



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

Название: Исследование методов защиты операционных систем и данных

Дисциплина: Операционные системы

Студент

ИУ6-52Б

(Группа)

(Подпись, дата)

С.В. Астахов

(И.О. Фамилия)

Преподаватель

А.М. Суровов

(Подпись, дата)

(И.О. Фамилия)

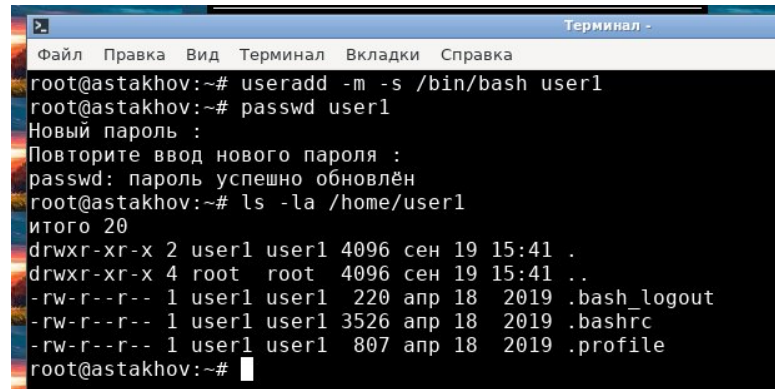
Москва, 2021

Цель работы: исследование методов защиты информации в Linux.

Вводная часть.

Задание: Создать нового пользователя и просмотреть содержимое его домашнего каталога.

Практическая часть: Для добавления пользователя воспользуемся командой “useradd”, заменим его пароль командой “passwd” и посмотрим содержимое его домашнего каталога командой “ls”.

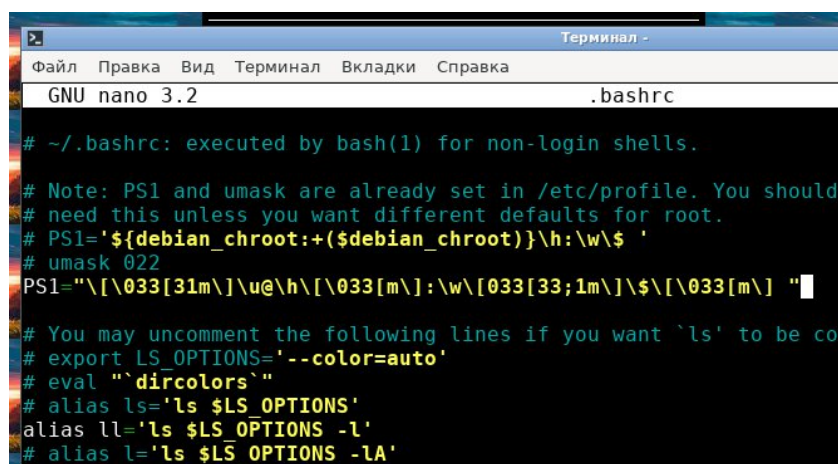


```
Терминал -
Файл  Правка  Вид  Терминал  Вкладки  Справка
root@astakhov:~# useradd -m -s /bin/bash user1
root@astakhov:~# passwd user1
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлён
root@astakhov:~# ls -la /home/user1
итого 20
drwxr-xr-x 2 user1 user1 4096 сен 19 15:41 .
drwxr-xr-x 4 root  root  4096 сен 19 15:41 ..
-rw-r--r-- 1 user1 user1  220  авг 18  2019 .bash_logout
-rw-r--r-- 1 user1 user1 3526  авг 18  2019 .bashrc
-rw-r--r-- 1 user1 user1  807  авг 18  2019 .profile
root@astakhov:~#
```

Рисунок 1 - содержимое домашнего каталога пользователя

Задание: Задать алиас “ll” для команды “ls -l”. Изменить вид приглашения командной строки.

Практическая часть: Изменим алиас команды “ls -l” в файле “.bashrc”. Изменим и раскомментируем строку “PS1=...” в том же файле.



```
Терминал -
Файл  Правка  Вид  Терминал  Вкладки  Справка
GNU nano 3.2                                .bashrc

# ~/.bashrc: executed by bash(1) for non-login shells.

# Note: PS1 and umask are already set in /etc/profile. You should
# need this unless you want different defaults for root.
# PS1='${debian_chroot:+($debian_chroot)}\h:\w\$ '
# umask 022
PS1="\[\033[31m\]\u@\h\[\033[m\]:\w\[\033[33;1m\]\$ \[\033[m\] "

# You may uncomment the following lines if you want `ls' to be col
# export LS_OPTIONS='--color=auto'
# eval "`dircolors`"
# alias ls='ls $LS_OPTIONS'
alias ll='ls $LS_OPTIONS -l'
# alias l='ls $LS_OPTIONS -lA'
```

Рисунок 2 - настройка bash пользователя

Задание: Просмотреть учетные данные всех пользователей.

