

Семинар #5: Управление доступом. Практика.

Предварительные замечания

- **Важно! Резервное клонирование ВМ.**

При выполнении данного задания придётся выполнять задания от имени суперпользователя (`root`), используя команды `su` и `sudo`. Выполняя такие команды можно случайно сломать систему. Поэтому перед выполнением данного задания на всякий случай клонируйте вашу виртуальную машину. В VirtualBox для этого нужно нажать правой кнопкой мыши на виртуальной машине и выбрать клонировать.

- **Активация root**

В только что установленной системе суперпользователь `root` может быть не активирован. Если это так и/или вы не знаете пароля от `root`, выполните:

```
$ sudo passwd root
```

Команда `sudo` сначала попросит ввести ваш пароль, а потом выполнит команду `passwd root`, которая устанавливает пароль пользователя `root`.

- **Простые пароли**

В процессе выполнения задания придётся часто переключаться между пользователями, поэтому советую в рамках этого задания устанавливать пользователям простые, запоминающиеся пароли.

- **Начинайте каждую задачу, работая под своим основным аккаунтом**

Убедитесь, что вы переключились на основную учетную запись, прежде чем приступить к новой задаче.

Задача 1. Просмотр системных файлов о пользователях и группах

- a. **Просмотр информации о пользователях**

Посмотрите файл `/etc/passwd`, содержащий информацию о пользователях:

```
$ cat /etc/passwd
```

- b. **Просмотр информации об одном пользователе**

Отфильтруйте информацию из файла `/etc/passwd` с помощью `grep` так, чтобы отобразить информацию только об одном пользователе `root`.

- c. **Просмотр информации о группах**

Посмотрите файл `/etc/group`, содержащий информацию о группах пользователей.

- d. **Просмотр информации о паролях пользователей**

Посмотрите файл `/etc/shadow`, содержащий информацию о паролях пользователей. В этом файле хранятся хэши паролей пользователей, а также сроки из действия. У обычных пользователей нет прав даже на просмотр этого файла. Поэтому его нужно просматривать от имени `root`, используя `sudo`:

```
$ sudo cat /etc/shadow
```

- e. **Просмотр информации о паролях групп**

Посмотрите файл `/etc/gshadow`, содержащий информацию о паролях групп.

- f. **Просмотр настроек команды sudo**

Посмотрите файл `/etc/sudoers`, содержащий настройки команды `sudo`.

- g. **Просмотр skeleton-директории**

Посмотрите директорию `/etc/skel`, используя `ls -la`. Эта директория содержит файлы-шаблоны, который копируются в домашний каталог нового пользователя. Посмотрите содержимое файла `.bashrc`, используя `less`. Это скрипт, который выполняется каждый раз при открытии окна терминала.

h. Просмотр UID и GID

Используйте команду `id`, чтобы просмотреть UID текущего пользователя и GID-ы всех его групп.

i. Группы пользователя

Используйте команду `groups`, чтобы просмотреть названия всех групп текущего пользователя.

Задача 2. Создание пользователей

a. Создание

Создайте нового пользователя `alice` вместе с домашней директории `/home/alice` для этого пользователя. Используйте команду:

```
$ sudo useradd alice -m
```

Посмотрите изменения, который произошли при выполнении этой команды:

- Новая запись в файле `/etc/passwd`.
- Новая запись в файле `/etc/group`. Так как при создании пользователя создаётся новая группа из одного участника с таким же названием. Поэтому при создании пользователя `alice` автоматически создастся новая группа по имени `alice`, состоящая из одного участника – `alice`.
- Новая запись в файле `/etc/shadow`. Так как у пользователя ещё не установлен пароль, то учётная запись ещё считается заблокированной. На это будет указывать восклицательный знак после имени пользователя.
- Новая папка в директории `/home` – домашняя папка пользователя `alice`.
- Содержимое папки `/home/alice` должно соответствовать скелетон-директории `/etc/skel`. Для просмотра директории `/home/alice` понадобятся права суперпользователя.
- Используйте команду `id` чтобы более удобно посмотреть UID `alice` и GID-ы её групп. Используйте команду `groups`, чтобы посмотреть все группы, в которых состоит `alice`. Она пока должна состоять в одной группе – `alice`.

b. Установка пароля

Установите пароль пользователя `alice`, используя команду:

```
$ sudo passwd alice
```

Посмотрите файл `/etc/shadow` и убедитесь, что учётная запись `alice` стала активна (должен пропасть символ `!` у пользователя `alice`).

c. Вход за нового пользователя

Переключитесь на третий виртуальный терминал (`tty3`), используя комбинацию `Ctrl-Alt-F3`. Когда потребуется вернуться обратно, нужно будет переключиться на второй виртуальный терминал – `Ctrl-Alt-F2`.

