользователей с одинаковыми простыми паролями. Создайте скелет и пользователя с шаблоном скелета в директории /home. Также попробуйте создать аккаунт реального пользователя без пароля.

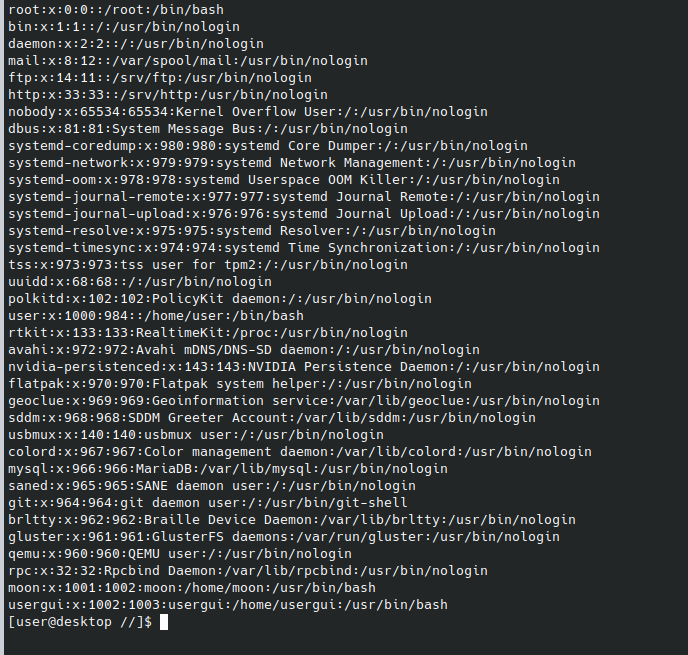
Первоначальное состояние файла passwd



Добавление стандартного пользователя с помощью графического интерфейса

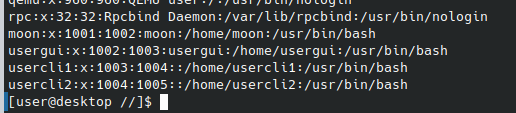


Файл passwd



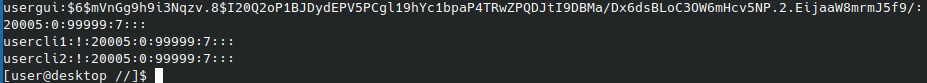
Создание пользователей с помощью командной строки



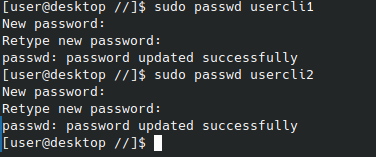


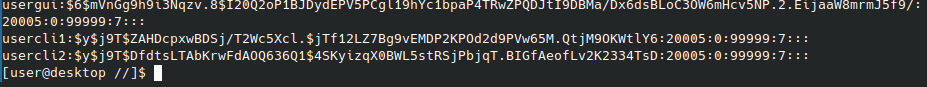
Просмотр файла shadow

sudo cat etc/shadow

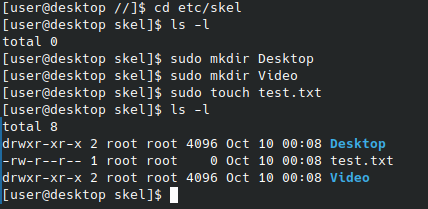


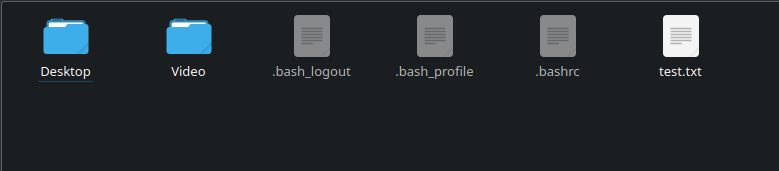
Установка пароля для двух новых пользователей





