

# Защита лабораторной работы №6

## Информационная безопасность

---

Данзанова С. З.

2024

Российский университет дружбы народов, Москва, Россия

## Докладчик

.....: {.columns align=center} ::: {.column width="70%"}

- Данзанова Саяна Зоригтоевна
- Студентка группы НПИбд-01-21
- Студ. билет 1032217624
- Российский университет дружбы народов

# Цель лабораторной работы

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache

1. **SELinux (Security-Enhanced Linux)** обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему

# Теоретическая справка (1)

*SELinux имеет три основных режим работы:*

- Enforcing: режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.
- Permissive: в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.
- Disabled: полное отключение системы принудительного контроля доступа.

2. **Apache** — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA)

## Теоретическая справка (2)

*Для чего нужен Apache сервер:*

- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

# Выполнение лабораторной работы

Убедились, что SELinux работает в режиме enforcing политики targeted

```
[szdanzanova@szdanzanova ~]$ getenforce
Enforcing
[szdanzanova@szdanzanova ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                    enforcing
Mode from config file:           enforcing
Policy MLS status:               enabled
Policy deny_unknown status:      allowed
Memory protection checking:      actual (secure)
Max kernel policy version:       33
```

**Рис. 1:** (Проверка режима enforcing политики targeted)



# Выполнение лабораторной работы

Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает

```
Выполнено!
[szdzanazanova@szdzanazanova ~]$ sudo systemctl start httpd
[szdzanazanova@szdzanazanova ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[szdzanazanova@szdzanazanova ~]$ 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; preset: disabled)
   Active: active (running) since Mon 2024-10-07 00:17:41 MSK; 38s ago
     Docs: man:httpd.service(8)
  Main PID: 6829 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
    Tasks: 177 (limit: 17412)
   Memory: 26.0M
      CPU: 130ms
   CGroup: /system.slice/httpd.service
           └─6829 /usr/sbin/httpd -DFOREGROUND
             └─6830 /usr/sbin/httpd -DFOREGROUND
               └─6831 /usr/sbin/httpd -DFOREGROUND
                 └─6835 /usr/sbin/httpd -DFOREGROUND
                   └─6837 /usr/sbin/httpd -DFOREGROUND

окт 07 00:17:41 szdzanazanova systemd[1]: Starting The Apache HTTP Server...
окт 07 00:17:41 szdzanazanova httpd[6829]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, setting 'ServerName' to localhost.
окт 07 00:17:41 szdzanazanova systemd[1]: Started The Apache HTTP Server.
окт 07 00:17:41 szdzanazanova httpd[6829]: Server configured, listening on: port 80
lines 1-20/20 (END)...skipping...
```

# Выполнение лабораторной работы

Определили контекст безопасности веб-сервера Apache

```
[szdanzanova@szdanzanova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 6829 0.0 0.4 20364 11476 ?
Ss 00:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6830 0.0 0.2 22096 7256 ?
S 00:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6831 0.0 0.6 1112656 17560 ?
Sl 00:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6835 0.0 0.3 981652 11172 ?
Sl 00:17 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 6837 0.0 0.3 981520 11172 ?
Sl 00:17 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 szdanza+ 7064 0.0 0.0 221
688 2432 pts/0 S+ 00:19 0:00 grep --color=auto httpd
```

**Рис. 3:** (Контекст безопасности веб-сервера Apache)

# Выполнение лабораторной работы

Посмотрели текущее состояние переключателей, многие из переключателей находятся в положении “off”

```
[szdanzanova@szdanzanova ~]$ sestatus -b httpd
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:              targeted
Current mode:                    enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Policy booleans:
abrt_anon_write                  off
abrt_handle_event                off
abrt_upload_watch_anon_write    on
antivirus_can_scan_system       off
antivirus_use_jit               off
auditadm_exec_content           on
authlogin_nsswitch_use_ldap     off
authlogin_radius                off
authlogin_yubikey               off
awstats_purge_apache_log_files  off
boinc_execmem                   on
```

# Выполнение лабораторной работы

Посмотрели статистику по политике. Множество пользователей - 8, ролей - 15, типов 5145

```
[szdanzanova@szdanzanova ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      135      Permissions:      457
Sensitivities: 1      Categories:      1024
Types:        5145     Attributes:       259
Users:        8       Roles:           15
Booleans:     356     Cond. Expr.:     388
Allow:        65504   Neverallow:      0
Auditallow:   176     Dontaudit:       8682
Type_trans:   271770  Type_change:     94
Type_member:  37      Range_trans:     5931
Role_allow:   40      Role_trans:      417
Constraints:  70      Validatetrans:   0
MLS Constrai: 72     MLS Val. Tran:   0
Permissives:  4      Polcap:          6
Defaults:     7      Typebounds:      0
Allowxperm:   0      Neverallowxperm: 0
Auditallowxperm: 0  Dontauditxperm:  0
Ibendportcon: 0      Ibpkeycon:       0
Initial SIDs: 27     Fs_use:          35
Genfscon:     109    Portcon:         665
Netifcon:     0      Nodecon:         0
```

