Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Операционные системы»

Лабораторная работа №7  
«Сервис динамической аутентификации PAM»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Коротяев А.Н.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. **Просмотр политик PAM** 3](#_Toc136673605)

[2. **Динамическое конфигурирование аутентификации (разрешение доступа к root без пароля)** 4](#_Toc136673606)

[3. **Динамическое конфигурирование аутентификации (запрет на доступ к root через su -)** 6](#_Toc136673607)

[4. **Парольная политика** 7](#_Toc136673608)

[5. **Соответствие списку pam\_cracklib** 10](#_Toc136673609)

[**Вывод:** 11](#_Toc136673610)

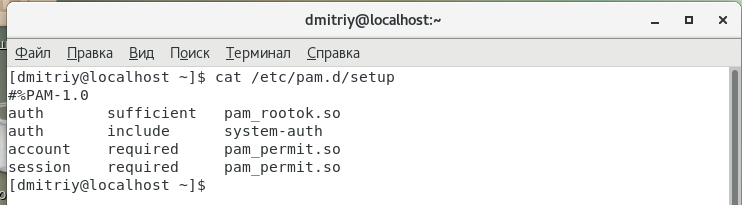
**Цель работы:** знакомство с сервисом PAM (Pluggable Authentification Modules) – системой динамической аутентификации пользователя в приложениях (службах), изучение основных команд и файлов по работе с ним, получение практических навыков решения задач (к примеру, работа с политиками паролей и динамическое конфигурирование аутентификации).

**Ход работы:**

Комментарий: Лабораторная работа выполнена в CentOS 7, установленной на виртуальной машине VMWare Workstation.

# **Просмотр политик PAM**

Для просмотра политики аутентификации необходимо просмотреть файл */etc/pam.d/setup* (рисунок 1).



**Рисунок 1**. Политики аутентификации

В данном случае указывается на то, что, например, служба account (Управление учетными записями) требует успешного завершения (флаг *required*) работы модуля *pam\_permit.so*. При этом модуль *pam\_permit.so* включает набор библиотек, находящихся по стандартным путям, указанным в *libpam*.

Вызов каждого модуля заканчивается результатом *success* или *failure*. Контрольные флаги определяют, что нужно делать в этих случаях. Это, например, важно если модули последовательно связаны между собой.

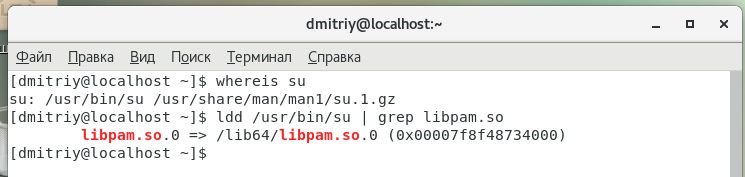
Файл setup подразумевает следующую логику аутентификации соответствующей утилиты (setup). Если аутентификация pam\_rootok.so закончилась успешно, команда выполняется, если нет, то проверка продолжается. При этом подключается библиотека */etc/pam.d/system-auth*; для учетных записей выполняется pam\_permit.so (разрешение на перезагрузку), затем производится попытка журналирования данного действия.

# **Динамическое конфигурирование аутентификации (разрешение доступа к root без пароля)**

Для того, чтобы убедиться в поддержке командой *su* динамической аутентификации, необходимо:

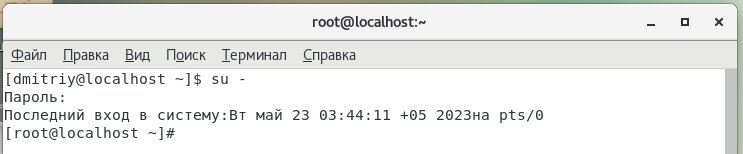
* узнать абсолютный путь до исполняемого файла командой *whereis su*;
* проверить на совместимость с PAM с помощью команды *ldd /usr/bin/su | grep libpam.so*.

Если данная библиотека имеется в выводе команды, то исполняемый файл имеет поддержку динамической аутентификации (рисунок 2).



