Лабораторная работа №2

Управление пользователями и группами

Юсупова Ксения Равилевна

Содержание

# 1 Цель работы

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

# 2 Задание

1. Прочитайте справочное описание man по командам ls, whoami, id, groups, su, sudo, passwd, vi, visudo, useradd, usermod, userdel, groupadd, groupdel.
2. Выполните действия по переключению между учётными записями пользователей, поуправлению учётными записями пользователей (раздел 2.4.1).
3. Выполните действия по созданию пользователей и управлению их учётными записями(раздел 2.4.2).
4. Выполните действия по работе с группами пользователей (раздел 2.4.3).

# 3 Выполнение лабораторной работы

Сначала вошли в систему как обычный пользователь и откыли терминал. Затем определили, какую учётную запись пользователя мы используем, введя команду whoami . Позже вывели на экран более подробную информацию, используя команду id . Пояснения по отображённой информации:

uid=1000 (ksyusha): вы работаете под обычным пользователем с ID 1000

gid=1000 (ksyusha): основная группа пользователя — ksyusha (ID 1000)

группы=1000(ksyusha),10(wheel): пользователь состоит в своей группе и в привилегированной группе wheel (дает право на повышение прав)

контекст=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023: политика SELinux применяется в неограниченном режиме

Далее использовали команду su для переключения к учётной записи root. При запросе пароля ввели пароль пользователя root. Набрали id; пояснения по отображённой информации:

uid=0(root): вы стали суперпользователем (root) с ID 0.

gid=0(root): основная группа — root (ID 0).

группы=0(root): пользователь root состоит только в группе root.

контекст=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023: контекст SELinux остался без изменений (неограниченный)

Затем мы вернулись к учётной записи своего пользователя. (рис. 1).

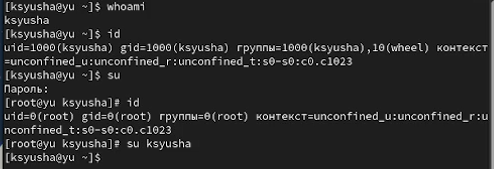


Рис. 1: Выполнили пункты 1-4 из раздела 2.4.1 (Переключение учётных записей пользователей)

Просмотрели в безопасном режиме файл /etc/sudoers, используя, sudo -i visudo.

visudo используется вместо любого редактора, потому что он проверяет синтаксис перед сохранением. Ошибка в /etc/sudoers, допущенная в обычном редакторе, полностью отключает sudo, исправить её будет невозможно без доступа root другими способами. Например sudo EDITOR=mcedit visudo — меняет редактор, но сохраняет проверку синтаксиса.

Убедились, что в открытом с помощью visudo файле присутствует строка %wheel ALL=(ALL) ALL

Строка wheel— ключевой механизм делегирования прав администратора в системе. Пользователь, добавленный в группу wheel, может получить полный контроль над системой через sudo, что безопаснее, чем работа напрямую из-под root.(рис. 2).

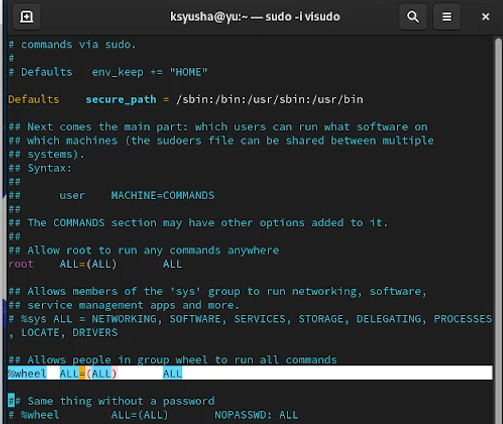


Рис. 2: Выполнили пункты 5 и 6 из раздела 2.4.1 (Переключение учётных записей пользователей)

Создали пользователя alice, входящего в группу wheel: sudo -i useradd -G wheel alice

Убедились, что пользователь alice добавлен в группу wheel, введя id alice

Задали пароль для пользователя alice, набрав sudo -i passwd alice. Позже переключились на учётную запись пользователя alice: su alice(рис. 3).

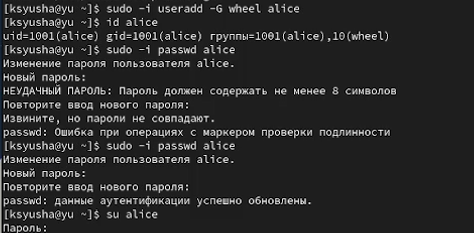


Рис. 3: Выполнили пункты 7-10 из раздела 2.4.1 (Переключение учётных записей пользователей)

Создали пользователя bob: sudo useradd bob. Затем ввели пароль при запросе. Проверили, что пользователь bob создан. Установили пароль для пользователя bob: sudo passwd bob. Просмотрели, в какие группы входит пользователь bob: id bob (рис. 4).