Практическая часть: Откроем файл “/etc/passwd” в leafpad.

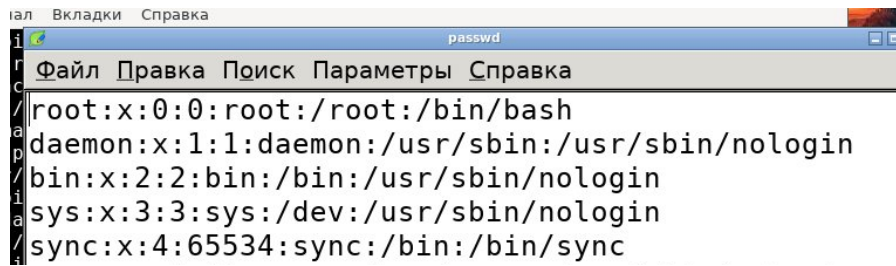


Рисунок 3 - просмотр учетных данных пользователей

Задание: Настроить для пользователей группы и просмотреть список групп.

Практическая часть: Для настройки групп пользователей воспользуемся командами “groupadd” и “usermod”. Список групп можно получить из файла “/etc/groups”.

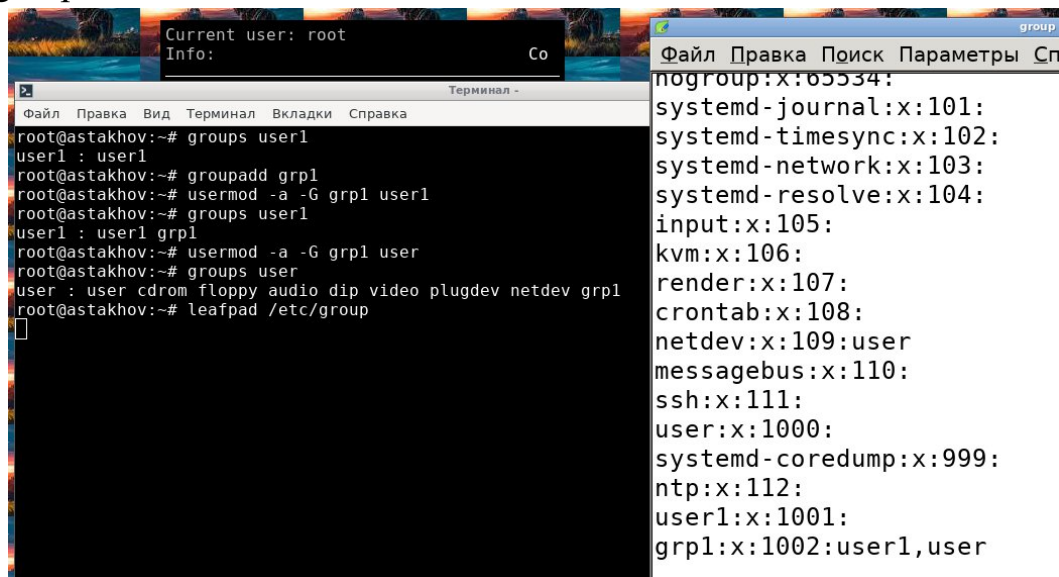


Рисунок 4 - работа с группами пользователей

Задание: отнять право “прочих” пользователей редактировать домашний каталог user1.

Практическая часть: воспользуемся командой “chmod o-...”.

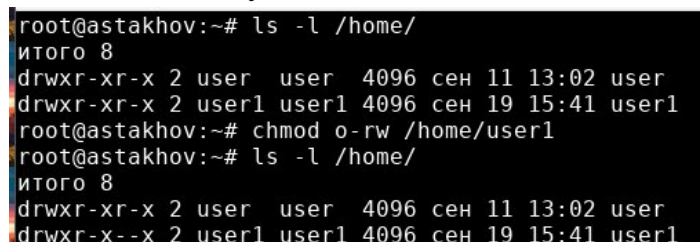
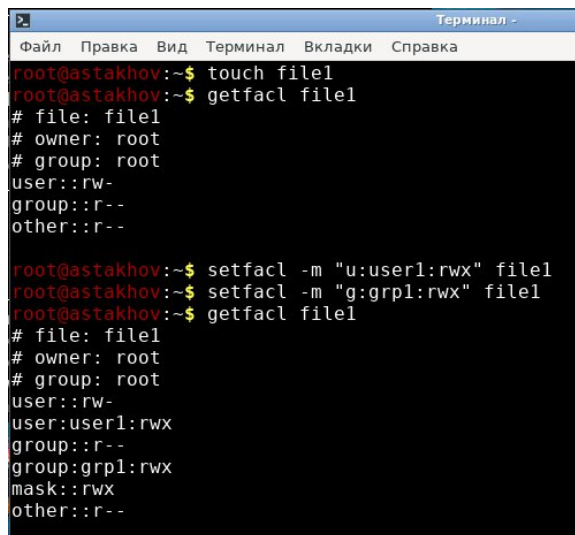


Рисунок 5 - изменение прав доступа к домашнему каталогу

Задание: Изменить с помощью ACL права доступа пользователя и группа к файлу и вывести полную информацию о правах доступа к файлу с помощью.