В `tty3` зайдите за нового пользователя `alice`. Сделайте следующее:

- Выполните `whoami`, чтобы убедиться, что вы зашли за `alice`.
- Выполните `pwd`, чтобы убедиться, что вы находитесь в домашней папке `alice`.
- Выполните команды `id` и `groups`, чтобы посмотреть UID пользователя и GID-ы и названия групп.
- Выполните команду `w`, чтобы посмотреть всех работающих в данный момент на машине пользователей.
- Выполните команду `echo $SHELL`, чтобы посмотреть, какая оболочка используется.
- Просмотрите файл `/etc/passwd`, используя `cat`.
- Попробуйте просмотреть файл `/etc/shadow`, используя `sudo` и `cat`. У вас не удастся этого сделать, так как `alice` не находится в группе `sudo` (или `wheel`).
- Создайте несколько файлов в домашней директории `alice`.
- Создайте файл `alice.txt` в директории `/tmp`. Это директория временных файлов в которой все пользователи могут создавать файлы. Файлы в этой директории удаляются после перезагрузки системы.
- Выйдите из оболочки, используя `exit` или `Ctrl-D`, и вернитесь на второй виртуальный терминал.

Задача 3. Модификация пользователя

a. Изменение оболочки

Измените оболочку пользователя `alice`. Если `alice` использует оболочку `/bin/sh`, то измените её на `/bin/bash`. Если же используется оболочка `/bin/bash`, то измените её наоборот на `/bin/sh`. Используйте команду `usermod`. После изменения сделайте следующее:

- Посмотрите файл `/etc/passwd` и убедитесь, что оболочка изменилась.
- Перейдите на пользователя `alice` в `tty3` и убедитесь, что используется другая оболочка. После этого вернитесь обратно на `tty2`.

b. Изменение имени пользователя

Измените имя пользователя с `alice` на `bob`, используя `usermod`.

- Посмотрите файл `/etc/passwd` и убедитесь, что имя изменилось.
- Проверьте, изменилась ли при этом основная группа пользователя (используйте `id` и `groups`).
- Проверьте, изменилась ли при этом домашняя директория пользователя.
- Зайдите в пользователь `bob` через `tty3` и убедитесь, что всё работает. Проверьте в какой директории вы оказались. Проверьте кто является владельцем файлов в этой директории. После этого вернитесь обратно на `tty2`.

c. Изменение домашней директории

Измените домашнюю директорию пользователя `bob` на `/home/bob` с переносом всех файлов из старой директории.

d. Изменение основной группы пользователя

Можно было бы переименовать группу `alice` на `bob` с помощью `groupmod`, но предположим, что мы хотим оставить группу `alice` существующей и с тем же именем.

- Создайте новую группу по имени `bobg`:

```
$ sudo groupadd bobg
```
- Проверьте, что группа создалась, просмотрев файл `/etc/group`.
- Измените основную группу пользователя `bob` на группу `bobg`.
- Проверьте, что группа `bobg` теперь является основной группой `bob`, просмотрев файлы `/etc/passwd` и `/etc/group`. Обратите внимание, что основная группа указывается именно в файле `/etc/passwd` через её `GID`. А в файле `/etc/group` не указано, что `bob` входит в группу `bobg`. Там указывается принадлежность только к дополнительным группам.
- Проверьте, что группа `bobg` теперь является основной группой `bob`, используя команды `id` и `groups`.

e. Изменение дополнительных групп пользователя

- Создайте новые группы по имени `students` и `devs`.
- Добавьте эти группы как дополнительные группы пользователя `bob`.
- Проверьте результат в файле `/etc/group`.
- Проверьте результат используя `id` и `groups`.

f. Добавление ещё одной дополнительной группы

Пользователь `bob` сейчас не может использовать `sudo`, так как не входит в группу `sudo` (или `wheel`, в зависимости от того, какая группа используется на вашей системе) и не указан в файле `/etc/sudoers`.

