
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

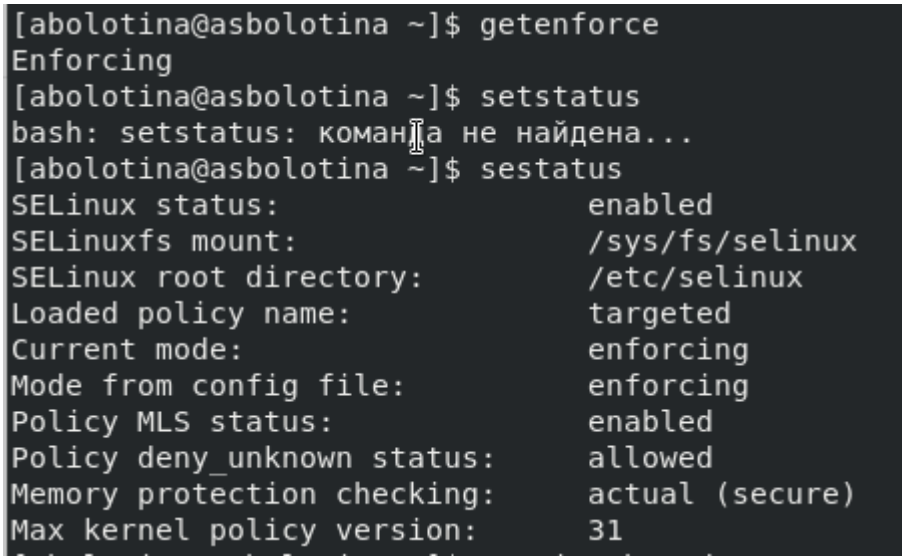
---

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.

2. 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.

```
[abolotina@asbolotina ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor prese>
  Drop-In: /etc/systemd/system/httpd.service.d
           └─nofile.conf
   Active: active (running) since Sat 2022-10-15 12:46:32 MSK; 2min 31s ago
     Docs: man:httpd.service(8)
 Main PID: 1352 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 5910)
   Memory: 12.1M
   CGroup: /system.slice/httpd.service
           ├─1352 /usr/sbin/httpd -DFOREGROUND
           ├─1376 /usr/sbin/httpd -DFOREGROUND
           ├─1377 /usr/sbin/httpd -DFOREGROUND
           ├─1378 /usr/sbin/httpd -DFOREGROUND
           └─1379 /usr/sbin/httpd -DFOREGROUND

окт 15 12:46:26 asbolotina systemd[1]: Starting The Apache HTTP Server...
окт 15 12:46:32 asbolotina httpd[1352]: AH00558: httpd: Could not reliably dete>
окт 15 12:46:32 asbolotina systemd[1]: Started The Apache HTTP Server.
окт 15 12:46:32 asbolotina httpd[1352]: Server configured, listening on: port 80
lines 1-21/21 (END)...skipping...
```

3. 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

```
[abolotina@asbolotina ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root        1352  0.0  0.1 281464  1092 ?
 Ss   12:46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      1376  0.0  0.0 294200   272 ?
 S    12:46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      1377  0.0  0.0 1351972  884 ?
 Sl   12:46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      1378  0.0  0.0 1483108  876 ?
 Sl   12:46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      1379  0.0  0.0 1351972  876 ?
 Sl   12:46   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aboloti+ 2999 0.0  0.0 121
08 996 pts/0 R+ 12:51   0:00 grep --color=auto httpd
[abolotina@asbolotina ~]$ sestarus -bigrep httpd
bash: sestarus: команда не найдена...
[abolotina@asbolotina ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v  Verbose check of process and file contexts.
  -b  Display current state of booleans.
```

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd Обратите внимание, что многие из них находятся в положении «off».

5. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.

```
[root@asbolotina html]# seinfo
bash: seinfo: команда не найдена...
Установить пакет «setools-console», предоставляющий команду «seinfo»? [N/y] y


 * Ожидание в очереди...
 * Загрузка списка пакетов....
Следующие пакеты должны быть установлены:
 setools-console-4.2.2-2.el8.x86_64     Policy analysis command-line tools for S
ELinux
Продолжить с этими изменениями? [N/y] y


 * Ожидание в очереди...
 * Ожидание аутентификации...
 * Ожидание в очереди... Не удалось установить пакеты: No URLs in mirrorlist
```

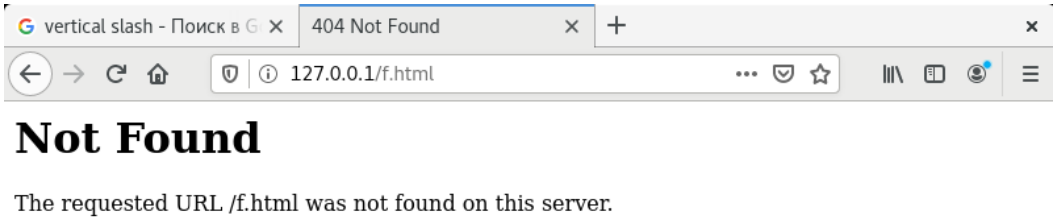
6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
7. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html

```
[abolotina@asbolotina ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 сен 15  2
020 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 сен 15  2
020 html
[abolotina@asbolotina ~]$ ls -lZ /var/www/html
итого 0
```

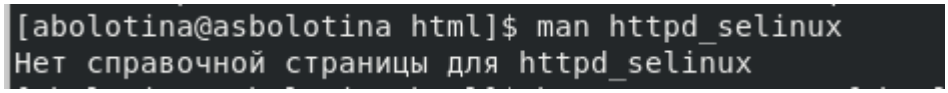
8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

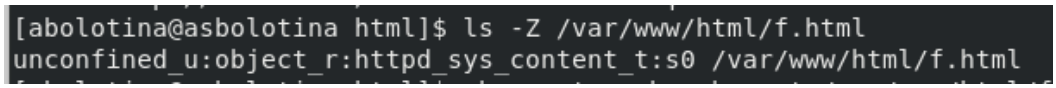
   test ![изображение](https://user-images.githubusercontent.com/113191444/196002387-a76752e2-bde9-475d-a250-340e9a42a41e.png)
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён.

- файл не отображён

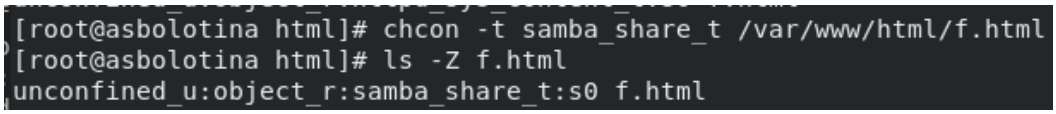


12. Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html





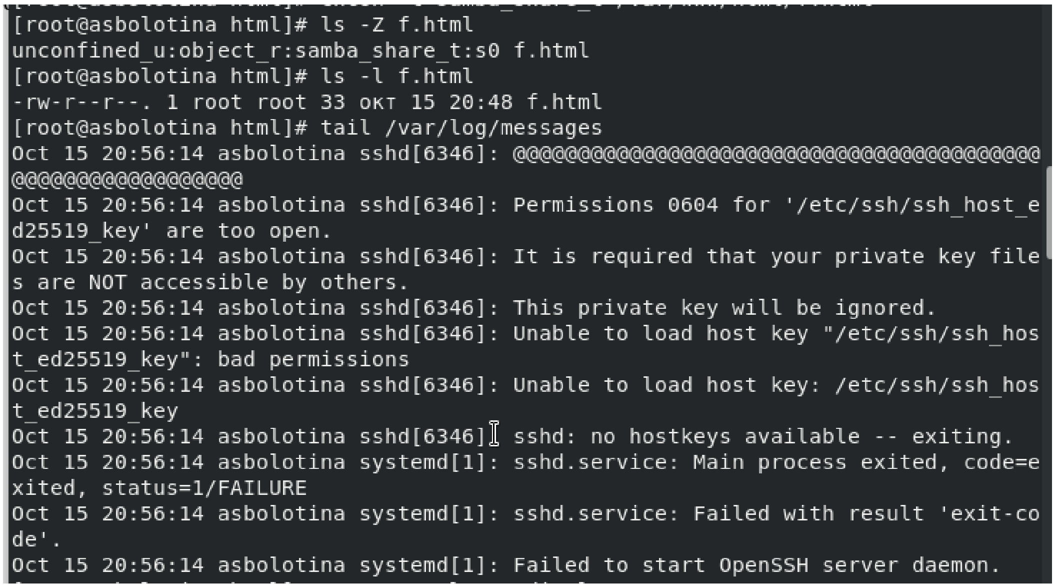
13. Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t: chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html После этого проверьте, что контекст поменялся.