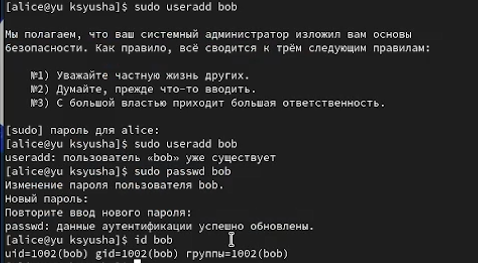


Рис. 4: Выполнили пункты 11-13 из раздела 2.4.1 (Переключение учётных записей пользователей)

Переключились в терминале на учётную запись пользователя root: su и открыли файл конфигурации /etc/login.defs (рис. 5).



Рис. 5: Выполнили пункты 1 и 2 из раздела 2.4.2 (Создание учётных записей пользователей)

Открыли файл конфигурации /etc/login.defs для редактирования: vim /etc/login.defs . Изменили несколько параметров. Например, нашли параметр CREATE\_HOME и убедились, что он установлен в значение yes. Также установили параметр USERGROUPS\_ENAB no Это позволит не добавлять нового пользователя в группу с тем же именем, что и пользователь, а использовать группу users (рис. 6).

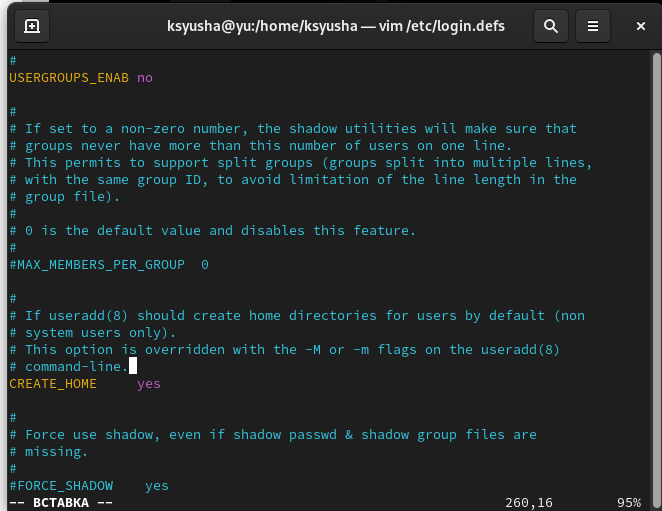


Рис. 6: Выполнили пункт 2 из раздела 2.4.2 (Создание учётных записей пользователей)

Перешли в каталог /etc/skel: cd /etc/skel. Создали каталоги Pictures и Documents. Затем изменили содержимое файла .bashrc, добавив строку export EDITOR=/usr/bin/mceditor Эта запись означает, что редактор mceditor будет уста- новлен по умолчанию для инструментов, которые нуждаются в изменении текстовых файлов (рис. 7).

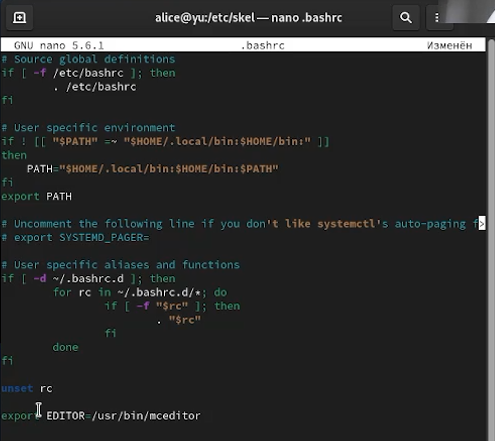


Рис. 7: Выполнили пункт 3 и 4 из раздела 2.4.2 (Создание учётных записей пользователей)

Переключились в терминале на учётную запись пользователя alice. Используя утилиту useradd, создали пользователя carol. Установили пароль для пользователя carol.

Пользователь carol имеет базовые права для работы в своей домашней директории и с файлами, к которым у группы users есть доступ. Она не может повышать свои привилегии до root. Её основная группа — users (gid=100);

также убедились, что каталоги Pictures и Documents были созданы в домашнем каталоге пользователя carol(рис. 8).

