## Front matter

title: "Лабораторная работа №6" subtitle: "Лабораторная работа № 6. Мандатное разграничение прав в Linux" author: "Болотина Александра Сергеевна"

## Generic otions

lang: ru-RU toc-title: "Содержание"

## Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

## Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: false # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt

## I18n polyglossia

polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs: name: english

## I18n babel

babel-lang: russian babel-otherlangs: english

## Fonts

mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9

## Biblatex

biblatex: true biblio-style: "gost-numeric" biblatexoptions:

parentracker=true backend=biber hyperref=auto language=auto autolang=other\* citestyle=gost-numeric

## Pandoc-crossref LaTeX customization

figureTitle: "Рис." tableTitle: "Таблица" listingTitle: "Листинг" lofTitle: "Список иллюстраций" lotTitle: "Список таблиц" lolTitle: "Листинги"

## Misc options

indent: true header-includes:

\usepackage{indentfirst}

\usepackage{float} # keep figures where there are in the text

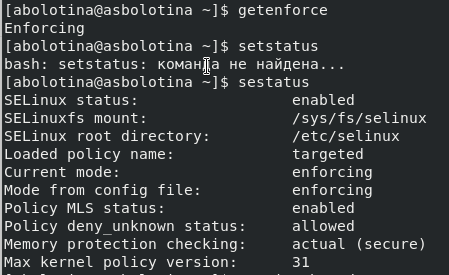
\floatplacement{figure}{H} # keep figures where there are in the text

# Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами.

Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Выполнение лабораторной работы

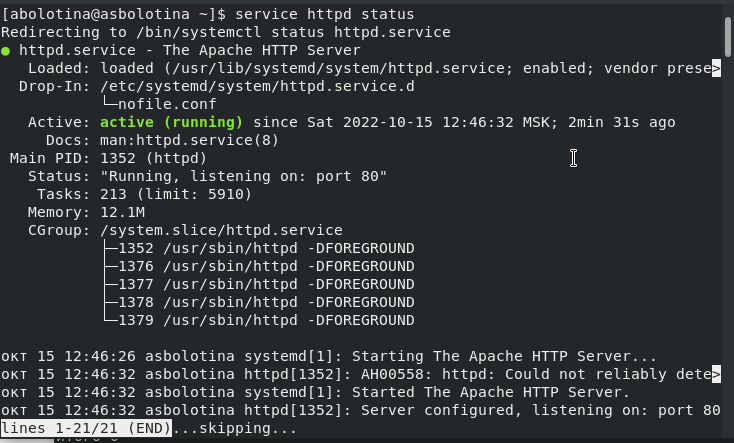
1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и

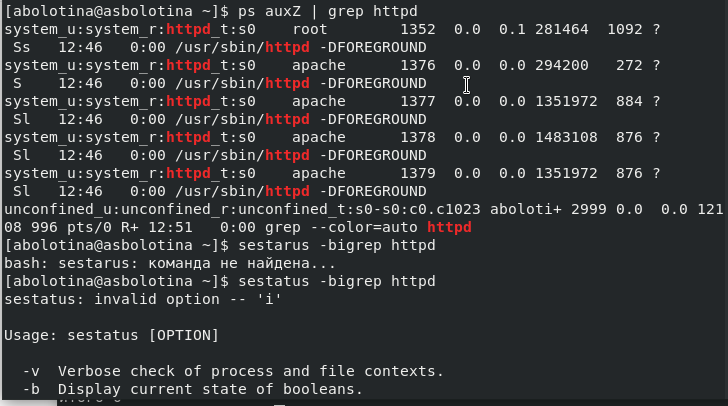
sestatus.

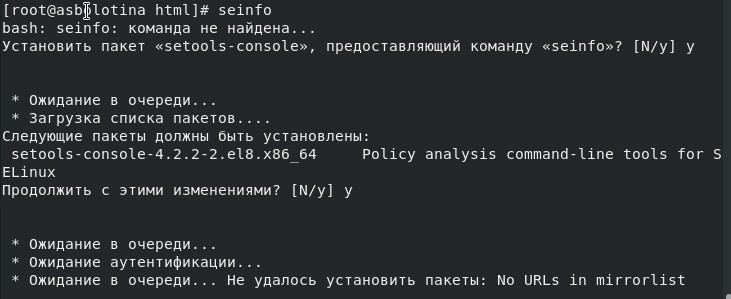
1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status или

/etc/rc.d/init.d/httpd status Если не работает, запустите его так же, но с

параметром start.