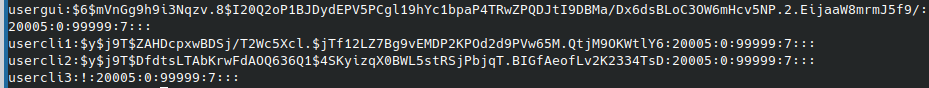
Создание скелета пользователя





Создание реального пользователя без пароля



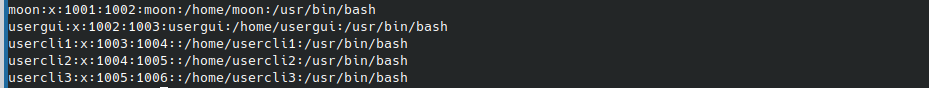


**Задание 2. Изменение параметров паролей пользователей:**

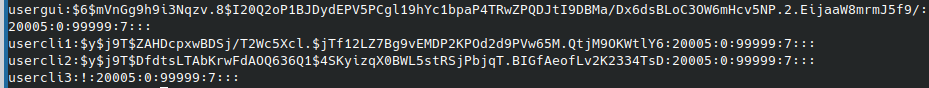
Пароли должны быть простые и одинаковые. Это нужно для проведения экспериментов. Просмотрите содержимое файла /etc/passwd, сравните атрибуты реальных пользователей. Просмотрите содержимое файла /etc/shadow, сравните атрибуты паролей пользователей, особое внимание обратите на шифр пароля у пользователей с одинаковым паролем.

Измените периоды изменения паролей для пользователей. Внесите ограничения в следующие атрибуты: минимальный возраст пароля (сутки); максимальный возраст пароля (сутки); период предупреждения пароля; период бездействия пароля; дата истечения срока действия аккаунта. Результат подтвердите скриншотом. Дайте пояснения.

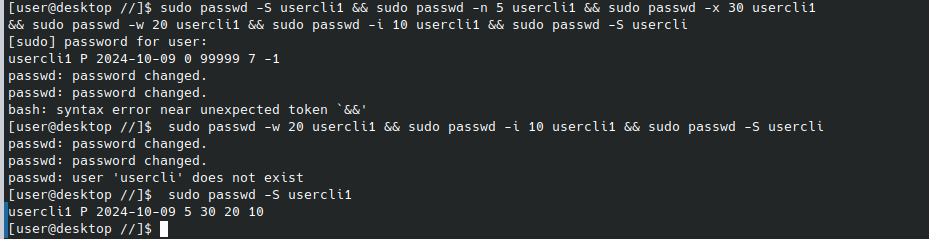
Содержимое файла /etc/passwd



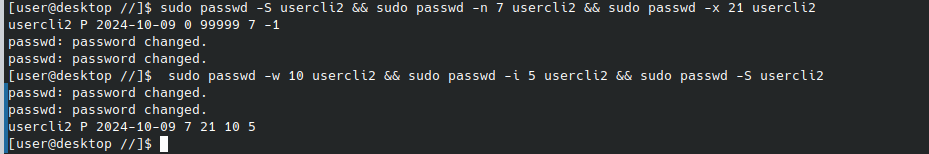
Содержимое файла /etc/shadow



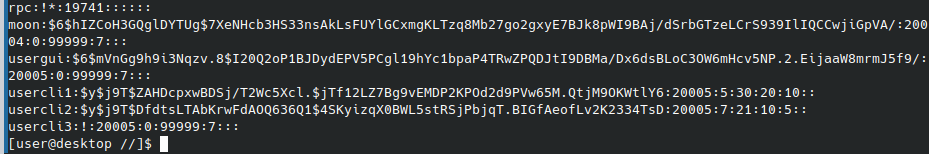
Результат изменения атрибутов пароля для первого пользователя



Результат изменения атрибутов пароля для второго пользователя



Содержимое файла /etc/shadow после изменения атрибутов пароля



**Задание 3.Создание групп и работа с правами доступа к файлам:**

Создайте пользователя (аккаунт) с правами администратора. В каталогах /home/ администраторов и других пользователей создайте по несколько файлов с разными правами доступа.

Создайте общую группу пользователей.