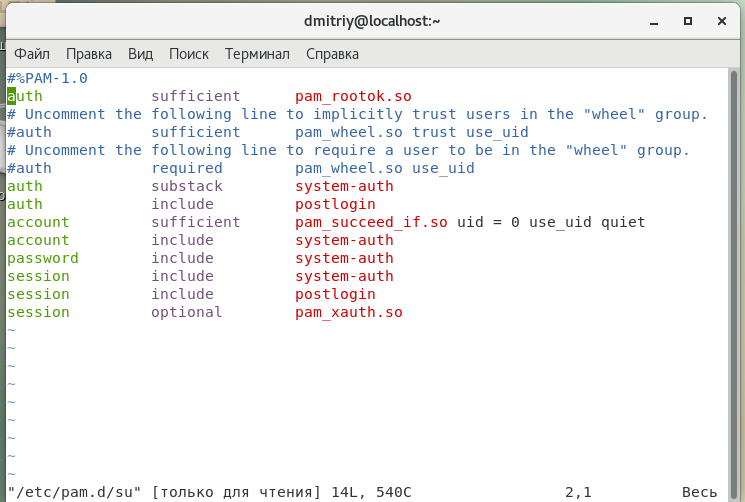
**Рисунок 2**. Проверка *su* на поддержку динамической аутентификации

При выполнении команды *su –* был запрошен пароль суперпользователя, после ввода которого был выполнен вход под суперпользователем (root) (рисунок 3).



**Рисунок 3**. Выполнение команды su -

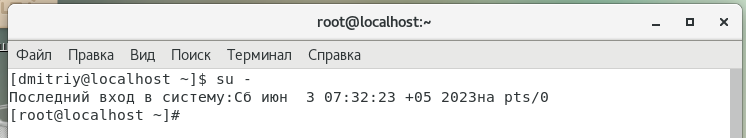
Для конфигурирования параметров аутентификации для утилиты su необходимо редактировать конфигурационный файл */etc/pam.d/su* (рисунок 4).



**Рисунок 4**. Исходные данные */etc/pam.d/su*

Для отключения запроса пароля необходимо изменить модуль *pam\_rootok.so* на *pam\_permit.so* (вторая строка рисунка 4).

После внесения изменений повторяю процедуру входа в суперпользователя, на этот раз пароль не запрашивался (рисунок 5).

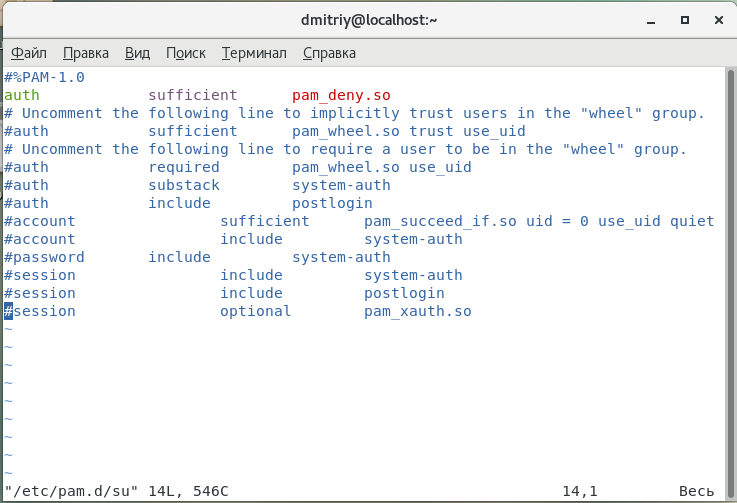


**Рисунок 5**. Отсутствие запроса пароля после внесения изменений в */etc/pam.d/su*

Для возврата системы в изначальное состояние необходимо возвратить вместо *pam\_permit.so* *pam\_rootok.so*.

