|  |  |
| --- | --- |
| **Gerb-BMSTU_01** | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

**ФАКУЛЬТЕТ \_ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**КАФЕДРА \_\_\_\_КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ (ИУ6)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**НАПРАВЛЕНИЕ ПОДГОТОВКИ \_\_09.03.01 Информатика и Вычислительная техника \_\_\_\_\_**

**Отчет**

**по лабораторной работе № \_6\_**

**Дисциплина:** Операционные системы

**Название лабораторной работы:** Исследование методов защиты

операционных систем и данных

Студент гр. **\_**ИУ6-52б**\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_**И.С. Марчук**\_\_\_**

(Подпись, дата) (И.О. Фамилия)

Преподаватель  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Подпись, дата) (И.О. Фамилия)

Москва, 2021

**Цель работы** - исследование методов защиты информации в Linux.

**Порядок выполнения работы.**

1. Создать нового пользователя и просмотреть содержимое его домашнего каталога.

useradd имя – добавление пользователя,

passwd имя – изменение пароля пользователя,

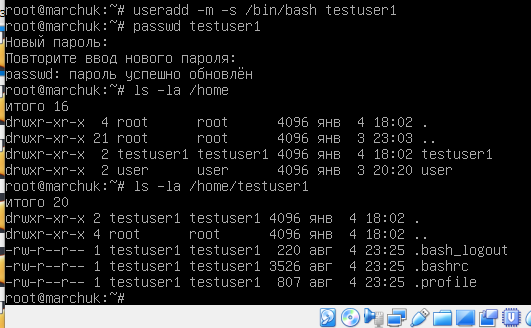


Рисунок 1 - содержимое домашнего каталога пользователя

1. Задать alias “ll” для команды “ls -l”. Изменить вид приглашения командной строки в файле “.bashrc”.

Изменим и раскомментируем строку “PS1=...” в том же файле.

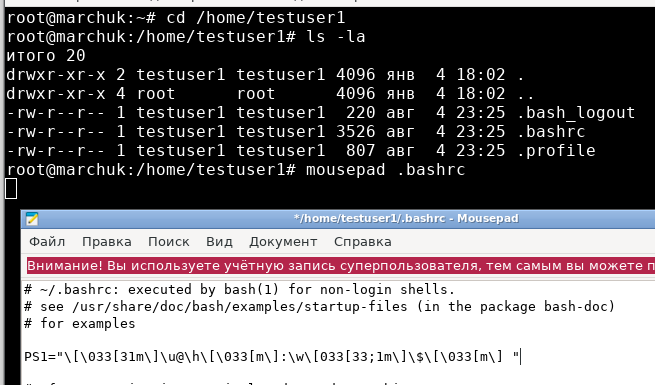


Рисунок 2 - настройка bash пользователя

1. Просмотреть учетные данные всех пользователей.

Откроем файл “/etc/passwd” в leafpad.

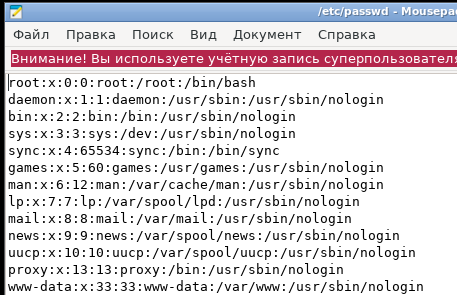


Рисунок 3 - просмотр учетных данных пользователей

1. Настроить для пользователей группы и просмотреть список групп.

groupadd имя – добавление новой группы

usermod – совокупность команд для задания пользователям групп

Список групп можно получить из файла “/etc/groups”.

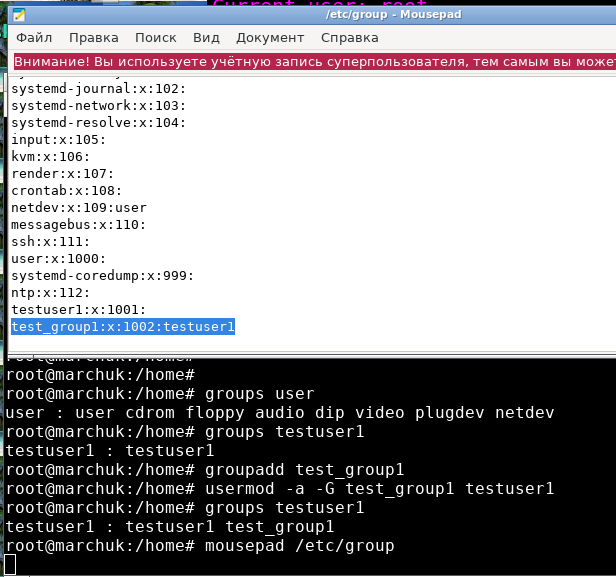


Рисунок 4 - работа с группами пользователей

1. отнять право “прочих” пользователей редактировать домашний каталог созданного пользователя.

chmod o-rw путь – отнимает права на чтение и запись у группы пользователей «прочие» для указанного пути

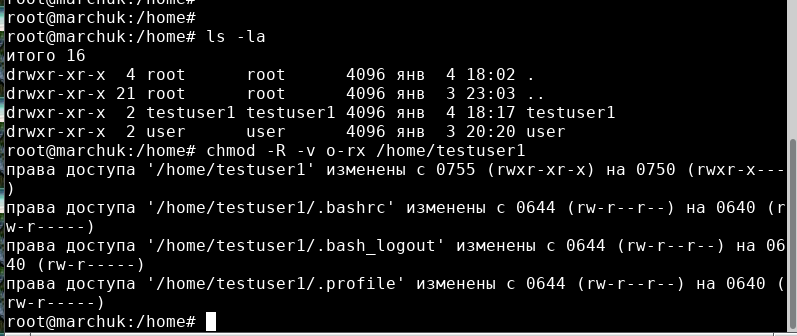


Рисунок 5 - изменение прав доступа к домашнему каталогу

1. установить и запустить Selinux.