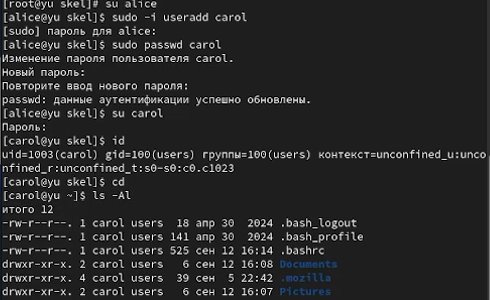


Рис. 8: Выполнили пункт 5-8 из раздела 2.4.2 (Создание учётных записей пользователей)

Переключились в терминале на учётную запись пользователя alice

Пароль пользователя carol надежно защищен современным алгоритмом хеширования SHA-512 с использованием 100000 раундов шифрования. Политика паролей для этой учетной записи настроена так: пароль можно менять когда угодно, его срок действия практически не ограничен, но система будет напоминать о смене за 7 дней, если срок все же истечет. Позже изменили свойства пароля пользователя carol следующим образом: sudo passwd -n 30 -w 3 -x 90 carol В этой записи срок действия пароля истекает через 90 дней (-x 90). За три дня до истечения срока действия пользователь получит предупреждение (-w 3). Убедились в изменении в строке с данными о пароле пользователя carol в файле /etc/shadow . Убедились, что идентификатор alice существует во всех трёх файлах, и что идентификатор carol существует не во всех трёх файлах (рис. 9).

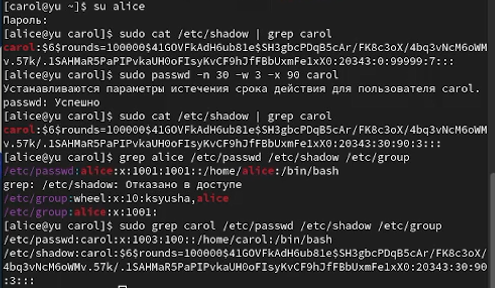


Рис. 9: Выполнили пункт 10-14 из раздела 2.4.2 (Создание учётных записей пользователей)

Находясь под учётной записью пользователя alice, создали группы main и third. Далее использовали usermod для добавления пользователей alice и bob в группу main, а carol, dan, dave и david — в группу third. Убедились, что пользователь carol правильно добавлен в группу third. Пользователю carol была назначена основная группа с идентификатором gid = 100 (users), а также он входит во вторичную группу third (GID=1004). Пользователь bob имеет основную группу bob (GID=1002) и входит во вторичную группу main (GID=1003). Пользователь alice, чья основная группа — alice (GID=1001), является участником двух вторичных групп: wheel (GID=10) и main (GID=1003). Таким образом, среди анализируемых пользователей только alice обладает административными полномочиями.([рис.@fig:010]).

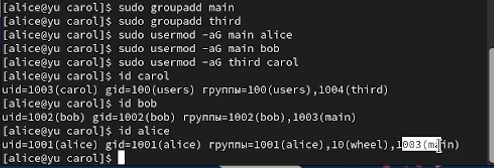


Рис. 10: была выполнена работа с группами

# 4 Ответы на контрольные вопросы

**1. Команды для получения информации о пользователе и группах:**

* id - показывает UID, GID и список групп текущего пользователя
* id <username> - показывает информацию для указанного пользователя
* groups <username> - отображает группы пользователя
* cat /etc/passwd | grep <username> - показывает запись пользователя
* cat /etc/group | grep <username> - показывает группы пользователя

**2. UID пользователя root:**

Пользователь root имеет UID=0. Узнать можно командами:

* id root → uid=0(root)
* cat /etc/passwd | grep root → root:x:0:0:root:/root:/bin/bash

**3. Различие между su и sudo:**

* su - переключение на другого пользователя (требует пароль целевого пользователя)
* sudo - выполнение команды с правами другого пользователя (обычно root) с проверкой прав через /etc/sudoers

**4. Конфигурационный файл sudo:**

Параметры sudo определяются в файле /etc/sudoers

**5. Безопасное изменение конфигурации sudo:**

Команда visudo - открывает /etc/sudoers с проверкой синтаксиса перед сохранением

**6. Группа для полного администрирования:**

Пользователь должен быть членом группы wheel (в RHEL/CentOS) или sudo (в Debian/Ubuntu)

**7. Файлы параметров создания учётных записей:**

* /etc/login.defs - настройки паролей, UID/GID диапазоны
* /etc/default/useradd - параметры по умолчанию
* /etc/skel/ - шаблоны файлов для домашних каталогов

**8. Хранение информации о группах:**

Информация хранится в:

* /etc/passwd - первичная группа (4 поле)
* /etc/group - дополнительные группы

Пример для alice:

alice:x:1001:1001:Alice:/home/alice:/bin/bash - первичная группа 1001 (alice)

В /etc/group: wheel:x:10:alice и main:x:1003:alice - дополнительные группы

**9. Команды для изменения информации о пароле:**

* chage - изменение параметров старения пароля
* passwd - изменение пароля
* usermod - изменение параметров пользователя

**10. Команда для изменения /etc/group:**

Прямое редактирование не рекомендуется. Следует использовать:

* groupadd, groupmod, groupdel - для безопасного управления группами
* usermod -G - для изменения членства в группах

Причина: системные утилиты обеспечивают корректность формата файла и предотвращают ошибки синтаксиса.

# 5 Выводы

В ходе лаборатоной работы мы получили представление о работе с учётными записями пользователей и группамипользователей в операционной системе типа Linux.