



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

О т ч е т
по лабораторной работе № 6

Дисциплина: Операционные системы

Название лабораторной работы: Исследование методов защиты
операционных систем и данных

Студент гр. ИУ6-526 _____ 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,

```
root@marchuk:~# useradd -m -s /bin/bash testuser1
root@marchuk:~# passwd testuser1
Новый пароль:
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
root@marchuk:~# ls -la /home
итого 16
drwxr-xr-x  4 root      root      4096 янв  4 18:02 .
drwxr-xr-x 21 root      root      4096 янв  3 23:03 ..
drwxr-xr-x  2 testuser1 testuser1 4096 янв  4 18:02 testuser1
drwxr-xr-x  2 user      user      4096 янв  3 20:20 user
root@marchuk:~# ls -la /home/testuser1
итого 20
drwxr-xr-x  2 testuser1 testuser1 4096 янв  4 18:02 .
drwxr-xr-x  4 root      root      4096 янв  4 18:02 ..
-rw-r--r--  1 testuser1 testuser1  220 авг  4 23:25 .bash_logout
-rw-r--r--  1 testuser1 testuser1 3526 авг  4 23:25 .bashrc
-rw-r--r--  1 testuser1 testuser1  807 авг  4 23:25 .profile
root@marchuk:~#
```

Рисунок 1 - содержимое домашнего каталога пользователя

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

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

```
root@marchuk:~# cd /home/testuser1
root@marchuk:/home/testuser1# ls -la
итого 20
drwxr-xr-x  2 testuser1 testuser1 4096 янв  4 18:02 .
drwxr-xr-x  4 root      root      4096 янв  4 18:02 ..
-rw-r--r--  1 testuser1 testuser1  220 авг  4 23:25 .bash_logout
-rw-r--r--  1 testuser1 testuser1 3526 авг  4 23:25 .bashrc
-rw-r--r--  1 testuser1 testuser1  807 авг  4 23:25 .profile
root@marchuk:/home/testuser1# mousepad .bashrc
```

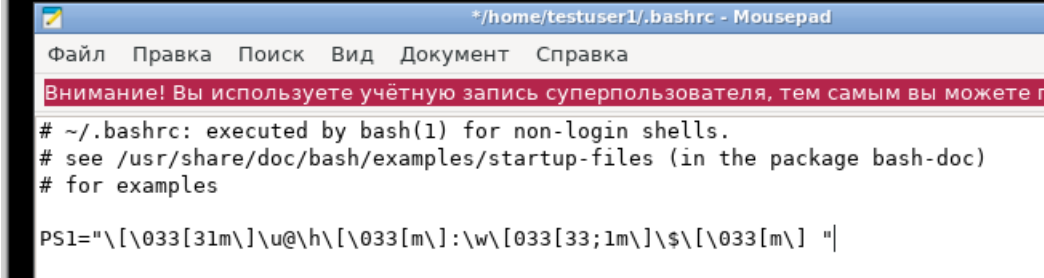
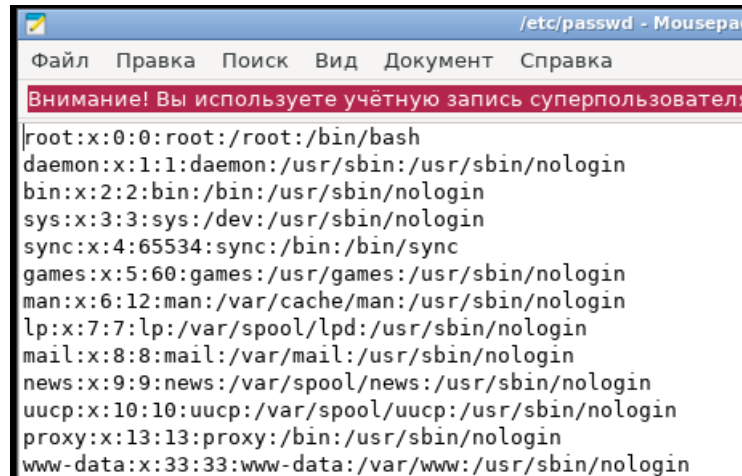


Рисунок 2 - настройка bash пользователя

3. Просмотреть учетные данные всех пользователей.

Откроем файл “/etc/passwd” в leafpad.



The screenshot shows the Mousepad text editor with the file /etc/passwd open. The menu bar includes 'Файл', 'Правка', 'Поиск', 'Вид', 'Документ', and 'Справка'. A red warning bar at the top states: 'Внимание! Вы используете учётную запись суперпользователя'. The main text area displays the contents of the /etc/passwd file, listing system users (root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data) and their associated home directories and shells. The entry 'test_group1:x:1002:testuser1' is highlighted in blue.

