



РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 9

Управление SELinux

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

Цель работы

Получить практические навыки работы с системой мандатного контроля доступа SELinux. Освоить методы управления режимами работы, восстановления контекстов безопасности, настройки политик для пользовательских сервисов и работы с переключателями (boolean).

Первый шаг: В начале работы был выполнен вход в систему под учетной записью суперпользователя root. В корневом каталоге были созданы директории /data/main и /data/third.

```
root@localhost:/# whoami
root
root@localhost:/# mkdir -p /data/main /data/third
root@localhost:/# ls -Al /data
ls: cannot access '-': No such file or directory
ls: cannot access 'Al': No such file or directory
/data:
main  third
root@localhost:/# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Dec 16 04:54 main
drwxr-xr-x. 2 root root 6 Dec 16 04:54 third
```

Второй шаг: для созданных директорий была изменена группа-владелец с root на соответствующие группы main и third. После этого были установлены базовые права доступа, разрешающие чтение, запись и выполнение для владельца и группы, а также запрещающие доступ для остальных пользователей.

```
root@localhost:/# chgrp main /data/main
root@localhost:/# chgrp third /data/third
root@localhost:/# ls -Al data
total 0
drwxr-xr-x. 2 root main 6 Dec 16 04:54 main
drwxr-xr-x. 2 root third 6 Dec 16 04:54 third
root@localhost:/# chmod 770 /data/main
root@localhost:/# chmod 770 /data/third
```

Третий шаг: под учетной записью пользователя bob были выполнены попытки доступа к каталогам. Было подтверждено, что пользователь может

работать с каталогом своей группы и не имеет доступа к каталогу другой группы.

```
root@localhost:/# su bob
bob@localhost:/$ cd /data/main
bob@localhost:/data/main$ touch emptyfile
bob@localhost:/data/main$ ls -Al
total 0
-rw-r--r--. 1 bob users 0 Dec 16 04:57 emptyfile
bob@localhost:/data/main$ ls -a
. .. emptyfile
bob@localhost:/data/main$ cd /data/third
bash: cd: /data/third: Permission denied
```

Четвертый шаг: для организации безопасной совместной работы в каталоге /data/main были настроены специальные права доступа. Был установлен бит идентификатора группы (SetGID), обеспечивающий наследование группы каталога для новых файлов. также был установлен sticky-bit, который предотвращает удаление файлов пользователями, не являющимися владельцами этих файлов, даже если они имеют доступ к каталогу.

```
root@localhost:/data/main# chmod g+s,o+t /data/main
alice@localhost:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice3
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice4
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob1
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob2
-rw-r--r--. 1 bob users 0 Dec 16 04:57 emptyfile
```

Пятый шаг: далее были использованы списки контроля доступа (ACL) для расширения стандартных прав. Группе third были предоставлены права чтения

и выполнения в каталоге /data/main, а группе main — аналогичные права в каталоге /data/third.

```
alice@localhost:/data/main$ su
Password:
root@localhost:/data/main# setfacl -m d:g:third:rwX /data/main
root@localhost:/data/main# setfacl -m d:g:main:rwX /data/third
root@localhost:/data/main# touch /data/main/newfile2
```

Шестой шаг: с помощью команды `getfacl` была выполнена проверка корректности установленных ACL. Было подтверждено, что дополнительные разрешения применены без изменения базовых прав.

```
root@localhost:/data/main# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rw-
group::rwX                               #effective:rw-
group:third:rwX                           #effective:rw-
mask::rw-
other::---
```

Седьмой шаг: для обеспечения наследования расширенных прав доступа были настроены ACL по умолчанию. После этого новые файлы, создаваемые в каталогах, автоматически получали соответствующие права.

```

manieyvazi@localhost:~$ su
Password:
root@localhost:/home/manieyvazi# setfacl -m g:third:rx /data/main
root@localhost:/home/manieyvazi# setfacl -m g:main:rx /data/third
root@localhost:/home/manieyvazi# detfacl /data/main
bash: detfacl: command not found...
root@localhost:/home/manieyvazi# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other:---

```

Восьмой шаг: в заключение работа прав доступа была проверена под учетной записью пользователя carol. Результаты показали, что пользователи могут выполнять только разрешенные действия, что подтверждает корректность настройки прав доступа

```

alice@localhost:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice3
-rw-r--r--. 1 alice main 0 Dec 16 05:03 alice4
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob1
-rw-r--r--. 1 bob users 0 Dec 16 05:01 bob2
-rw-r--r--. 1 bob users 0 Dec 16 04:57 emptyfile

```

заключение

В ходе лабораторной работы были успешно освоены основные приёмы работы с пакетными менеджерами dnf и rpm. Приобретены навыки:

- подключения и настройки репозиториев;
- поиска, установки, обновления и удаления пакетов;
 - работы с группами пакетов;
- анализа установленных пакетов с помощью rpm;
- управления историей транзакций dnf;
- настройки конфигурационных файлов и работы через прокси.

Полученные знания являются фундаментальными для администрирования Linux-систем, основанных на RPM-пакетах, таких как RHEL, CentOS, Fedora и других.

1. Какая команда позволяет вам искать пакет rpm, содержащий файл useradd?

```
dnf provides useradd  
rpm -qf $(which useradd)
```

2. Какие команды вам нужно использовать, чтобы показать имя группы dnf, которая содержит инструменты безопасности и показывает, что находится в этой группе?

```
dnf grouplist | grep -i security  
  
dnf groupinfo "Security Tools"
```

3. Какая команда позволяет вам установить gpm, который вы загрузили из Интернета и который не находится в репозиториях?

```
dnf install /путь/к/файлу.rpm  
rpm -Uhv /путь/к/файлу.rpm
```

4. Вы хотите убедиться, что пакет gpm, который вы загрузили, не содержит никакого опасного кода сценария. Какая команда позволяет это сделать?

```
rpm -q --scripts имя_пакета.rpm
```

5. Какая команда показывает всю документацию в gpm?

```
rpm -qd имя_пакета
```

6. Какая команда показывает, какому пакету gpm принадлежит файл?

```
rpm -qf /путь/к/файлу
```