14. 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.

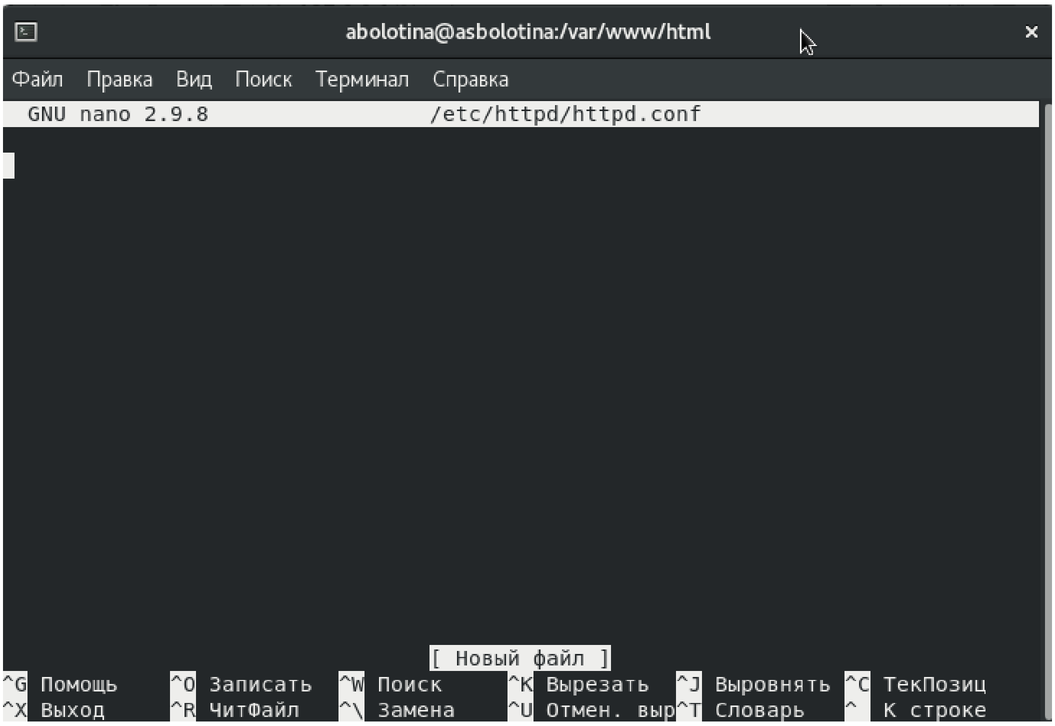
15. Проанализируйте ситуацию. ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail

/var/log/messages



16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-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



17. Выполните перезапуск веб-сервера Apache.

18. Проанализируйте лог-файлы: tail -nl /var/log/messages

```
[root@asbolotina html]# tail /nl /var/log/messages
tail: невозможно открыть '/nl' для чтения: Нет такого файла или каталога
==> /var/log/messages <==
Oct 15 20:56:56 asbolotina sshd[6350]: This private key will be ignored.
Oct 15 20:56:56 asbolotina sshd[6350]: Unable to load host key "/etc/ssh/ssh_hos
t_ed25519_key": bad permissions
Oct 15 20:56:56 asbolotina sshd[6350]: Unable to load host key: /etc/ssh/ssh_hos
t_ed25519_key
Oct 15 20:56:56 asbolotina sshd[6350]: sshd: no hostkeys available -- exiting.
Oct 15 20:56:56 asbolotina systemd[1]: sshd.service: Main process exited, code=e
xited, status=1/FAILURE
Oct 15 20:56:56 asbolotina systemd[1]: sshd.service: Failed with result 'exit-co
de'.
Oct 15 20:56:56 asbolotina systemd[1]: Failed to start OpenSSH server daemon.
Oct 15 20:57:03 asbolotina systemd[1]: Starting dnf makecache...
Oct 15 20:57:07 asbolotina dnf[6353]: Кэш метаданных недавно обновлен.
Oct 15 20:57:07 asbolotina systemd[1]: Started dnf makecache.
```