Выполните следующие требования:

1. Одного из пользователей перевести в группу shadow

2. Создать у каждого пользователей директорию с 2 файлами

3. Просмотреть текущие права доступа к файлам для всех пользователей

4. Каталог пользователя в группе shadow сделать доступным только в своей группе

5. Файлы второго пользователя сделать доступными только владельцам

6. Под админом назначить всем созданным файлам права только для чтения для всех пользователей

7. Пользователем в группе shadow лишить всех остальных пользователей права исполнять его файлы

8. Под админом назначить всем пользователям все права

9. Удалить пользователя, находящегося в группе shadow

Укажите является ли группа системной или создана пользователем.

Получите идентификаторы пользователей и состояние активных пользователей системы. Проверьте содержимое файлов /etc/shadow, /etc/passwd, /etc/group.

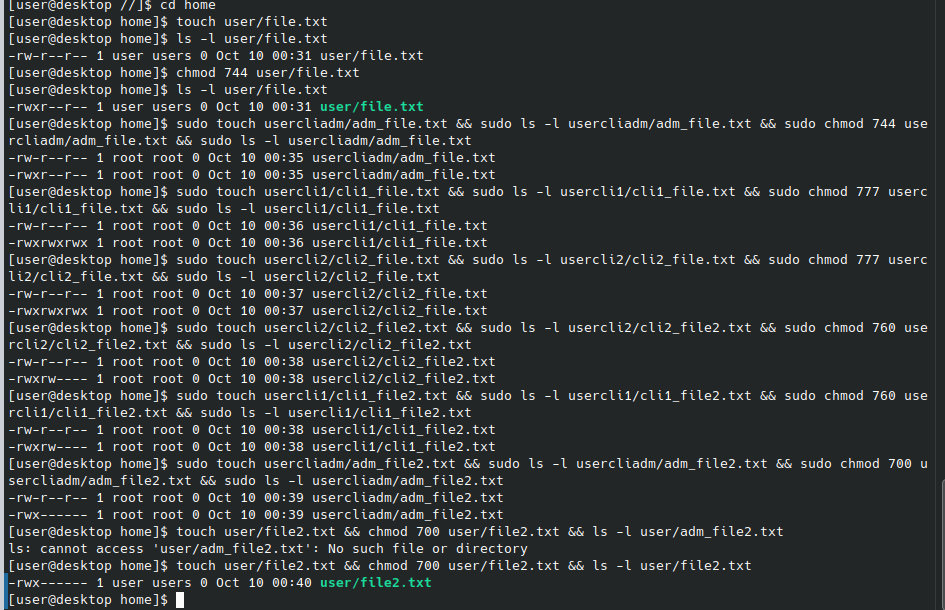
Некоторые файлы защитите липким битом. Попробуйте удалить созданные файлы из других аккаунтов администраторов и простых пользователей. Опишите какой получили результат.

Создайте жесткую ссылку, перенесите эту ссылку в пространство другого пользователя и откройте ее в сеансе этого пользователя, затем присвойте жесткой ссылке одну группу и откройте ссылку из пользователя этой группы. Измените владельца и группу жесткой ссылки и посмотрите, как изменились атрибуты основного файла.

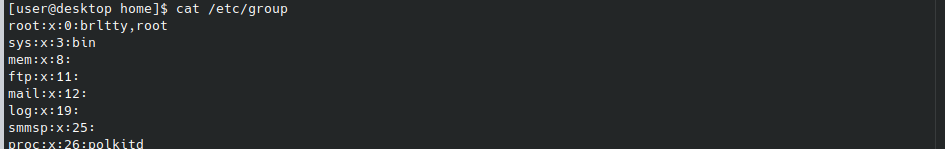
Создание пользователя с правами администратора