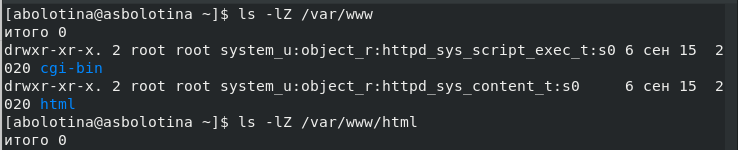


1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd
2. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd Обратите внимание, что многие из них находятся в положении «off».
3. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.



1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
2. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ

/var/www/html



1. Определите круг пользователей, которым разрешено создание файлов в директории

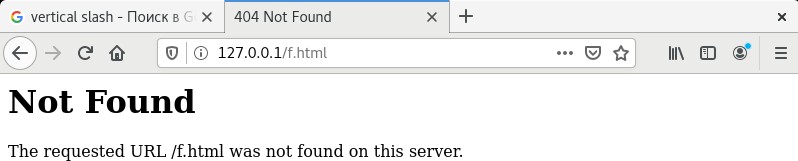
/var/www/html.

1. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

test ![изображение](https://user- images.githubusercontent.com/113191444/196002387-a76752e2-bde9-475d-a250- 340e9a42a41e.png)

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
2. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён.

файл не отображён



1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html



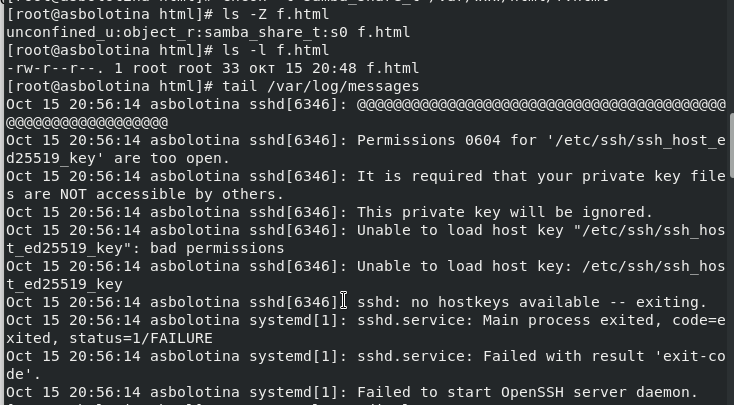
1. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t: chcon -t samba\_share\_t /var/www/html/test.html ls -Z

/var/www/html/test.html После этого проверьте, что контекст поменялся.



1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Вы должны получить сообщение об ошибке: Forbidden You don't have permission to access /test.html on this server.
2. Проанализируйте ситуацию. ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail

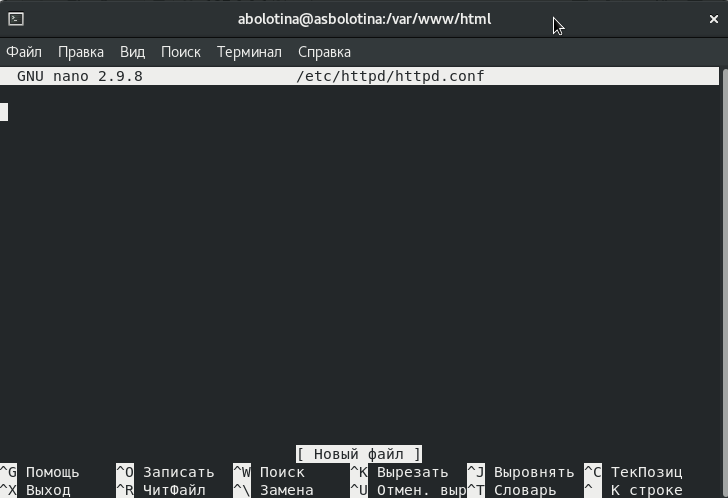
/var/log/messages



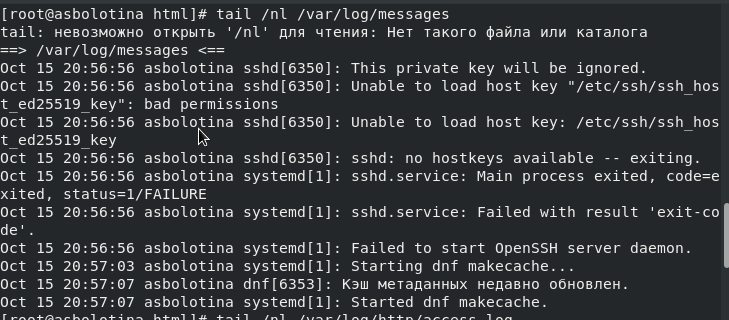
1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле

/etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.

файл пуст

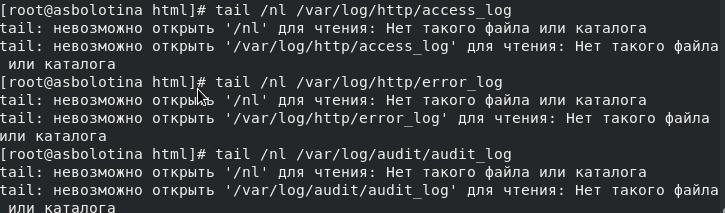


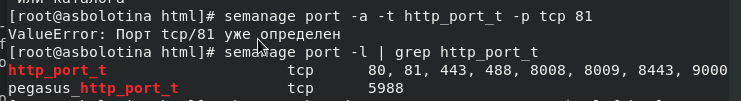
1. Выполните перезапуск веб-сервера Apache.
2. Проанализируйте лог-файлы: tail -nl /var/log/messages



Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и

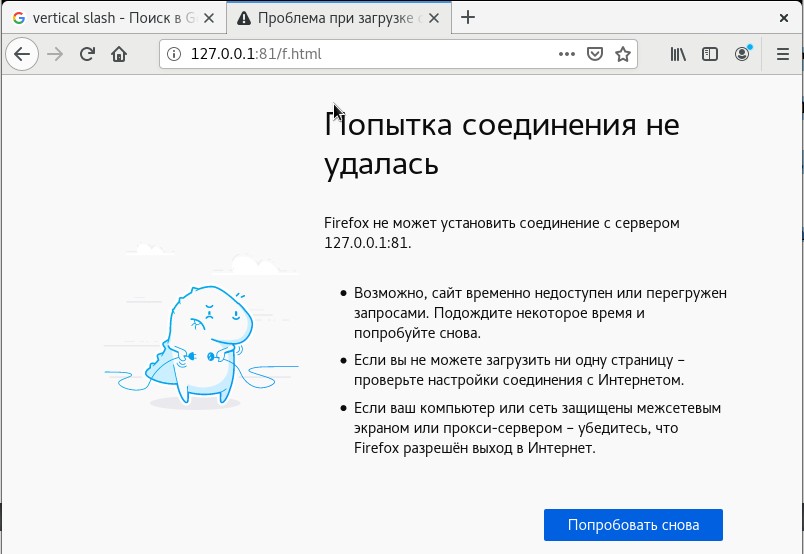
/var/log/audit/audit.log и выясните, в каких файлах появились записи.



1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке.
2. Попробуйте запустить веб-сервер Apache ещё раз.
3. Верните контекст httpd\_sys\_cоntent t к файлу /var/www/html/ test.html: chcon - t httpd\_sys\_content\_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово

«test».



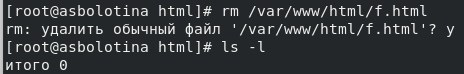


1. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
2. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp

81 и проверьте, что порт 81 удалён.



1. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html



# Выводы

Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практических навыков работы в консоли с дополнительными атрибутами.

Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

1. Лабораторная работа № 5

::: {#refs} :::