

Вебинар №6. Управление учётными записями, домены и мандатное управление доступом

Что будет сегодня



Узнаете об управлении
учётными записями
пользователей и групп



Научитесь настраивать
домен ALD и DNS-сервер,
включая NTP-сервер



Познакомитесь с мандатным
управлением доступом
и узнаете как с ним работать



Научитесь создавать
пользователей с мандатным
уровнем и переопределять
их метки безопасности,
включая разбор скриптов

Управление учётными записями пользователей и групп

Создание, изменение и удаление учётных записей

Создание нового пользователя:

```
sudo useradd -m -s /bin/bash jane
```

Добавление пользователя в группу sudo:

```
sudo usermod -a -G sudo user_name
```

(где user_name — имя пользователя)

Описание параметров:

- -m — создание домашней директории пользователя.
- -s — выбор оболочки по умолчанию.
- -a — добавить пользователя в дополнительную группу(ы). Этот параметр следует использовать только вместе с параметром -G.
- -G — добавления пользователя в дополнительные группы.

Изучение локальных баз учётных записей

Файл `/etc/passwd` содержит информацию о пользователях, включая их имена, идентификаторы (UID), номера групп, комментарии, домашние директории и оболочки по умолчанию. Каждый пользователь имеет свою строку в файле.

Например:

```
vladimir:x:1000:1000:vladimir_D:/home/vladimir:/bin/bash
```

- `vladimir` — имя пользователя.
- `x` — указатель на зашифрованный пароль (хеш).
- `1000` — UID пользователя.
- `1000` — GID пользователя.
- `vladimir_D` — комментарий
- `/home/vladimir` — домашняя директория пользователя.
- `/bin/bash` — оболочка по умолчанию.

Изучение локальных баз учётных записей

Файл `/etc/shadow` хранит заблокированные и зашифрованные пароли пользователей. Только пользователь `root` имеет доступ к его содержимому. Каждый пользователь имеет свою строку в файле `/etc/shadow`, которая выглядит примерно так:

```
vladimir:$6$rgZkNTnK$T2lLkBzcZHrVmsoqj2DiDgzcJDJfF5a8zMFOf.NGLBZ0j.fgQmpeZGu  
d0Uj.wRz/l/9RMw/XJhRQ5x5Z/jcmL1:18763:0:99999:7:::
```

Изучение локальных баз учётных записей

vladimir:\$6\$rgZkNTnK\$T2lKbZcZHrVmsoqj2DiDgzcJDJfF5a8zMFOf.NGLBZ0j.fgQmpeZG
ud0Uj.wRz/I/9RMw/XJhRQ5x5Z/jcmL1:18763:0:99999:7:::

Каждая строка файла /etc/shadow состоит из нескольких полей, разделённых двоеточием. Рассмотрим каждое из них:

- vladimir - имя пользователя.
- \$6\$rgZkNTnK\$T2lKbZcZHrVmsoqj2DiDgzcJDJfF5a8zMFOf.NGLBZ0j.fgQmpeZGud0Uj.wRz/I/9RMw/XJhRQ5x5Z/jcmL1 - зашифрованный пароль пользователя.
- 18763 - количество дней с 1 января 1970 года до последней смены пароля.
- 0 - минимальное количество дней до возможности следующей смены пароля. 0 означает, что пароль не будет истекать.
- 99999 - максимальное количество дней до следующей смены пароля и 99999 означает, что пароль не будет истекать.
- 7 - предупреждение о смене пароля в днях до истечения пароля, после чего пользователь получит предупреждение о необходимости смены пароля.
- :: (пустое поле) - дата истечения учётной записи. Пустое поле означает, что учётная запись будет действительной на неопределённое время.

Управление паролями

1. Установка пароля для новой учётной записи:

sudo passwd username

2. Изменение существующего пароля учётной записи:

sudo passwd username

3. Удаление пароля учётной записи:

sudo passwd -d username

4. Ограничение срока действия пароля (в днях):

sudo chage -M 30 username

5. Запрет на использование старых паролей (в днях):

sudo chage -i 5 username

6. Блокировка учётной записи:

sudo passwd -l username

7. Разблокировка учётной записи:

sudo passwd -u username

Настройка окружения пользователя

При входе любого пользователя в систему для него запускается особый экземпляр оболочки — login shell. В процессе запуска в качестве login shell, bash ищет следующие файлы в указанном порядке и выполняет содержащиеся в них команды:

- /etc/profile
- ~/.bash_profile
- ~/.bash_login
- ~/.profile.

