

Лабораторная работа №6

Мандатное разграничение прав в Linux

Щербак Маргарита Романовна

НПИбд-02-21

Студ. билет: 1032216537

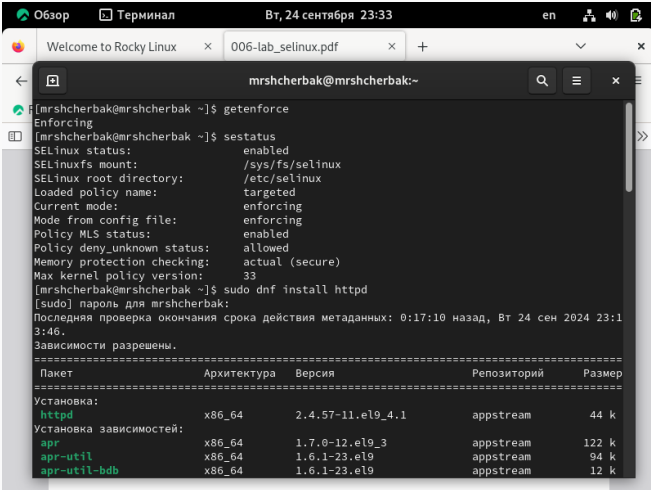
2024

RUDN

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

Информационная безопасность представляет собой защиту данных и поддерживающей инфраструктуры от случайных или преднамеренных воздействий природного или искусственного характера, которые могут нанести ущерб владельцам или пользователям этой информации и инфраструктуры.

Выполнение лабораторной работы



The screenshot shows a web browser window with a terminal tab titled "Терминал". The terminal is running on a Rocky Linux system. The user, mrshcherbak, has executed the following commands:

```
[mrshcherbak@mrshcherbak ~]$ getenforce
Enforcing
[mrshcherbak@mrshcherbak ~]$ 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
[mrshcherbak@mrshcherbak ~]$ sudo dnf install httpd
[sudo] пароль для mrshcherbak:
Последняя проверка окончания срока действия метаданных: 0:17:10 назад, Вт 24 сен 2024 23:13:46.
Зависимости разрешены.
```

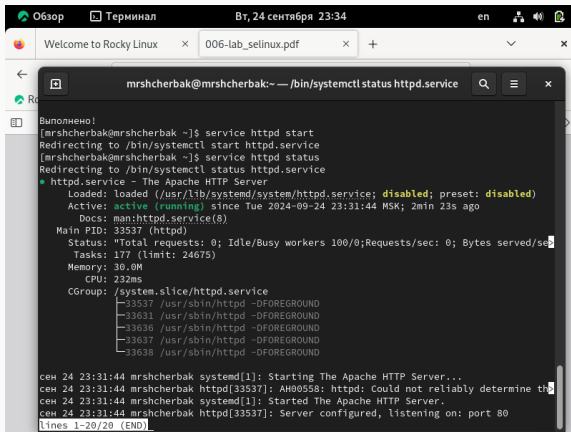
Below the command output, a table lists the installed packages and their dependencies:

Пакет	Архитектура	Версия	Репозиторий	Размер
Установка:				
httpd	x86_64	2.4.57-11.el9_4.1	appstream	44 k
Установка зависимостей:				
apr	x86_64	1.7.0-12.el9_3	appstream	122 k
apr-util	x86_64	1.6.1-23.el9	appstream	94 k
apr-util-bdb	x86_64	1.6.1-23.el9	appstream	12 k

Рис. 1: getenforce и sestatus

Выполнение лабораторной работы

Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает.