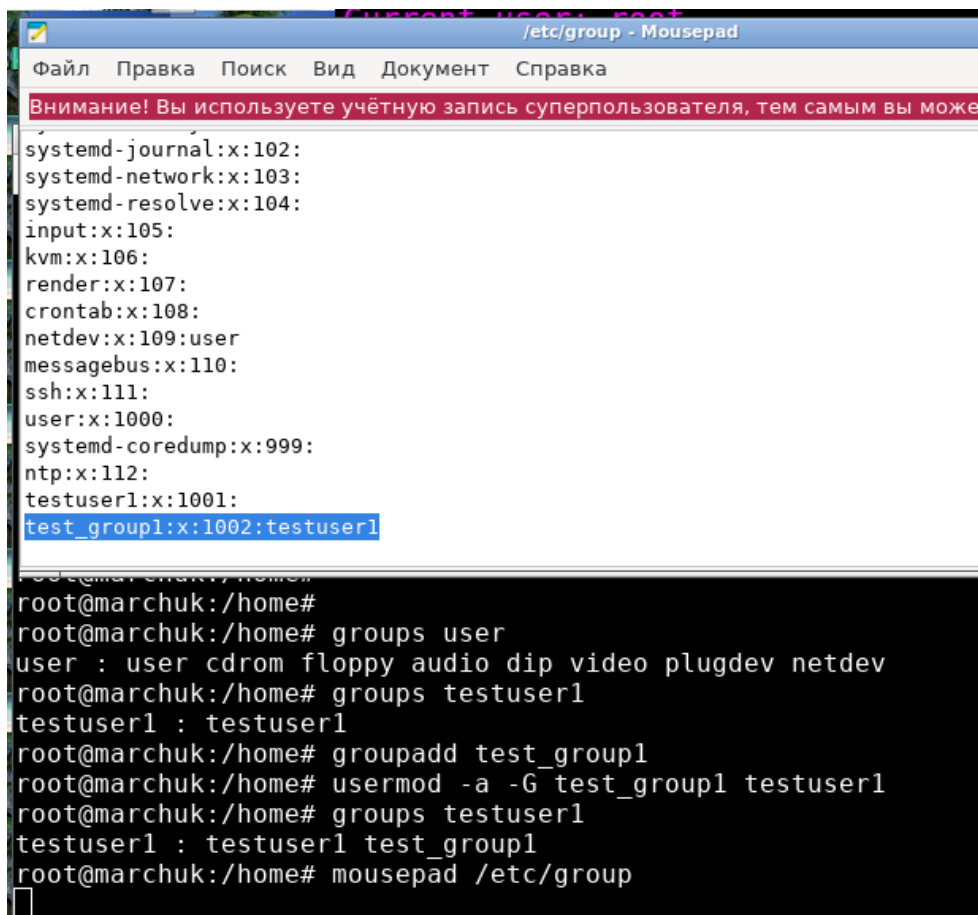
Рисунок 3 - просмотр учетных данных пользователей

4. 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”.



The screenshot is divided into two parts. The top part shows the Mousepad editor with the file /etc/group open. The menu bar is the same as in the previous screenshot. The red warning bar is present. The text area shows the contents of the /etc/group file, listing system groups (systemd-journal, systemd-network, systemd-resolve, input, kvm, render, crontab, netdev, messagebus, ssh, user, systemd-coredump, ntp, testuser1, test_group1) and their associated users. The entry 'test_group1:x:1002:testuser1' is highlighted in blue. The bottom part shows a terminal window with the following commands and output:

```
root@marchuk:/home#  
root@marchuk:/home# groups user  
user : user cdrom floppy audio dip video plugdev netdev  
root@marchuk:/home# groups testuser1  
testuser1 : testuser1  
root@marchuk:/home# groupadd test_group1  
root@marchuk:/home# usermod -a -G test_group1 testuser1  
root@marchuk:/home# groups testuser1  
testuser1 : testuser1 test_group1  
root@marchuk:/home# mousepad /etc/group
```

Рисунок 4 - работа с группами пользователей

5. 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

```
root@marchuk:/home#  
root@marchuk:/home# ls -la  
итого 16  
drwxr-xr-x  4 root      root      4096 янв  4 18:02 .  
drwxr-xr-x 21 root      root      4096 янв  3 23:03 ..  
drwxr-xr-x  2 testuser1 testuser1 4096 янв  4 18:17 testuser1  
drwxr-xr-x  2 user       user       4096 янв  3 20:20 user  
root@marchuk:/home# chmod -R -v o-rx /home/testuser1  
права доступа '/home/testuser1' изменены с 0755 (rwxr-xr-x) на 0750 (rwxr-x---)  
)  
права доступа '/home/testuser1/.bashrc' изменены с 0644 (rw-r--r--) на 0640 (rw-r-----)  
права доступа '/home/testuser1/.bash_logout' изменены с 0644 (rw-r--r--) на 0640 (rw-r-----)  
права доступа '/home/testuser1/.profile' изменены с 0644 (rw-r--r--) на 0640 (rw-r-----)  
root@marchuk:/home#
```

Рисунок 5 - изменение прав доступа к домашнему каталогу

6. установить и запустить Selinux.