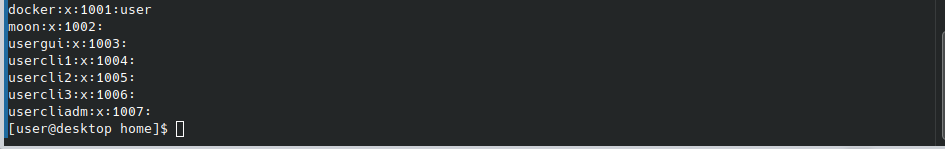


Создание файлов и изменение прав доступа к ним

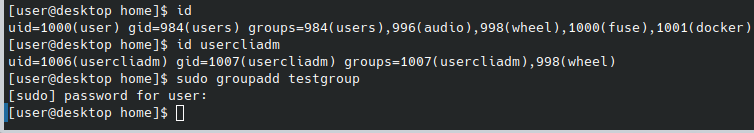


Содержимое файла group

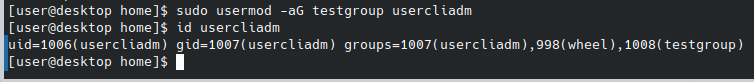




Просмотр групп для пользователей, создание группы

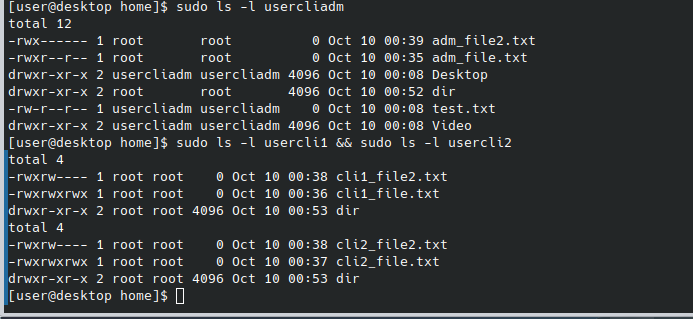


Добавление пользователя в группу

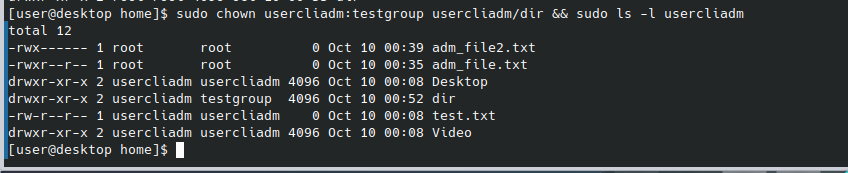


Создание директорий для всех пользователей

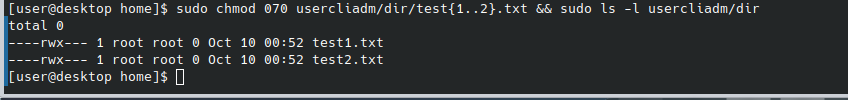
Текущие права доступа пользователей



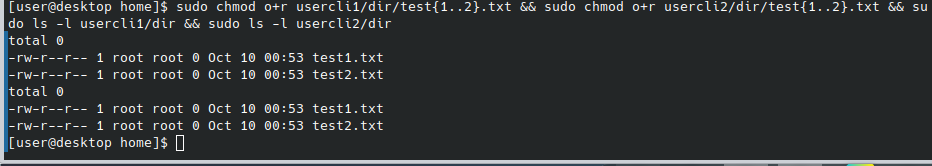
Изменение прав доступа пользователя в группе shadow

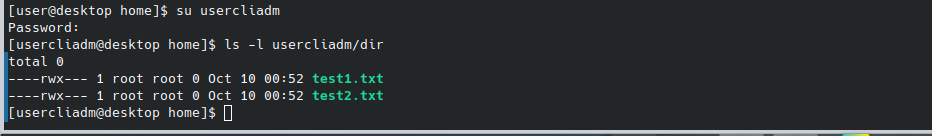


Делаем файлы второго пользователя доступными только владельцу

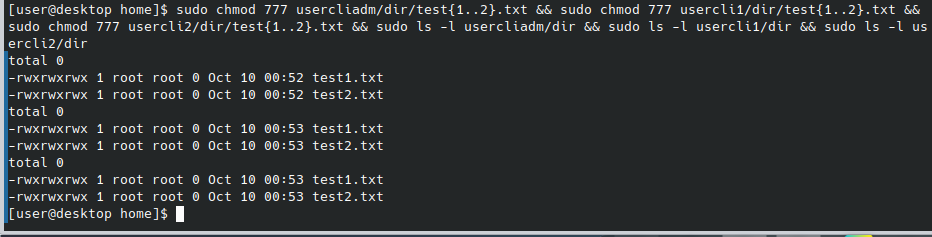


Под админом назначим всем созданным файлам права только для чтения для всех пользователей