После установки с помощью apt и активации убедимся в работоспособности selinux с помощью команды “sestatus”.

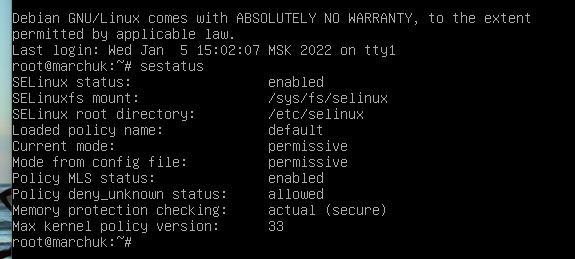


Рисунок 7 - статус selinux

1. Просмотреть контекст безопасности для пользователя и процессов.

**Практическая часть:** При работе selinux контекст безопасности отображается при вызове команды “id” и “ps”.

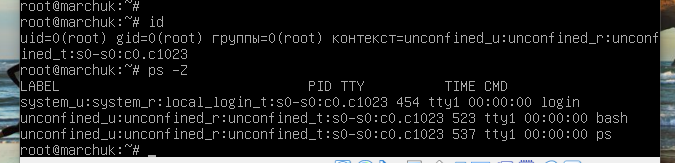


Рисунок 8 - контекст безопасности пользователя и безопасности процессов

**Задание к ЛР**

Задача:

с помощью команд, не пользуясь ACL и SELinux!

1 Создать несколько пользователей, включая пользователя от имени которого работает сервис распознавания.

2 Для каждого пользователя создать каталоги:

◦ in — для файлов, предназначенных для распознавания

◦ out — для распознанных файлов

3 Настроить доступ к файлам и каталогам. Пользователи не должны иметь доступ к файлам других пользователей. Не забудьте дать права сервису распознавания.

4 Создать каталог, в который выкладывают файлы пользователи группы «DSP». Только пользователи этой группы должны иметь к нему доступ.

5 Создать файл протокола, в который записывает сообщения сервис распознавания. Все пользователи должны иметь права на чтение этого файла.

**Практическая часть:** создадим пользователей командами

“useradd -m user1”,

“useradd -m user2” ,

“useradd -m user3” ,

“useradd -m scanner”

и описанный в задании каталоги и файлы для каждого пользователя командами ниже, запустив их в домашнем каталоге каждого пользователя (кроме scanner)

“mkdir docs”,

“mkdir docs/in”,

“mkdir docs/out”

Для scanner создадим папку “DSP” и файл лога командой “touch scan.log”.



Рисунок 12 - структура каталогов

Создадим группу «comp\_group» (команда «groupadd comp\_group») и добавим в группу “comp\_group” пользователей 2, 3 и сканер.

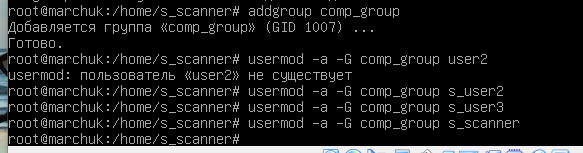


Рисунок 13 - настройка группы «DspGroup»

Сканер добавим в группы всех пользователей, чтобы он имел доступ к их файлам.



Рисунок 14 - настройка групп пользователей



Рисунок 14 - группа «DspGroup»

Я переназначил для папок «DSP» и «docs», «in», «out» пользователей, права группы-хозяина полный доступ (chmod g+rwx) а для группы-остальных пользователей отключил доступ (chmod o-rwx). Для лога сканера, группе-хозяина и группе-остальных, оставил только права на чтение («chmod g-wx scan.log» и «chmod o-wx scan.log»).

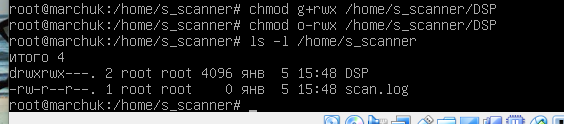


Рисунок 14 - разрешения для папки сканера

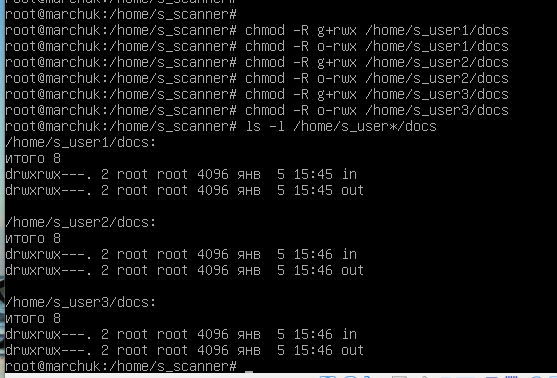


Рисунок 14 - разрешения для папок пользователей

**Вывод:** Я изучил методы защиты данных в операционных системах семейства Linux в соответствии с их моделями управления доступом.