- Добавьте пользователя `bob` в ещё одну дополнительную группу `sudo` (или `wheel`).
- Используйте команду `groups`, чтобы проверить, что `bob` входит во все группы:

```
$ groups
bobg students devs sudo
```

Переключитесь на пользователя `bob` и попробуйте посмотреть файл `/etc/shadow`, используя `sudo`.

g. Изменение UID

Проверьте владельца файла `/tmp/alice.txt`. Измените `uid` пользователя `bob`. Проверьте, изменился ли владелец у файла `/tmp/alice.txt`. После изменения `UID` нужно будет изменить `UID` владельца у всех файлов в системе у которых владельцем был `bob`. Используйте команду `find` с опцией `-exec`.

Задача 4. Удаление и создание

a. Удаление группы

Удалите группу `alice` из прошлой задачи используя `groupdel`.

b. Удаление пользователя

Удалите пользователя `bob` из прошлой задачи используя `userdel`.

```
$ sudo userdel -r bob
```

Тут используем опцию `-r`, чтобы удалить не только пользователя, но и домашнюю директорию и некоторые другие файлы пользователя `bob`.

- Проверьте, удалась ли домашняя директория `/home/bob` в этом случае.
- Проверьте, удалась ли группа `bobg`. Это была основная группа пользователя `bob`, при этом больше никто в эту группу не входил. Если она не удалась, удалите её.
- Проверьте, удалились ли группа `students` и `devs`. Это были дополнительные группы пользователя `bob`, при этом больше никто в эти группы не входил. Их пока не удаляйте.

c. Создание пользователя с опциями

Создайте пользователя `alice` и сразу же при создании нужно сделать следующее:

- Задать путь до домашней папки как `/home/alices_place`.
- Создать домашнюю папку `/home/alices_place`.
- Задать оболочку пользователя `/bin/bash`.
- Записать пользователя `alice` в дополнительные группы `students` и `devs`.
- Задать UID пользователя значением `1234`.

Всё это нужно сделать одной командой. После создания пользователя, просмотрите файл `/etc/passwd` и убедитесь, что все поля были заданы корректно. Убедитесь, что папка `/home/alices_place` была создана. Также убедитесь, что автоматически была создана новая группа `alice`.

d. Ещё одно удаление пользователя

Удалите пользователя `alice`, используя команду `sudo userdel -r alice`.

- Проверьте, удалась ли группа `alice`. Это была основная группа пользователя `alice`, при этом больше никто в эту группу не входил. Если она не удалась, удалите её.
- Проверьте, удалились ли группа `students` и `devs`. Это были дополнительные группы пользователя `bob`, при этом больше никто в эти группы не входил. Если она не удалилась, удалите их.

Задача 5. Блокировка

- Создайте нового пользователя `alice` и установите пароль:

```
$ sudo useradd -s /bin/bash -m alice
$ sudo passwd alice
```

- Проверьте, что учётная запись `alice` активна, зайдя под пользователем `alice` на `tty3`. Вернитесь обратно.
- Заблокируйте пользователя `alice`, используя `usermod`.
- Посмотрите файл `/etc/shadow`. В записи `alice` должен появиться восклицательный знак. При этом хэш пароля должен всё ещё храниться в файле.
- Попробуйте вновь зайти под пользователем `alice`.
- Разблокируйте пользователя `alice`.
- Снова проверьте файл `/etc/shadow`. Восклицательный знак в записи `alice` должен появиться исчезнуть.
- Попробуйте вновь зайти под пользователем `alice`.

Задача 6. su и sudo

a. Просмотр переменных среды

- Просмотрите все переменные среды, используя команду `env`.
- Просмотрите переменную среды `USER`:

```
$ echo $USER
```
- Просмотрите также переменные среды `LOGNAME`, `HOME` и `PATH`.

b. Неполное переключение

- Переключитесь на пользователя `root`, используя команду `su`. Введите пароль пользователя `root`.
- Выполните команду `whoami`, чтобы напечатать имя текущего пользователя.
- Просмотрите переменные среды `LOGNAME` и `PATH`.
- Выйдите из под `root` выполнив `exit` или нажав `Ctrl-D`.