Настройка окружения пользователя

Если `bash` запускается повторно из командной строки в интерактивном режиме (т. е. не для выполнения какой-то одиночной команды), он находит файл `~/.bashrc` и выполняет содержащиеся в нём команды.

```
PS1='\[\e[42m\]\u@\h \w \$ \[\e[0m\]
```

Эта строка задаёт значение переменной `PS1` в следующем формате:

- `\[\e[42m\]` — зелёный цвет фона;
- `\u@\h` — имя пользователя и имя хоста;
- `\w` — текущая рабочая директория;
- `\$` — знак доллара для обозначения командной строки;
- `\[\e[0m\]` — возврат к обычному цвету текста.

Чтобы обновить текущую среду после редактирования `.bashrc`, используйте:

```
source ~/.bashrc.
```

Настройка ssh

Для настройки и изменения конфигурации SSH-сервера используется файл `/etc/ssh/sshd_config`. После редактирования `/etc/ssh/sshd_config` не забудьте рестартовать службу:

```
sudo systemctl restart sshd
```

```
ssh-keygen -t rsa -b 4096
```

После выполнения команды получим публичный (открытый) и приватный (закрытый) ключи.

По умолчанию они находятся в домашнем каталоге в скрытой папке `.ssh` файлы `id_rsa` и `id_rsa.pub`.

Для доступа к удалённой машине необходимо разместить публичный ключ в следующей строке файла `.ssh/authorized_keys`.

Наиболее часто используемые атрибуты при генерации:

- `-t` — тип ключа;
- `-b` — длина ключа в битах (по умолчанию 3072 для RSA);
- `-f` — путь к файлу ключа (по умолчанию `~/.ssh/id_rsa`);
- `-C` — комментарий к ключу (по умолчанию `username@hostname`);
- `-P` — пароль для доступа к ключу.

После того как ключ будет сгенерирован, его можно отправить на нужную машину. Это удобнее всего сделать через `ssh-copy-id` так:

```
ssh-copy-id -i $HOME/.ssh/id_rsa.pub <имя пользователя>@<ip-адрес сервера куда хотим получить доступ>.
```

Настройка домена ALD и DNS-сервера

DNS

```
sudo apt-get install bind9 bind9utils bind9-doc
```

1. Отредактировать конфигурационный файл /etc/bind/db.test.
2. Отредактировать конфигурационный файл /etc/bind/db.192.168.1.
3. Отредактировать конфигурационный файл /etc/bind/named.conf.local.
4. Отредактировать конфигурационный файл /etc/bind/db.root.
5. Отредактировать конфигурационный файл /etc/bind/named.conf.options.
6. Отредактировать конфигурационный файл /etc/resolv.conf.
7. Отредактировать конфигурационный файл /etc/hosts.
8. Перезапустить службу Bind.
9. nslookup srv1.

ALD

Для корректной работы ALD-сервера необходим сервер точного времени (NTP).

Команда

```
sudo apt install fly-admin-ald-server ald-server-common smolensk-security-ald ald-client-common fly-admin-ald-client
```

1. Отредактировать файл конфигурации `/etc/ald/ald.conf`.
2. Инициализировать домен `fly-admin-ald-server`.
3. Смена максимального времени жизни билета Kerberos:
`for i in `kadmin -p admin/admin -w пароль_домена -q "listprincs"`; do kadmin -p admin/admin -w пароль_домена -q "modprinc -maxlife 5days $i";done.`
4. Увеличить ограничение по количеству открытых файлов в файле `/etc/security/limits.conf`
`soft nofile 2048 hard nofile 4096.`

Для смены пароля ALD администратора `admin/admin` выполнить следующие команды:

```
sudo kadmin.local
```

```
listprincs
```

```
change_password admin/admin@домен.ru.
```

Мандатное управление доступом

Мандатный контроль целостности



Уровни и категории конфиденциальности, мандатная целостность

Пример метки безопасности: 3:63:0xffffffffffffff

Первый и третий атрибуты (уровень конфиденциальности и категория конфиденциальности) отвечают за то, чтобы информация не попадала к тому, кто не уполномочен её получать.

Классический пример уровней конфиденциальности — это степени повышающейся секретности документов (сущностей):

- «Не секретно».
- «ДСП».
- «Секретно».
- «Совершенно секретно».

Второй атрибут — уровень целостности — в первую очередь отвечает за безопасность самой информационной системы; во вторую — за то, чтобы информацию не могли изменять те, кому не положено её изменять.

Мандатный атрибут **ccnr**

- Определяет, что каталог может содержать файлы с различными классификационными метками, но не большими, чем его собственная метка.
- Чтение содержимого такого каталога разрешается пользователю вне зависимости от значения классификационной метки этого пользователя.
- Пользователю доступна информация:
 - про находящиеся в этом каталоге файлы с классификационной меткой не большей, чем собственная классификационная метка пользователя;
 - про каталоги, также имеющие мандатный атрибут управления доступом **ccnr**.