Практическая часть: воспользуемся командами “setfacl” и “getfacl”.



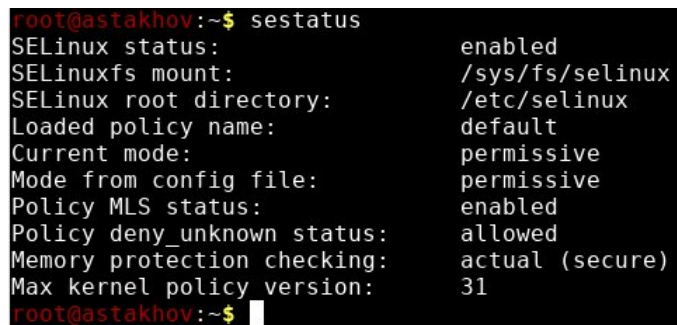
```
Терминал -
Файл  Правка  Вид  Терминал  Вкладки  Справка
root@astakhov:~$ touch file1
root@astakhov:~$ getfacl file1
# file: file1
# owner: root
# group: root
user::rw-
group::r--
other::r--

root@astakhov:~$ setfacl -m "u:user1:rw" file1
root@astakhov:~$ setfacl -m "g:grp1:rw" file1
root@astakhov:~$ getfacl file1
# file: file1
# owner: root
# group: root
user::rw-
user:user1:rw
group::r--
group:grp1:rw
mask::rw
other::r--
```

Рисунок 6 - настройка прав доступа с помощью ACL

Задание: установить и запустить Selinux.

Практическая часть: после установки с помощью apt и активации убедимся в работоспособности selinux с помощью команды “sestatus”.

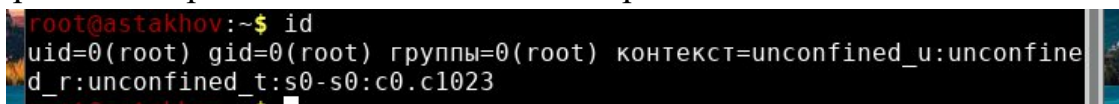


```
root@astakhov:~$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:          default
Current mode:                permissive
Mode from config file:       permissive
Policy MLS status:           enabled
Policy deny_unknown status:  allowed
Memory protection checking:  actual (secure)
Max kernel policy version:   31
root@astakhov:~$
```

Рисунок 7 - статус selinux

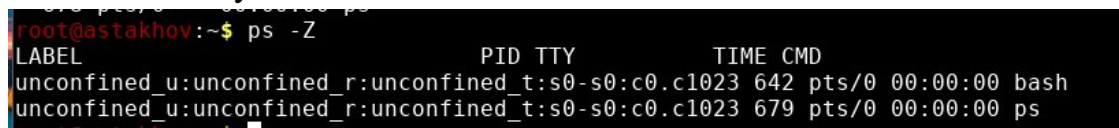
Задание: Просмотреть контекст безопасности для пользователя и процессов.

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



```
root@astakhov:~$ id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
root@astakhov:~$
```

Рисунок 8 - контекст безопасности пользователя



```
root@astakhov:~$ ps -Z
LABEL                                PID TTY          TIME CMD
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 642 pts/0 00:00:00 bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 679 pts/0 00:00:00 ps
```

Рисунок 9 - контекст безопасности процессов

Задание: Установить сервер Apache и настроить его для работы с selinux.

Практическая часть: Изначально после запуска selinux сервер не будет работать из-за блокировки 81 порта от веб-сервисов. После настройки 81 порта так же надо разрешить доступ веб-сервисов к файлам с разметкой веб-страниц.

```
root@astakhov:~$ setenforce 1
root@astakhov:~$ systemctl restart apache2
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xe" for details.
root@astakhov:~$ grep -E 'denied.*permissive=0' /var/log/audit/audit.log
type=AVC msg=audit(1632069354.000:154): avc: denied { name_bind } for pid=1633 comm="apache2" s
rc=81 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:reserved_port_t:s0 tclass=t
cp_socket permissive=0
type=AVC msg=audit(1632069354.000:155): avc: denied { name_bind } for pid=1633 comm="apache2" s
rc=81 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:reserved_port_t:s0 tclass=t
cp_socket permissive=0
root@astakhov:~$ setenforce 0
root@astakhov:~$ semanage port -a -t http_port_t -p tcp 81
libsemanage.add_user: user sddm not in password file
root@astakhov:~$ setenforce 1
root@astakhov:~$ systemctl restart apache2
root@astakhov:~$ w3m http://127.0.0.1:81 | more
Forbidden

You don't have permission to access this resource.

Apache/2.4.48 (Debian) Server at 127.0.0.1 Port 81
```