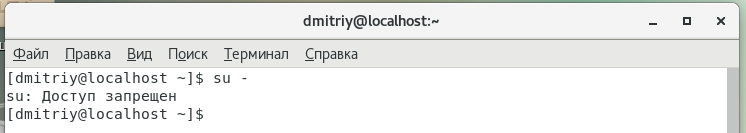
# **Динамическое конфигурирование аутентификации (запрет на доступ к root через su -)**

Для запрета всем пользователям входа через суперпользователя необходимо в том же конфигурационном файле */etc/pam.d/su* заменить *pam\_rootok.so* на *pam\_deny.so* и закомментировать остальные строки (рисунок 6).



**Рисунок 6**. Конфигурация для запрета входа в суперпользователя через команду *su -*

После внесения изменений необходимо произвести попытку входа в суперпользователя командой *su -*, действительно, команда не выполняется (рисунок 7).



**Рисунок 7**. Запрет доступа к суперпользователю командой *su -*

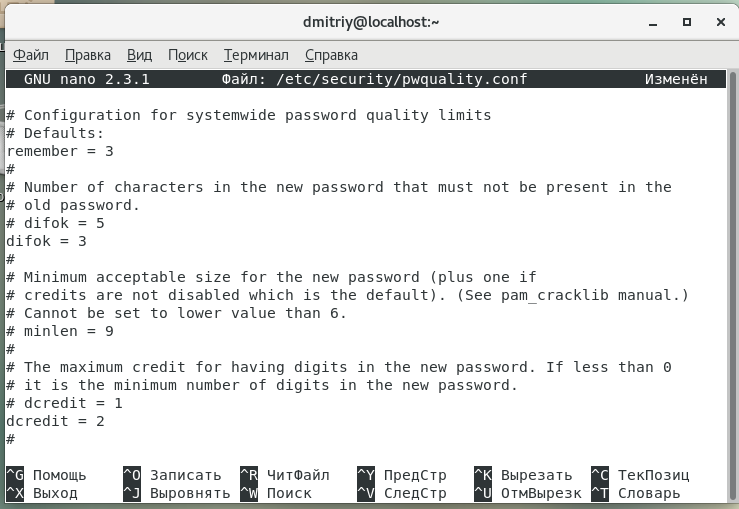
Для возврата системы в исходное состояние необходимо обратить изменения в файле */etc/pam.d/su*, с использованием приставки *sudo* (так как для внесения изменений в конфигурационный файл необходимы права суперпользователя).

# **Парольная политика**

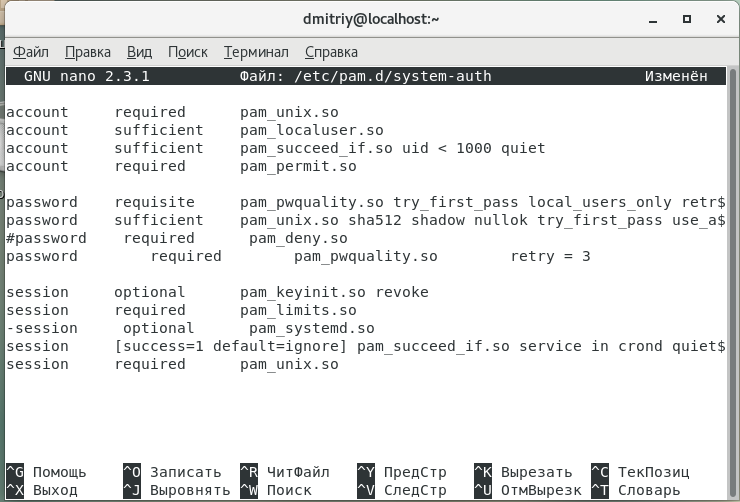
За парольную политику системы отвечает файл */etc/security/pwquality.conf*. Для того, чтобы реализовать проверку пароля на наличие не менее 2 цифр, запоминания 3 предыдущих паролей и различие как минимум 3 символов в новом пароле по сравнению с предыдущими необходимо внести следующие изменения:

* dcredit = 2 – минимум 2 цифры в пароле;
* remember = 3 – запоминание 3 предыдущих паролей в файле */etc/security/opasswd*;
* difok = 3 – проверка на различие как минимум 3 символов по сравнению с предыдущими паролями.