# Выполнение лабораторной работы

Посмотрели файлы и поддиректории, находящиеся в директории /var/www. Определили, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html

```
[szdanzanova@szdanzanova ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 апр  8 19
:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр  8 19
:30 html
[szdanzanova@szdanzanova ~]$ ls -lZ /var/www/html
итого 0
```

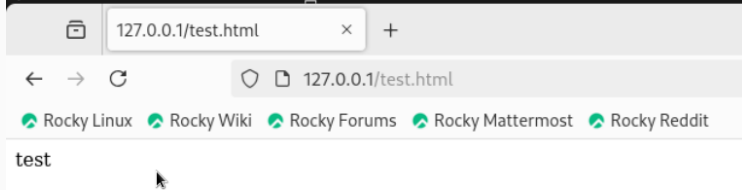
**Рис. 6:** (Просмотр файлов и поддиректорий в директории /var/www)

# Выполнение лабораторной работы

От имени суперпользователя создали html-файл. Контекст созданного файла - httpd\_sys\_content\_t

Обратились к файлу через веб-сервер, введя в браузере адрес "http://127.0.0.1/test.html". Файл был успешно отображен

```
[root@szdanzanova szdanzanova]# touch /var/www/html/test.html
[root@szdanzanova szdanzanova]# nano /var/www/html/test.html
[root@szdanzanova szdanzanova]# cat /var/www/html/test.html
<html>
<body> test </body>
</html>
```



# Выполнение лабораторной работы

Изучив справку `httpd_selinux`, выяснили, какие контексты определены для файлов `httpd`.

Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона).

Изменили контекст файла на `samba_share_t`

Попробовали еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “`http://127.0.0.1/test.html`” и получили сообщение об ошибке (т.к. кустановленному ранее контексту процесс `httpd` не имеет доступа)

# Выполнение лабораторной работы

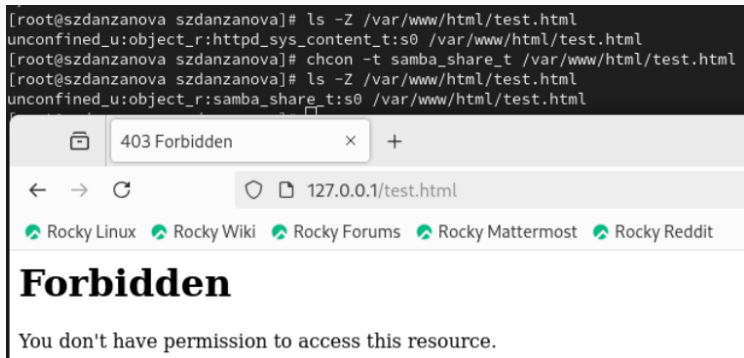


Рис. 8: (Изменение контекста. Обращение к файлу через веб-сервер)



# Выполнение лабораторной работы

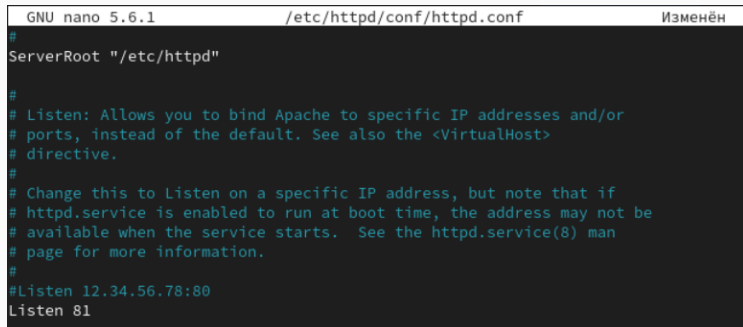
Убедились, что читать данный файл может любой пользователь.