Мандатный атрибут **ccnri**

- Определяет, что каталог может содержать файлы с различными уровнями целостности, но не большими, чем его собственный уровень целостности;
- Применяется только к каталогам.

Мандатный атрибут **ehole**

- Может присваиваться файлам, имеющим минимальную метку безопасности. Его наличие приводит к игнорированию мандатных правил управления доступом к файлам;
- Атрибут предназначен для файлов, из которых пользователи не могут прочитать данные, записанные в них пользователями с более высокой классификационной меткой, чем его собственная (например, /dev/null).

Установка меток и дополнительных атрибутов безопасности на файлы и каталоги

```
pdpl-file [ОПЦИИ]... [УРОВЕНЬ][:УРОВЕНЬ_ЦЕЛОСТНОСТИ[:КАТЕГОРИЯ[:ФЛАГИ]]] ФАЙЛ...  
pdpl-file -R 3:0:0xffffffffffff:CCNRI /data/samba/sov.sekret/
```

Изменяет мандатные свойства файла на УРОВЕНЬ, УРОВЕНЬ_ЦЕЛОСТНОСТИ, КАТЕГОРИЮ и ФЛАГИ.

-f, --silent, --quiet	не выводить сообщения об ошибках;
-v, --verbose	выводить диагностические сообщения для каждого файла;
-c, --changes	то же, что и --verbose, но сообщает только об изменениях;
-u, --unite	объединить текущую метку файла с заданной в качестве аргумента;
-s, --subtract	вычесть из текущей метки файла заданную в качестве аргумента;
-R, --recursive	применить рекурсивно;
-r, --reverse	сначала файлы в директории, потом — директорию;
-h, --help	вывести эту справку и выйти;
--version	вывести информацию о версии и выйти.

Установка меток и дополнительных атрибутов безопасности на файлы и каталоги

```
pdpl-file [ОПЦИИ]... [УРОВЕНЬ][:УРОВЕНЬ_ЦЕЛОСТНОСТИ[:КАТЕГОРИЯ[:ФЛАГИ]]] ФАЙЛ...  
pdpl-file -R 3:0:0xffffffffffff:CCNRA /data/samba/sov.sekret/
```

УРОВЕНЬ и УРОВЕНЬ_ЦЕЛОСТНОСТИ могут быть заданы именем или десятичным значением.

КАТЕГОРИЯ может быть задана именем или шестнадцатеричным значением.

ФЛАГИ могут быть заданы значением или именами через запятую:

- Для директорий: csnr, csnri; можно использовать алиас CCNRA (csnr,csnri).
- Для файлов: ehole (с мин. меткой) ИЛИ whole (с макс. меткой).

Для просмотра установленных меток и дополнительных атрибутов безопасности используется команда:

```
pdp-ls [КЛЮЧ]... [ФАЙЛ]...
```

Для получения справки о применении и ключах команды pdp-ls введите команду:

```
pdp-ls --help.
```

Работа с мандатным уровнем доступа

rsync при работе с файлами с мандатным уровнем доступа

Простейший пример для удалённого копирования с помощью инструмента rsync:

```
sudo rsync -a --X --A --exclude=/proc --exclude=/lost+found --exclude=/mnt --  
exclude=/sys --exclude=/parsecfs --rsync-path="sudo /rsync --fake-super" /  
admin@host.astradomain.ru:backup
```

В примере применены ранее описанные атрибуты --xattrs и --acls (в краткой форме -X и -A) и добавлен новый атрибут --rsync-path, который переопределяет вызов удалённого экземпляра rsync как:

- вызов rsync от имени и с правами суперпользователя (sudo), что позволяет выставлять на удалённом компьютере любые атрибуты создаваемым файлам-копиям;
- вызов rsync с параметром --fake-super, разрешающим выставлять создаваемым файлам-копиям атрибуты исходных файлов независимо от валидности этих атрибутов в целевой ОС.

Запуск служб на мандатном уровне доступа

Для запуска служб с определённой ненулевой меткой безопасности следует назначить службе эту метку. Для этого:

1. Выполнить команду:

```
sudo systemctl edit <имя_службы>.service
```

2. В открывшемся текстовом редакторе в секции [Service] указать нужную метку (например, для задания уровня безопасности равным 1 и с высшим уровнем конфиденциальности):

[Service]

PDPLabel=1:63:0

Формат метки: PDPLabel=<Уровень>:<Уровень целостности>:<Категории>

Формат метки PDPLabel аналогичен принятому в системе PARSEC (рассматривали в 21-м модуле) за исключением поля типа «метки».

3. Сохранить изменения и перезапустить службу:

```
sudo systemctl restart <имя_службы>.service.
```

Переопределение метки безопасности пользователей (скрипты)

Спасибо за внимание!