Рисунок 10 - настройка доступа к 81 порту

```
root@astakhov:~$ grep -E 'denied.*permissive=0' /var/log/audit/audit.log
type=AVC msg=audit(1632069354.000:154): avc: denied { name_bind } for pid=1633 comm="apache2" s
rc=81 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:reserved_port_t:s0 tclass=t
cp_socket permissive=0
type=AVC msg=audit(1632069354.000:155): avc: denied { name_bind } for pid=1633 comm="apache2" s
rc=81 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:reserved_port_t:s0 tclass=t
cp_socket permissive=0
type=AVC msg=audit(1632069565.103:177): avc: denied { getattr } for pid=1658 comm="apache2" pat
h="/srv/www/site2/index.html" dev="sda1" ino=164807 scontext=system_u:system_r:httpd_t:s0 tcontext
=unconfined_u:object_r:var_t:s0 tclass=file permissive=0
type=AVC msg=audit(1632069565.103:178): avc: denied { getattr } for pid=1658 comm="apache2" pat
h="/srv/www/site2/index.html" dev="sda1" ino=164807 scontext=system_u:system_r:httpd_t:s0 tcontext
=unconfined_u:object_r:var_t:s0 tclass=file permissive=0
root@astakhov:~$ setenforce 0
root@astakhov:~$ semanage fcontext -a -t httpd_sys_content_t "srv/www(/.*)?"
libsemanage.add_user: user sddm not in password file
root@astakhov:~$ restorecon -R /srv/www/
root@astakhov:~$ setenforce 1
root@astakhov:~$ w3m http://127.0.0.1:81 | more
This is site2
```

Рисунок 11 - настройка доступа к файлам с разметкой

Задание к ЛР

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

- Для каждого пользователя создать каталоги:
- in — для файлов, предназначенных для распознавания
- out — для распознанных файлов

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

- Создать каталог, в который выкладывают файлы пользователи группы «DSP». Только пользователи этой группы должны иметь к нему доступ.
- Создать файл протокола, в который записывает сообщения сервис распознавания. Все пользователи должны иметь права на чтение этого файла.

Практическая часть: создадим пользователей и описанный в задании каталоги и файлы.

```
scanner@astakhov:~$ tree /home/
/home/
├── scanner
│   ├── DSP
│   └── scan.log
├── user
│   ├── user1
│   │   └── docs
│   │       ├── in
│   │       └── out
│   ├── user2
│   │   └── docs
│   │       ├── in
│   │       └── out
│   └── user3
│       └── docs
│           ├── in
│           └── out
└── 15 directories, 1 file
```

Рисунок 12 - структура каталогов

Добавим в группу “DSP” пользователей 2, 3 и сканер, а сканер добавим в группы всех пользователей.

```
root@astakhov:/home/user3/docs$ groups scanner
scanner : scanner user1 user2 user3 DspGroup
root@astakhov:/home/user3/docs$ grep DspGroup: /etc/group
DspGroup:x:1006:user2,user3,scanner
root@astakhov:/home/user3/docs$
```

Рисунок 13 - группа “DSP”

Для “DSP” и групп пользователей дадим группе-хозяину все права, а для остальных - отключим их. Для файлов сканера для группы-хозяина и “остальных” оставим разрешения только на чтение.

```
root@astakhov:/home/user3/docs$ ls -l /home/scanner/
итого 4
drwxrwxr--. 2 scanner DspGroup 4096 сен 19 20:03 DSP
-rw-r--r--. 1 scanner scanner    0 сен 19 20:03 scan.log
root@astakhov:/home/user3/docs$ ls -l /home/user*/docs/
/home/user1/docs/:
итого 8
drwxrwx---. 2 user1 user1 4096 сен 19 19:55 in
drwxrwx---. 2 user1 user1 4096 сен 19 19:55 out

/home/user2/docs/:
итого 8
drwxrwx---. 2 user2 user2 4096 сен 19 19:54 in
drwxrwx---. 2 user2 user2 4096 сен 19 19:54 out

/home/user3/docs/:
итого 8
drwxrwx---. 2 user3 user3 4096 сен 19 19:56 in
drwxrwx---. 2 user3 user3 4096 сен 19 19:56 out
```

Рисунок 14 - разрешения для файлов

Вывод: в ходе лабораторной работы были изучены модели управления доступом в ОС семейства Linux.