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.

```
[root@asbolotina html]# tail /nl /var/log/http/access_log
tail: невозможно открыть '/nl' для чтения: Нет такого файла или каталога
tail: невозможно открыть '/var/log/http/access_log' для чтения: Нет такого файла
 или каталога
[root@asbolotina html]# tail /nl /var/log/http/error_log
tail: невозможно открыть '/nl' для чтения: Нет такого файла или каталога
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла
или каталога
[root@asbolotina html]# tail /nl /var/log/audit/audit_log
tail: невозможно открыть '/nl' для чтения: Нет такого файла или каталога
tail: невозможно открыть '/var/log/audit/audit_log' для чтения: Нет такого файла
 или каталога
```

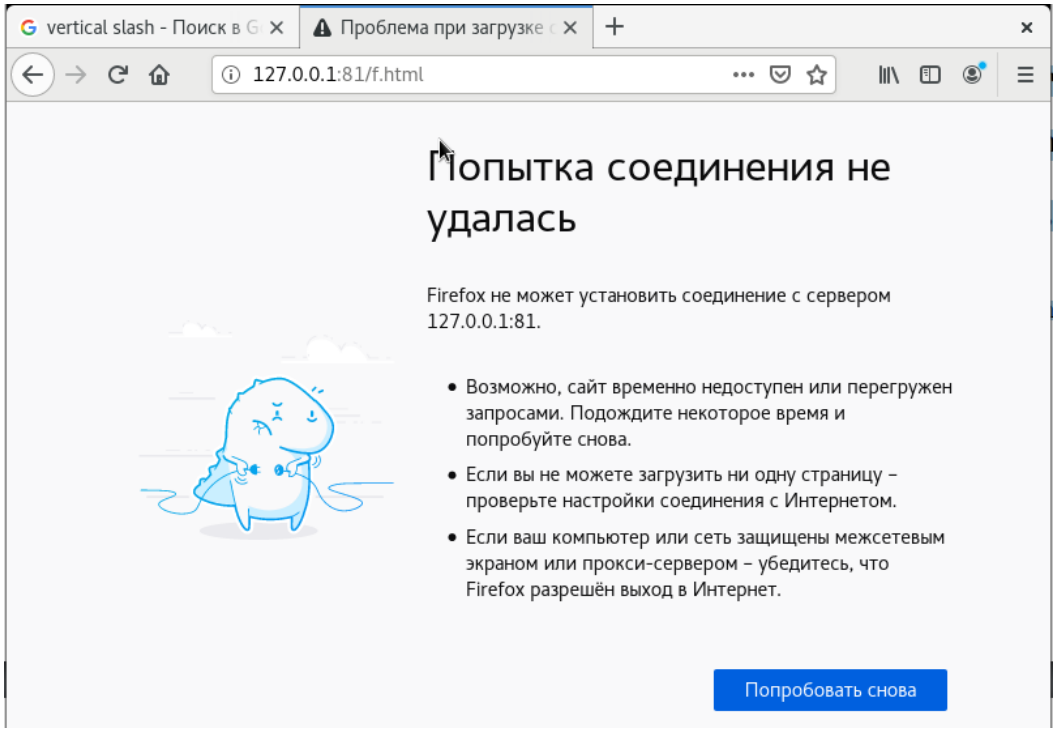
19. Выполните команду semanage port -a -t http_port_t -p tcp 81 После этого проверьте список портов командой semanage port -l | grep http_port_t Убедитесь, что порт 81 появился в списке.

```
[root@asbolotina html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@asbolotina html]# semanage port -l | grep http_port_t
http_port_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t            tcp      5988
```

20. Попробуйте запустить веб-сервер Apache ещё раз.

21. Верните контекст httpd_sys_content__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».

```
[root@asbolotina html]# chcon -t httpd_sys_content_t /var/www/html/f.html
```



22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.

23. Удалите привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 и проверьте, что порт 81 удалён.

```
[root@asbolotina html]# semanage port -d -t http_port_t -p tcp 81
rmValueError: Порт tcp/81 определен на уровне политики и не может быть удален
```

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

```
[root@asbolotina html]# rm /var/www/html/f.html
rm: удалить обычный файл '/var/www/html/f.html'? y
[root@asbolotina html]# ls -l
итого 0
```

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} :::