c. Полное переключение

- Переключитесь на пользователя `root`, используя команду `su -`. Введите пароль пользователя `root`.
- Выполните команду `whoami`, и просмотрите переменную среды `LOGNAME`.
- Выйдите из под `root`.

d. Полное переключение через sudo

- Переключитесь на пользователя `root`, используя команду `sudo -i`. Введите пароль вашего текущего пользователя.
- Выполните команду `whoami`, и просмотрите переменную среды `LOGNAME`.
- Выйдите из под `root`.

e. Полное переключение на пользователя alice

- Сделайте полное переключение на пользователя `alice`
- Выполните команду `whoami`, и просмотрите переменную среды `LOGNAME`.
- Выйдите из под `alice`.

f. Выполнение одной команды от имени другого пользователя

В этой подзадаче нужно не переключаться на других пользователей, а использовать `sudo` для выполнения команд от имени другого пользователя.

- Выполните команду `cat /etc/shadow` от имени пользователя `root`:

```
$ sudo cat /etc/shadow
```
- Перейдите в папку `/tmp` и создайте там файл `a.txt`. Используйте `ls -l`, чтобы посмотреть владельца этого файла и группу-владельца этого файла.
- Создайте файл `b.txt` от имени `root`. Посмотрите владельца этого файла и группу-владельца.
- Создайте файл `c.txt` от имени `alice`. Посмотрите владельца этого файла и группу-владельца.
- Измените владельца файла `a.txt` на `alice`.
- Измените группу владельца файла `a.txt` на `root`.

g. Запрещённая команда

Вы пытаетесь создать новый файл в системной директории `/etc`:

```
$ touch /etc/myfile
```

но у вас ничего не выходит, так как у вас нет прав на это. Выполните эту команду, используя `sudo`.

h. Запрещённая команда 2

Вы пытаетесь записать в новый файл в системной директории `/etc`:

```
$ echo "Hello" > /etc/myfile
```

но у вас ничего не выходит, так как у вас нет прав на это. Выполните эту команду, используя `sudo`.

Задача 7. Права доступа

a. Конвертация из символьного представления в числовое

Конвертируйте запись следующих прав доступа из символьного представления в числовое:

```
-----  
rwx-----  
r--r--r--  
r---w---x  
rw-r--r--  
rwxr-xr-x  
rwxrwxrwx
```

Для решение этой подзадачи нужно создать файл `07a.txt` и записать туда все ответы в виде:

```
000  
700  
...
```

b. Просмотр прав файла

В своей домашней директории создайте два файла `a.txt` и `b.txt`:

```
touch a.txt b.txt
```

Используйте команду `ls`, чтобы просмотреть права файла (и другую информацию) только файла `a.txt`.

c. Просмотр прав директории

Создайте директорию `test`:

```
mkdir test
```

Используйте команду `ls`, чтобы просмотреть права только директории `test`. Другие файлы при этом отображаться не должны.

d. Изменение прав доступа

Измените права доступа файлов `a.txt` и `b.txt` на нулевые:

```
chmod 000 a.txt b.txt
```

После этого дайте файлу `a.txt` права доступа: `rwxr-xr--`, используя синтаксис символьного представления прав доступа. Задачу нужно решить в одну строку.

Файлу `b.txt` также дайте права доступа: `rwxr-xr--`, но используя числовое представление прав доступа.

e. Изменение прав доступа директории

Измените права директории `test` на `-wx-wx-wx`. После этого ответьте на вопросы:

- Можете ли вы просматривать директорию, используя `ls test`?
- Можете ли вы создавать файлы в директории, используя `echo hello > test/h.txt`?
- Можете ли вы заходить в директорию, используя `cd test`?
- Можете ли вы зайти в директорию и просмотреть там файлы, используя `ls`?

Просмотрите содержимое директории `test`, используя `sudo`.

f. Права вложенных директорий

Создайте директорию `one/` и вложенную в неё директорию `one/two/`. Дайте директории `two` права `rwxrwxrwx` (полные права), а директории `one` права `-----` (нулевые права). После этого ответьте на вопросы:

- Можете ли вы просматривать директорию `two`?
- Можете ли вы создавать файлы в директории `two`?
- Можете ли вы заходить в директорию `two`?

g. Права вложенных директорий 2

Измените права директории `one` на `--x--x--x` и заново ответьте на те же вопросы.