Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Ильин Андрей Владимирович

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# 2 Задачи

1. Создать, настроить пользователя guest и изучить информацию о пользователе.
2. Создать и изучить дериктории, провести эксперименты с правами доступа.
3. Заполнить таблицы “Установленные права и разрешённые действия” и “Минимальные права для совершения операций”.

# 3 Теоретическое введение

## 3.1 Термины

* Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями. [1]
* Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. [2]

## 3.2 Окружение

* Rocky Linux - это корпоративная операционная система с открытым исходным кодом, разработанная таким образом, чтобы быть на 100% совместимой с Red Hat Enterprise Linux. Он находится в стадии интенсивной разработки сообществом. [3]
* Git - это распределенное программное обеспечение для контроля версиями. [4]
* VirtualBox - это кросс-платформенное ПО для виртуализации x86 и AMD64/Intel64 с открытым кодом для корпоративного и домашнего использования. [5]

# 4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest. Зададим пароль для пользователя guest, после чего выйдем из текщего пользователя. (рис. [1](#fig:001))

sudo useradd guest  
sudo passwd guest  
logout

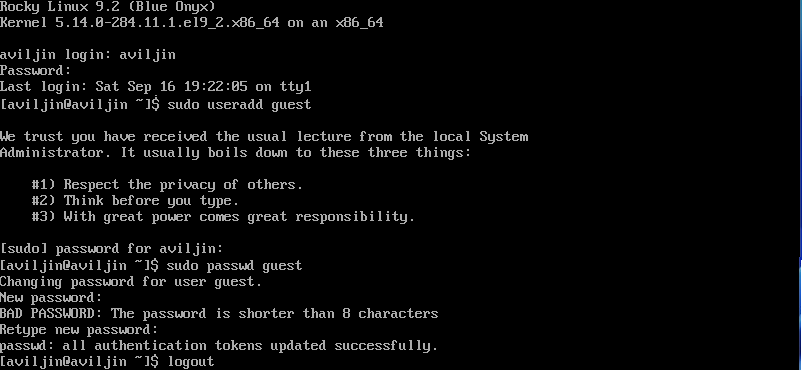


Figure 1: Пользователь guest

1. Залогинимся под новым пользователем. Определим директорию, в которой находимся: директория является домашней. Уточним имя пользователя, используя whoami. Уточним имя, группу, а также группы, куда входит пользователь, командой id. Вспользуемся командой groups. Просмотрим файл /etc/passwd. (рис. [2](#fig:002))

pwd  
whoami  
id  
groups  
cat /etc/passwd | grep guest

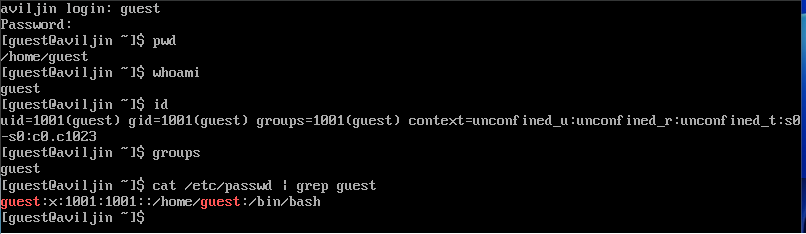


Figure 2: Изучение пользователя

1. Определим существующие в системе директории. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home. Создадим в домашней директории поддиректорию dir1, определим командами, какие права доступа и расширенные атрибуты она имеет. (рис. [3](#fig:003))

ls -l /home/  
lsattr /home  
mkdir dir1  
ls -l  
lsattr

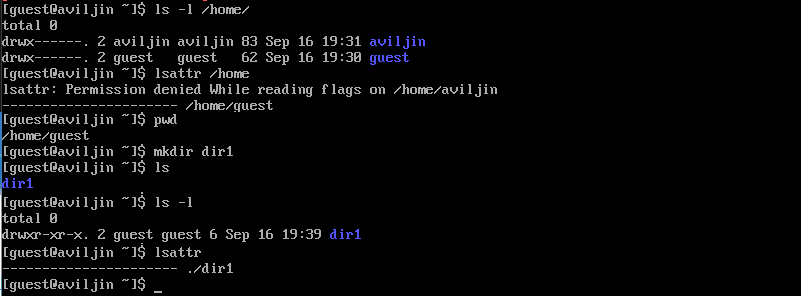


Figure 3: Проверка директории /home и созданной dir1

1. Cнимем с директории dir1 все атрибуты. Попытаемся создать в директории dir1 файл file1. (рис. [4](#fig:004))

chmod 000 dir1  
ls -l  
echo "test" > /home/guest/dir1/file1  
ls -l /home/guest/dir1

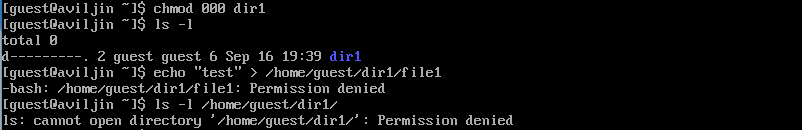


Figure 4: Права доступа

1. Заполним таблицу «Установленные права и разрешённые действия» [6]. (рис. [5](#fig:005), [6](#fig:006), [7](#fig:007))



Figure 5: Эксперименты с правами доступа (1)