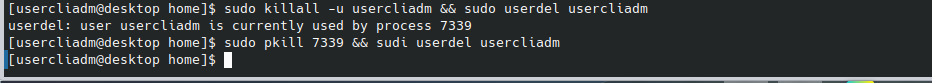




Под админом назначить всем пользователям все права



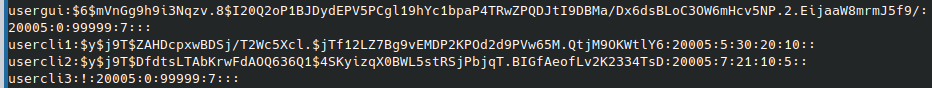
Удалить пользователя, находящегося в группе testgroup



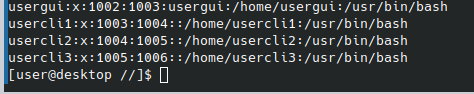
Получение идентификаторов



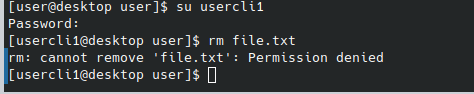
Файл /etc/shadow



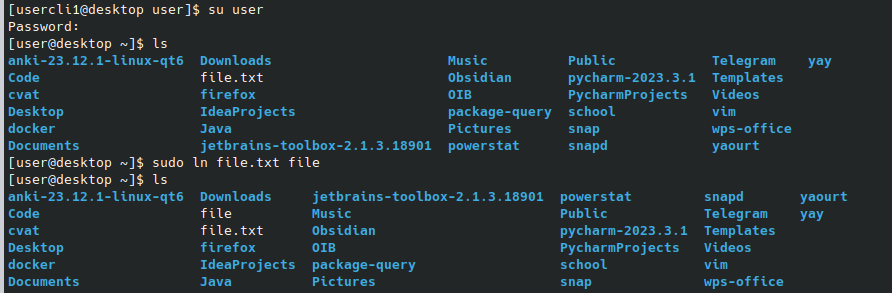
Файл /etc/passwd



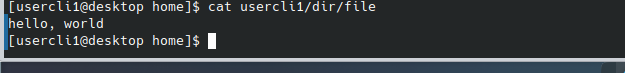
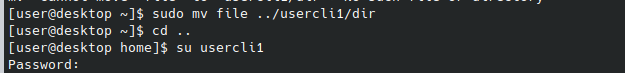
Защита файла липким битом и попытка удалить файл от имени другого пользователя



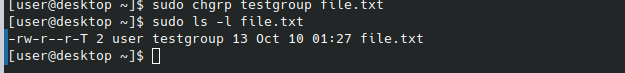
Создание файла и создание жесткой ссылки к файлу



Переносим ссылку в пространство другого пользователя и открываем её в сеансе этого пользователя



Присвоение жесткой ссылки группе



**Ответы на контрольные вопросы:**

1. **Какая концепция прав доступа к файлу реализована в ядре?**

 Концепция прав доступа к файлу в ядре Linux основана на модели доступа UNIX. Каждый файл имеет три типа прав доступа: чтение ®, запись (w) и выполнение (x). Эти права могут быть назначены трем категориям пользователей: владельцу файла, группе и остальным пользователям. Права доступа определяются с помощью команд chmod, chown и chgrp. В ядре также реализованы расширенные атрибуты (ACL), которые позволяют более гибко управлять правами доступа. Концепция прав доступа обеспечивает безопасность и контроль над файлами и каталогами в системе.

1. **Какие типы пользователей существуют в Linux (UNIX)?**

В Linux (UNIX) существует три основных типа пользователей: суперпользователь (root), обычные пользователи и системные пользователи. Суперпользователь имеет полный доступ ко всем командам и файлам в системе. Обычные пользователи имеют ограниченные права и могут выполнять только те действия, которые разрешены их учетной записью. Системные пользователи обычно используются для выполнения фоновых процессов и служб и имеют минимальные права доступа. Каждый пользователь идентифицируется уникальным идентификатором пользователя (UID).