Строка в файле */etc/pam.d/system-auth* ***password required pam\_pwquality.so retry=3*** позволяет указать количество попыток ввода пароля перед возвращением ошибки (при вводе неправильного пароля). Для последующего возврата к исходному состоянию параметры по умолчанию будут закомментированы, а новые значения внесены в файл рядом с изначальными значениями (рисунок 8, 9).

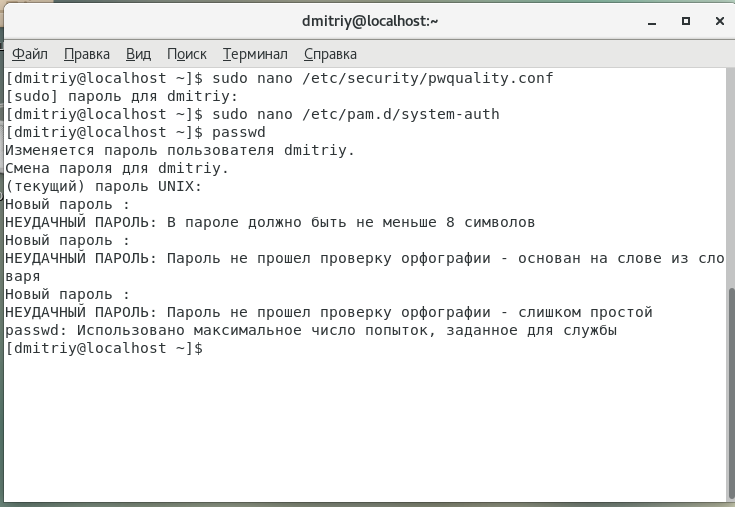


**Рисунок 8**. Внесение изменений в файл */etc/security/pwquality.conf*



**Рисунок 9**. Внесение изменений в файл */etc/pam.d/system-auth*

После записи изменений необходимо произвести попытку изменения пароля – команда *passwd* (рисунок 10).



**Рисунок 10**. Попытка изменения пароля

Итого:

* минимальная требуемая длина пароля составляет 8 символов;
* дается 3 попытки на ввод нового пароля;
* недопустимы пароли, содержащие последовательность “qwerty”;
* при вводе пароля без цифр выдается сообщение о слишком простом пароле.

Для реализации парольной политики, проверяющей пароль на наличие как минимум 2 цифр, 2 заглавных букв, 2 специальных символов и общей длиной не менее 8 символов необходимо в файле */etc/security/pwquality.conf* внести следующие изменения:

* требование о наличии как минимум 2 цифр было реализовано шагом ранее;
* о запоминании предыдущих паролей ничего не сказано, поэтому необходимо вернуть значения по умолчанию для полей *remember* и *difok*;
* проверка на как минимум 2 заглавные буквы – *ucredit = 2*;
* проверка на как минимум 2 специальных символа – *ocredit = 2*;
* проверка на общую длину – параметр *minlen = 11* (в документации написано, что каждый требуемый тип символа должен увеличивать значение minlen на 1, в данном случае требуются цифры, заглавные буквы и специальные символы: 8 + 3 = 11).

Для возврата в исходное состояние необходимо раскомментировать закомментированные ранее строки.

# **Соответствие списку pam\_cracklib**

Библиотека *pam\_cracklib.so* принимает параметры, указанные в пункте 4 данной лабораторной работы (такие, как *ucredit*, *difok* и др.). Также имеется функциональность сравнения паролей со словарями паролей (к примеру, самые популярные последовательности, такие, как qwerty, password и др.) Для реализации такой проверки необходимо указать параметр *dictpath = <путь\_к\_словарю>*. При указании данного параметра, если введенный пользователем пароль совпадет с любой строкой из словаря, то пароль будет считаться как ненадежный и не будет принят.

# **Вывод:**

В ходе выполнения лабораторной работы поставленные цели были успешно выполнены. Были освоены методы работы с сервисом PAM в ОС Linux. Изучены команды, конфигурационные файлы данного сервиса. Произведена работа по редактированию политики паролей. Было выполнено динамическое конфигурирование аутентификации. Закреплены навыки работы с ОС Linux, с оболочкой ее командной строки.