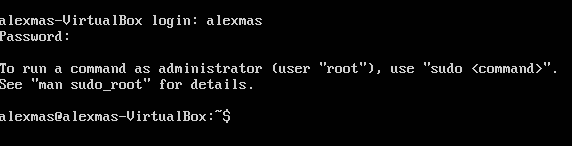
Маслов А.Н. ИД23-1  
Сетевые Системы и Приложения  
Семинар 8

Практическая работа – Управление правами доступа

Основные задания:

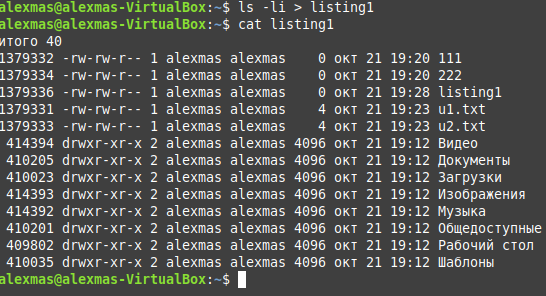
1. Войти в систему с собственной учетной записью:



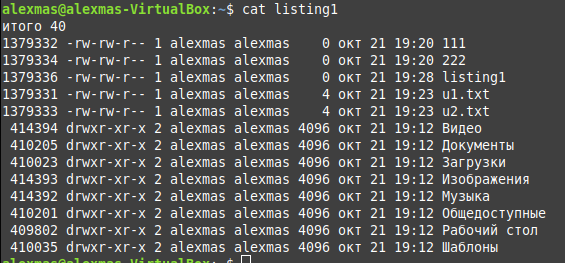
1. Создать в домашнем каталоге 2-3 файла произвольного содержания (имена файлов - u1, u2, u3):



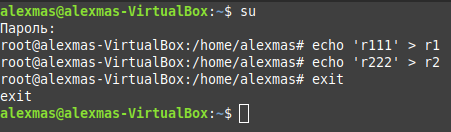
1. Получить развернутый список файлов домашнего каталога и сохранить его в файле listing1:



1. Просмотреть файл listing1, обратив внимание на поля прав доступа, владельца и группы



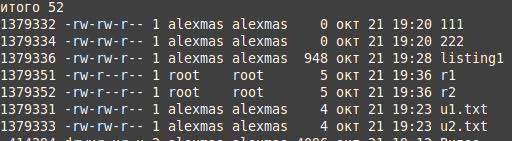
1. Повторить п. 2 от имени пользователя root в новом сеансе или по команде su (имена файлов - r1, r2, r3). Завершить сеанс root:



1. Повторить п.3, результат дописать в файл listing1:



1. Открыть файл listing1 и сравнить права доступа для файлов, созданных от вашего имени и от имени суперпользователя:



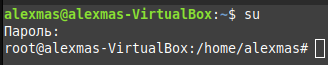
1. Cоздать директорию labs в корневом каталоге. В нем создать каталоги library и tests:







1. Открыть сеанс root:



1. Перейти в каталог /home/ваша\_учетная\_запись:



1. Изменить права доступа к файлам u1 и r1 следующим образом:

u1: запретить запись для владельца и группы

r1: разрешить запись для всех



1. Переключиться в сеанс пользователя и изменить содержимое файлов u1 и r1. Сохранить изменения:





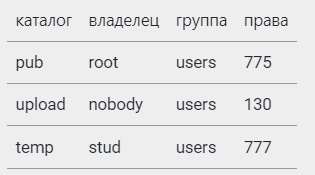
1. Перейти в сеанс root и изменить владельца файлов u1 и u2 на root, а группу - на stud

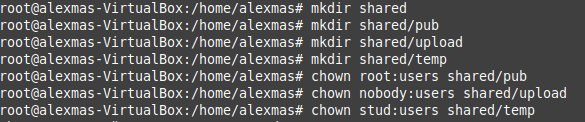


1. Из tty1 попробовать изменить файл u2



1. Из tty2 создать каталоги /home/shared, home/shared/pub, /home/shared/upload, /home/shared/temp. Установить на них следующие права:









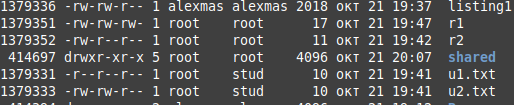
* 1. Выполнить копирование, чтение, удаление файлов u1, u2, u3, r1, r2, r3 в каталоги, созданные в п. 15 из сеансов root, stud и вашего. Сравнить и проанализировать результаты.

Для каталога pub у пользователя root и пользователей группы users будет доступ ко всем правам, а у других только к просмотру файлов и переходу в каталог.

Для каталога temp все права есть у всех пользователей.

Для каталога upload nobody может только переходить в каталог, а пользователи группы users переходить в каталог и добавлять и удалять файлы. У других каких-либо прав нет, кроме root.





Задания для самостоятельной работы:

1. В текущей папке создать файл hello следующего содержания.

Изображение выглядит как текст, Шрифт, программное обеспечение, линия

Автоматически созданное описание

1. Выполнить следующие действия и проанализировать результаты:

* набрать в командной строке имя файла hello и нажать Enter
* набрать в командной строке sh hello и нажать Enter
* установить для файла hello права на исполнение (x), ввести имя файла в командной строке (./hello) и нажать Enter

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, Графика

Автоматически созданное описание

1. Разберитесь, как в Linux можно организовать специальные каталоги-файлообменники - такие, что создавать в них файлы могут любые пользователи, а удалять - только владельцы файлов (тот, кто их создал).

Используя: chmod +t

Контрольные вопросы:

1. Зачем у файла нужны атрибуты доступа?

Защита данных и разделение прав

1. Для каких трех категории пользователей задаются права доступа каждого конкретного файла?

Владелец (u)

Группа (g)

Другие (o)

1. Для чего в UNIX-подобных системах используются пользовательские группы?

Для упрощения управления правами доступа.

1. Какие действия с файлами регламентируются правами доступа?

Чтение – r

Запись – w

Выполнение – x

1. На какой системе счисления основывается числовое представление прав доступа?

На восьмеричной.

1. Чем отличается назначение прав доступа к простому файлу и к директории?

Чтение для файлов позволяет просматривать содержимое файла, а для каталога – видеть список файлов в нем.

Запись для файлов позволяет изменять содержимое файла, а для каталога – изменять его содержимое.

Выполнение для файлов позволяет запускать программу или скрипт, а для каталога – переходить в каталог.

1. Кто может менять права доступа определенного файла?

Владелец файла и суперпользователь.

1. Каково назначение специальных битов прав доступа?

Setuid (u+s) – позволяет пользователю запускать исполняемый файл с правами владельца этого файла.

Setgid (g+s) – позволяет пользователю запускать исполняемый файл с правами группы этого файла.

Sticky Bit (+t) - файлы в каталоге могут быть удалены только их владельцем.