1. **Поясните понятие «реальный пользователь».**

Реальный пользователь — это пользователь, который инициировал процесс. В системе Linux каждый процесс имеет идентификатор реального пользователя (RUID), который соответствует UID пользователя, запустившего процесс. Это важно для контроля доступа и безопасности, так как права доступа процесса зависят от прав реального пользователя. Реальный пользователь отличается от эффективного пользователя, который может быть изменен с помощью команды setuid для выполнения задач с повышенными привилегиями.

1. **В чем различие понятий «пользователь» и «владелец файла»?**

Пользователь — это учетная запись в системе, которая имеет уникальный идентификатор (UID) и может выполнять различные действия в системе. Владелец файла — это пользователь, которому принадлежит файл и который имеет право изменять права доступа к этому файлу. Владелец файла может быть изменен с помощью команды chown. Важно понимать, что владелец файла имеет больше прав на управление файлом, чем другие пользователи, даже если они находятся в той же группе.

1. **Что такое «аккаунт» или «логин», из каких атрибутов состоит?**

Аккаунт или логин — это учетная запись пользователя в системе, которая позволяет ему аутентифицироваться и получать доступ к ресурсам системы. Аккаунт состоит из нескольких атрибутов, таких как имя пользователя, UID, GID (идентификатор группы), домашний каталог и оболочка по умолчанию. Эти атрибуты хранятся в файле /etc/passwd. Аккаунт также может включать дополнительные атрибуты, такие как пароль, который хранится в файле /etc/shadow.

1. **Опишите отличия команд su и sudo.**

Команда su (substitute user) позволяет переключиться на другого пользователя, запрашивая пароль этого пользователя. Обычно используется для перехода на суперпользователя (root). Команда sudo (superuser do) позволяет выполнять команды от имени суперпользователя или другого пользователя, запрашивая пароль текущего пользователя. sudo предоставляет более гибкий и безопасный способ выполнения команд с повышенными привилегиями, так как позволяет ограничить доступ к определенным командам и ведет журнал выполненных команд.

1. **В чем отличие символов строки приглашения $ и # ?**

В командной строке Linux символы $ и # имеют разные значения:

$: Этот символ используется для обозначения приглашения командной строки обычного пользователя. Когда вы видите ‘$`, это означает, что вы работаете под учетной записью с обычными правами.

#: Этот символ используется для обозначения приглашения командной строки суперпользователя (root). Когда вы видите #, это означает, что вы работаете под учетной записью с административными правами, что позволяет выполнять команды, требующие повышенных привилегий.

**8) Для чего предназначена системная директория etc, какие файлы в ней**

**хранятся?**

 Директория /etc предназначена для хранения конфигурационных файлов системы и программ. В ней хранятся файлы, необходимые для настройки и управления системой, такие как /etc/passwd, /etc/shadow, /etc/fstab, /etc/hosts и многие другие. Эти файлы содержат информацию о пользователях, паролях, монтировании файловых систем, сетевых настройках и других аспектах конфигурации системы. Например, файл /etc/hosts используется для сопоставления IP-адресов с именами хостов, а файл /etc/fstab содержит информацию о файловых системах, которые должны быть смонтированы при загрузке системы.

**9) Какую информацию содержат конфигурационные файлы passwd и**

**shadow?**

 Файл /etc/passwd содержит информацию о пользователях системы, включая имя пользователя, UID, GID, домашний каталог и оболочку по умолчанию. Файл /etc/shadow содержит зашифрованные пароли пользователей и дополнительные атрибуты паролей, такие как дата последнего изменения пароля, минимальный и максимальный возраст пароля, период предупреждения о смене пароля и срок действия учетной записи. Эти файлы используются для аутентификации и управления учетными записями пользователей. Например, строка в файле /etc/passwd может выглядеть так:

john:x:1001:1001:John Doe:/home/john:/bin/bash

А соответствующая строка в файле /etc/shadow:

john:$6$saltsalt$hashedpassword:19000:0:99999:7:::

**10) В чет различие понятий «пользователь» и «аккаунт пользователя»?**

**Объясните это на примере строки файла /etc/passwd.**

 Пользователь — это физическое лицо или процесс, который выполняет действия в системе. Аккаунт пользователя — это учетная запись, которая позволяет пользователю аутентифицироваться и получать доступ к ресурсам системы. В файле /etc/passwd строка имеет следующий формат:

username:x:UID:GID:comment:home\_directory:shell

Например:

john:x:1001:1001:John Doe:/home/john:/bin/bash

Здесь john — это имя пользователя, 1001 — UID, 1001 — GID, John Doe — комментарий, /home/john — домашний каталог, /bin/bash — оболочка по умолчанию. Эта строка описывает аккаунт пользователя john.