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

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Jan  5 15:02:07 MSK 2022 on tty1  
root@marchuk:~# sestatus  
SELinux status:                enabled  
SELinuxfs mount:                /sys/fs/selinux  
SELinux root directory:         /etc/selinux  
Loaded policy name:              default  
Current mode:                   permissive  
Mode from config file:          permissive  
Policy MLS status:              enabled  
Policy deny_unknown status:     allowed  
Memory protection checking:     actual (secure)  
Max kernel policy version:      33  
root@marchuk:~#
```

Рисунок 7 - статус selinux

7. Просмотреть контекст безопасности для пользователя и процессов.

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

```
root@marchuk:~#  
root@marchuk:~# id  
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
root@marchuk:~# ps -Z  
LABEL                                PID TTY          TIME CMD  
system_u:system_r:local_login_t:s0-s0:c0.c1023 454 tty1 00:00:00 login  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 523 tty1 00:00:00 bash  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 537 tty1 00:00:00 ps  
root@marchuk:~#
```

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”.

```
root@marchuk:/home/s_scanner#  
root@marchuk:/home/s_scanner# tree /home/  
/home/  
├── s_scanner  
│   ├── DSP  
│   └── scan.log  
├── s_user1  
│   └── docs  
│       ├── in  
│       └── out  
├── s_user2  
│   └── docs  
│       ├── in  
│       └── out  
├── s_user3  
│   └── docs  
│       ├── in  
│       └── out  
├── testuser1  
├── user  
└── mysoftlink -> /mnt/d1/myFolder/file.txt  
  
16 directories, 2 files  
root@marchuk:/home/s_scanner#
```

Рисунок 12 - структура каталогов

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

```
root@marchuk:/home/s_scanner# addgroup comp_group  
Добавляется группа «comp_group» (GID 1007) ...  
Готово.  
root@marchuk:/home/s_scanner# usermod -a -G comp_group user2  
usermod: пользователь «user2» не существует  
root@marchuk:/home/s_scanner# usermod -a -G comp_group s_user2  
root@marchuk:/home/s_scanner# usermod -a -G comp_group s_user3  
root@marchuk:/home/s_scanner# usermod -a -G comp_group s_scanner  
root@marchuk:/home/s_scanner#
```

Рисунок 13 - настройка группы «DspGroup»

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

```
root@marchuk:/home/s_scanner# usermod -a -G s_user1,s_user2,s_user3 s_scanner  
root@marchuk:/home/s_scanner#
```

Рисунок 14 - настройка групп пользователей

```

root@marchuk:/home/s_scanner#
root@marchuk:/home/s_scanner# groups s_scanner
s_scanner : s_scanner s_user1 s_user2 s_user3 comp_group
root@marchuk:/home/s_scanner# grep comp_group: /etc/group
comp_group:x:1007:s_user2,s_user3,s_scanner
root@marchuk:/home/s_scanner#

```

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»).

```

root@marchuk:/home/s_scanner# chmod g+rwX /home/s_scanner/DSP
root@marchuk:/home/s_scanner# chmod o-rwx /home/s_scanner/DSP
root@marchuk:/home/s_scanner# ls -l /home/s_scanner
итого 4
drwxrwx---. 2 root root 4096 янв  5 15:48 DSP
-rw-r--r--. 1 root root    0 янв  5 15:48 scan.log
root@marchuk:/home/s_scanner#

```

Рисунок 14 - разрешения для папки сканера

```

root@marchuk:/home/s_scanner#
root@marchuk:/home/s_scanner# chmod -R g+rwX /home/s_user1/docs
root@marchuk:/home/s_scanner# chmod -R o-rwx /home/s_user1/docs
root@marchuk:/home/s_scanner# chmod -R g+rwX /home/s_user2/docs
root@marchuk:/home/s_scanner# chmod -R o-rwx /home/s_user2/docs
root@marchuk:/home/s_scanner# chmod -R g+rwX /home/s_user3/docs
root@marchuk:/home/s_scanner# chmod -R o-rwx /home/s_user3/docs
root@marchuk:/home/s_scanner# ls -l /home/s_user*/docs
/home/s_user1/docs:
итого 8
drwxrwx---. 2 root root 4096 янв  5 15:45 in
drwxrwx---. 2 root root 4096 янв  5 15:45 out

/home/s_user2/docs:
итого 8
drwxrwx---. 2 root root 4096 янв  5 15:46 in
drwxrwx---. 2 root root 4096 янв  5 15:46 out

/home/s_user3/docs:
итого 8
drwxrwx---. 2 root root 4096 янв  5 15:46 in
drwxrwx---. 2 root root 4096 янв  5 15:46 out
root@marchuk:/home/s_scanner#

```

Рисунок 14 - разрешения для папок пользователей

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