Просмотрели системный лог-файл веб-сервера Apache, отображающий ошибки

```
[root@szdanzanova szdanzanova]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 32 окт  7 00:31 /var/www/html/test.html
[root@szdanzanova szdanzanova]# tail /var/log/messages
Oct  7 00:37:48 szdanzanova systemd[1]: Started dbus-1.1-org.fedoraproject.Setrou
bleshootPrivileged@0.service.
Oct  7 00:37:51 szdanzanova setroubleshoot[8262]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файлу /var/www/html/test.html. Для выполнения всех сообщений
SELinux: sealert -l 42385416-fae5-4b19-b8a5-b8c69ca05aa7
Oct  7 00:37:51 szdanzanova setroubleshoot[8262]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файлу /var/www/html/test.html.#012#012***** Модуль restorec
on предлагает (точность 92.2) *****#012#012Если вы хотите и
справить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#01
2То вы можете запустить restorecon. Возможно, попытка доступа была остановлена и
з-за недостаточных разрешений для доступа к родительскому каталогу, и в этом слу
чае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#0
12# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_cont
ent предлагает (точность 7.83) *****#012#012Если вы хотите лечи
ть test.html как общедоступный контент#012То необходимо изменить метку test.html
с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a
-t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html
/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getat
tr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ош
ибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сде
лать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct  7 00:37:51 szdanzanova setroubleshoot[8262]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файлу /var/www/html/test.html. Для выполнения всех сообщений
SELinux: sealert -l 42385416-fae5-4b19-b8a5-b8c69ca05aa7
Oct  7 00:37:52 szdanzanova setroubleshoot[8262]: SELinux запрещает /usr/sbin/ht
tpd доступ getattr к файлу /var/www/html/test.html.#012#012***** Модуль restorec
on предлагает (точность 92.2) *****#012#012Если вы хотите и
справить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#01
2То вы можете запустить restorecon. Возможно, попытка доступа была остановлена и
```

# Выполнение лабораторной работы

В файле `/etc/httpd/conf/httpd.conf` заменили строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81



```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Изменён
#
ServerRoot "/etc/httpd"

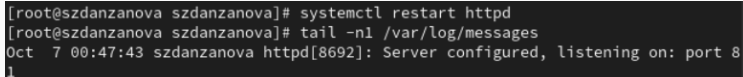
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
```

**Рис. 10:** (Установка веб-сервера Apache на прослушивание TCP-порта 81) 18/25

# Выполнение лабораторной работы

Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -n1 /var/log/messages”

Просмотрели файлы “var/log/http/error\_log”, “/var/log/http/access\_log” и “/var/log/audit/audit.log” и выяснили, что запись появилась в последнем файле



```
[root@szdanzanova szdanzanova]# systemctl restart httpd
[root@szdanzanova szdanzanova]# tail -n1 /var/log/messages
Oct  7 00:47:43 szdanzanova httpd[8692]: Server configured, listening on: port 8
1
```

**Рис. 11:** (Перезапуск веб-сервера и анализ лог-файлов)

# Выполнение лабораторной работы

Проверили список портов командой, убедились, что порт 81 есть в списке и запускаем веб-сервер Apache снова

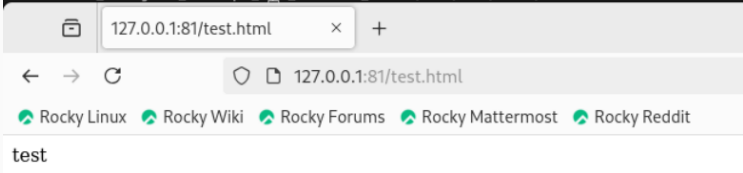
```
[szdanzanova@szdanzanova ~]$ sudo semanage port -a -t http_port_t -p tcp 81
[sudo] пароль для szdanzanova:
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module
               ,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81
[szdanzanova@szdanzanova ~]$ sudo 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
[szdanzanova@szdanzanova ~]$ systemctl restart httpd
```

**Рис. 12:** (Проверка установки порта 81)

# Выполнение лабораторной работы

Вернули контекст “httpd\_sys\_content\_t” файлу “/var/www/html/test.html” и попробовали получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, увидели содержимое файла - слово “test”

```
[szdanzanova@szdanzanova ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[szdanzanova@szdanzanova ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```



The screenshot shows a web browser window with the address bar set to `127.0.0.1:81/test.html`. The browser's address bar also displays the full URL `http://127.0.0.1:81/test.html`. Below the address bar, there are several links: [Rocky Linux](#), [Rocky Wiki](#), [Rocky Forums](#), [Rocky Mattermost](#), and [Rocky Reddit](#). The main content area of the browser displays the word `test`.

**Рис. 13:** (Обращение к файлу через веб-сервер)

# Выполнение лабораторной работы

Исправили обратно конфигурационный файл apache, вернув “Listen 80”. Попытались удалить привязку http\_port к 81 порту, но этот порт определен на уровне политики, поэтому его нельзя удалить

```
#  
#Listen 12.34.56.78:80  
Listen 80
```

**Рис. 14:** (Возвращение Listen 80 и попытка удалить порт 81)

# Выполнение лабораторной работы

Удалили файл “/var/www/html/test.html”

```
[root@szdanzanova szdanzanova]# sudo rm /var/www/html/test.html  
[root@szdanzanova szdanzanova]# ls /var/www/html/test.html  
ls: невозможно получить доступ к '/var/www/html/test.html': Нет такого файла или каталога
```

**Рис. 15:** (Удаление файла test.html)

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.



# Список литературы. Библиография

[0] Методические материалы курса

[1] SELinux: <https://habr.com/ru/companies/kingservers/articles/209644/>

[2] Apache: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>