**11) Поясните атрибуты пользователя записанные в файле**

**/etc/passwd.**

 В файле /etc/passwd каждая строка содержит следующие атрибуты пользователя:

* username: имя пользователя.
* x: символ-заполнитель для пароля (пароль хранится в файле /etc/shadow).
* UID: уникальный идентификатор пользователя.
* GID: идентификатор основной группы пользователя.
* comment: комментарий, обычно содержит полное имя пользователя.
* home\_directory: путь к домашнему каталогу пользователя.
* shell: путь к оболочке по умолчанию, которая запускается при входе пользователя в систему

**12) Поясните атрибуты пароля пользователя в файле /etc/shadow.**

В файле /etc/shadow каждая строка содержит следующие атрибуты пароля пользователя:

* username: имя пользователя.
* password: зашифрованный пароль.
* last\_changed: дата последнего изменения пароля (в днях с 1 января 1970 года).
* min\_age: минимальный возраст пароля (в днях).
* max\_age: максимальный возраст пароля (в днях).
* warn: период предупреждения о смене пароля (в днях).
* inactive: период неактивности учетной записи (в днях).
* expire: дата истечения срока действия учетной записи (в днях с 1 января 1970 года).
* reserved: зарезервированное поле для будущего использования.

**13) Что такое липкий бит (Sticky bit), для чего и как он применяется?**

Липкий бит (Sticky bit) — это специальный атрибут файла или каталога, который предотвращает удаление или переименование файлов в этом каталоге пользователями, не являющимися владельцами этих файлов. Он применяется в общедоступных каталогах, таких как /tmp, чтобы предотвратить случайное или злонамеренное удаление файлов другими пользователями. Устанавливается липкий бит командой:

chmod +t /path/to/directory

**14) Что такое иноды файлов?**

Иноды (index nodes) — это структуры данных в файловой системе, которые хранят информацию о файлах и каталогах, такую как права доступа, владельца, размер, временные метки и местоположение данных на диске. Каждый файл и каталог имеет уникальный инод. Иноды не содержат имени файла, имена хранятся в каталогах, которые являются специальными файлами, содержащими ссылки на иноды.

**15) Что такое жесткая ссылка и какие ограничения она имеет?**

Жесткая ссылка — это ссылка на инод файла, которая позволяет нескольким именам файлов указывать на один и тот же набор данных на диске. Жесткие ссылки создаются командой ln:

ln /path/to/file /path/to/hardlink

Ограничения жестких ссылок включают невозможность создания ссылок на каталоги (для предотвращения циклических ссылок) и невозможность создания ссылок на файлы, находящиеся на разных файловых системах.

**16) Что такое символическая ссылка, что такое «битая» ссылка?**

Символическая ссылка (symlink) — это специальный тип файла, который содержит путь к другому файлу или каталогу. Она создается командой ln -s:

ln -s /path/to/target /path/to/symlink

Символическая ссылка может указывать на файлы и каталоги, даже если они находятся на разных файловых системах. «Битая» ссылка — это символическая ссылка, которая указывает на несуществующий файл или каталог. Это может произойти, если целевой файл был удален или перемещен.

**17) Каким образом в вашем дистрибутиве отображена битая**

**ссылка?**

В большинстве дистрибутивов Linux битая ссылка отображается с помощью команды ls -l, которая показывает путь, на который указывает ссылка, и указывает, что целевой файл не существует. Например:

ls -l /path/to/symlink

Вывод может выглядеть так:

lrwxrwxrwx 1 user group 12 Oct 8 18:00 /path/to/symlink -> /nonexistent

Здесь видно, что ссылка указывает на несуществующий путь /nonexistent.