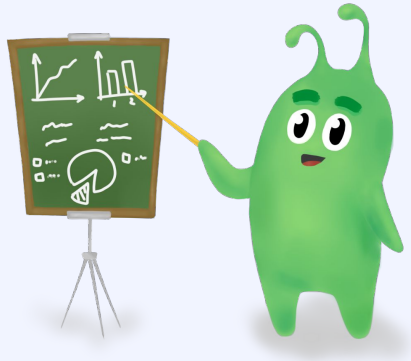
Безопасность в Linux

План занятия

- PAM
- sudoers
- SSH
- SELinux



PAM

Pluggable Authentication Modules

Набор модулей для аутентификации пользователей

Модули — /usr/lib/x86_64-linux-gnu/security

Конфиги PAM – /etc/pam.d

Конфиги модулей PAM – /etc/security

Конфиг PAM (CentOS 7)

[root@localhost ~]# cat /etc/pam.d/sudo

```
auth        include      system-auth
account     include      system-auth
password    include      system-auth
session     optional     pam_keyinit.so     revoke
session     include      system-auth
```

Тип модуля	Флаг контроля	Модуль	Параметры

Типы модулей

auth – аутентификация пользователя

account – проверка возможности доступа к сервису

password – обновление механизма аутентификации

session – действия при входе пользователя в систему

Флаги контроля

required – указанный модуль должен успешно отработать
остальные модули **будут** запущены при неудаче

requisite – указанный модуль должен успешно отработать
остальные модули **не будут** запущены при неудаче

sufficient – если указанный модуль отработает успешно
весь сервис будет считаться доступным

optional – результат модуля не имеет значения
если он не единственный

include – подключить содержимое другого конфига PAM

sudoers

Основной файл — /etc/sudoers

Дополнительная конфигурация — /etc/sudoers.d/

```
%wheel    ALL=(ALL)    ALL

user      ALL=         NOPASSWD: /usr/bin/less
user      ALL=         NOEXEC: NOPASSWD: /usr/bin/less
```

Меры защиты SSH-сервера

Нестандартный порт

PermitRootLogin no

PasswordAuthentication no

Двухфакторная аутентификация

iptables

iptables

Ограничивает доступ на уровне сети

Конфигурация состоит из цепочек правил

Управляется командой iptables

SELinux

В следующей серии

namespaces и cgroups