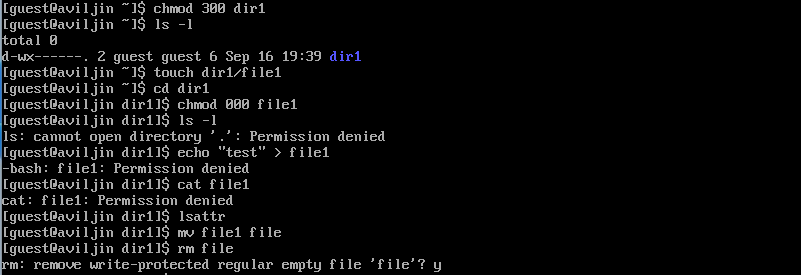


Figure 6: Эксперименты с правами доступа (2)

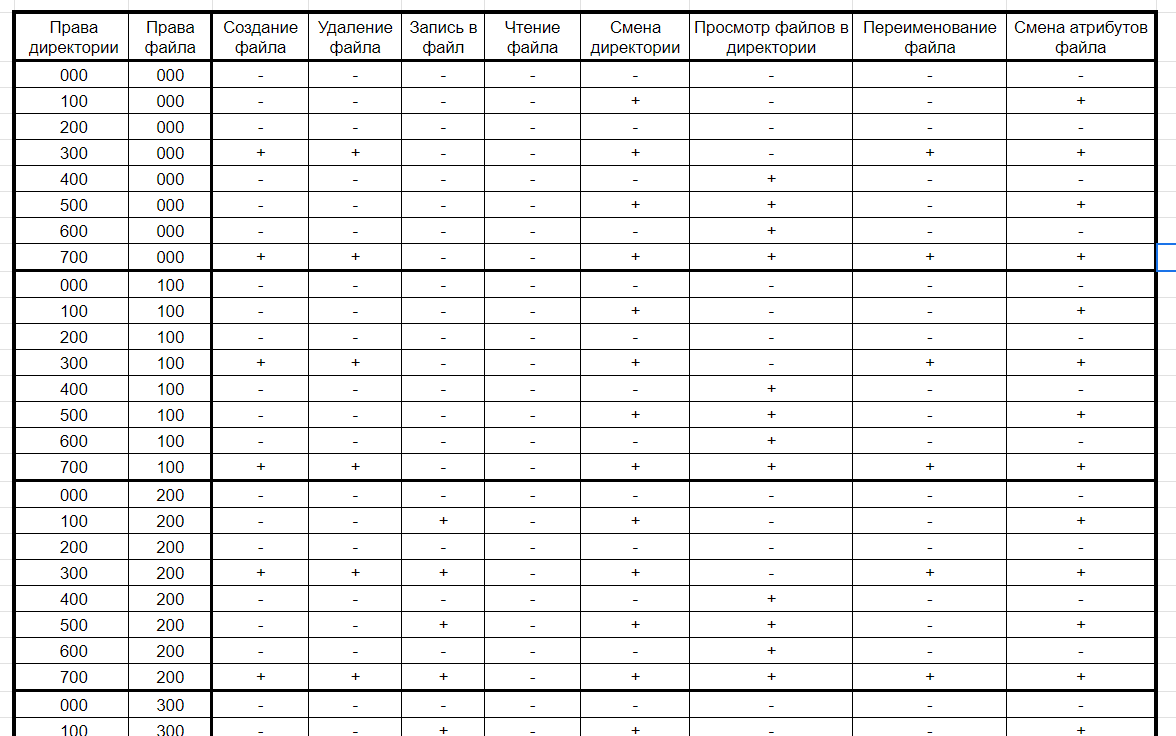


Figure 7: Фрагмент таблицы «Установленные права и разрешённые действия»

1. Заполним таблицу «Минимальные права для совершения операций» [6]. (рис. [8](#fig:008))

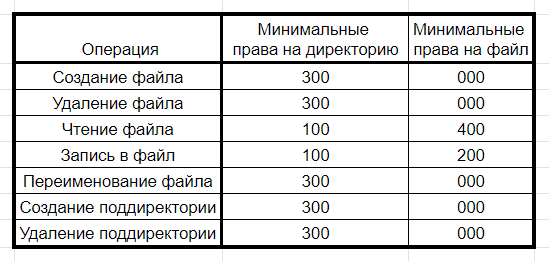


Figure 8: Таблицы «Минимальные права для совершения операцийя»

# 5 Анализ результатов

Работа выполненна без непредвиденных проблем в соответствии с руководством. Ошибок и сбоев не произошло.

# 6 Выводы

В рамках лабораторной работы был создан новый пользовтель guest. На примере данного пользователя мы разобрали базовые команды, изучили информацию о пользователе. Также подробно разобрали права доступа.

# Список литературы

1. Терминал Linux [Электронный ресурс]. URL: <{https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%20(%D0%B8%D0%BB%D0%B8%20%C2%ABBash%C2%BB%2C,%D1%81%20%D1%84%D0%B0%D0%B9%D0%BB%D0%B0%D0%BC%D0%B8%20%D0%B8%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8}>.

2. Права доступа [Электронный ресурс]. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.

3. Документация Rocky Linux [Электронный ресурс]. URL: <https://docs.rockylinux.org/>.

4. Git-Guides [Электронный ресурс]. URL: <https://github.com/git-guides>.

5. VirtualBox [Электронный ресурс]. URL: <https://www.virtualbox.org/>.

6. Полная таблица «Установленные права и разрешённые действия» [Электронный ресурс]. URL: <https://github.com/av-ilin/study_2023-2024_infosec.git>.