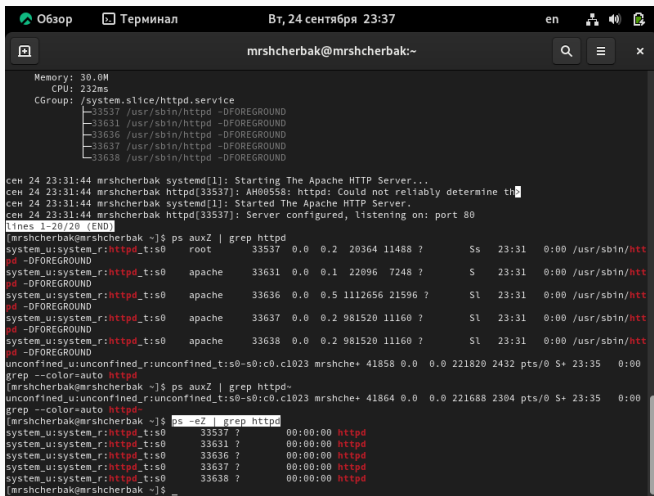
```
Обзор Терминал Вт, 24 сентября 23:34 en
Welcome to Rocky Linux x 006-lab_selinux.pdf x +
mrshcherbak@mrshcherbak:~ — /bin/systemctl status httpd.service
Выполнено!
[mrshcherbak@mrshcherbak ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[mrshcherbak@mrshcherbak ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
   Active: active (running) since Tue 2024-09-24 23:31:44 MSK; 2min 23s ago
     Docs: man:httpd.service(8)
   Main PID: 33537 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
      Tasks: 177 (limit: 24675)
     Memory: 30.0M
        CPU: 232ms
    CGroup: /system.slice/httpd.service
            └─33537 /usr/sbin/httpd -DFOREGROUND
              └─33631 /usr/sbin/httpd -DFOREGROUND
                └─33636 /usr/sbin/httpd -DFOREGROUND
                  └─33637 /usr/sbin/httpd -DFOREGROUND
                    └─33638 /usr/sbin/httpd -DFOREGROUND

сен 24 23:31:44 mrshcherbak systemd[1]: Starting The Apache HTTP Server...
сен 24 23:31:44 mrshcherbak httpd[33537]: AH00558: httpd: Could not reliably determine the
сен 24 23:31:44 mrshcherbak systemd[1]: Started The Apache HTTP Server.
сен 24 23:31:44 mrshcherbak httpd[33537]: Server configured, listening on: port 80
Lines 1-20/20 (END)
```

Рис. 2: Веб-сервер httpd

Выполнение лабораторной работы

Нашла веб-сервер Apache в списке процессов.



```
Обзор Терминал Вт, 24 сентября 23:37 en [user icon] [volume icon] [refresh icon]
mrshcherbak@mrshcherbak:~

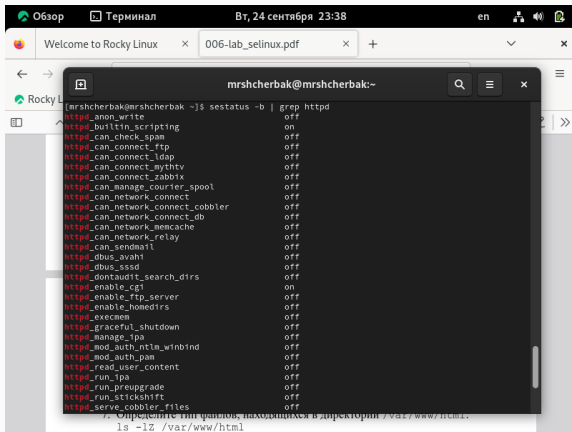
Memory: 30.0M
CPU: 232ms
CGroup: /system.slice/httpd.service
├─33537 /usr/sbin/httpd -DFOREGROUND
├─33631 /usr/sbin/httpd -DFOREGROUND
├─33636 /usr/sbin/httpd -DFOREGROUND
├─33637 /usr/sbin/httpd -DFOREGROUND
└─33638 /usr/sbin/httpd -DFOREGROUND

сен 24 23:31:44 mrshcherbak systemd[1]: Starting The Apache HTTP Server...
сен 24 23:31:44 mrshcherbak httpd[33537]: AH00558: httpd: Could not reliably determine the
сен 24 23:31:44 mrshcherbak systemd[1]: Started The Apache HTTP Server.
сен 24 23:31:44 mrshcherbak httpd[33537]: Server configured, listening on: port 80
lines 1-20/20 (END)
[mrshcherbak@mrshcherbak ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 33537 0.0 0.2 20364 11488 ? Ss 23:31 0:00 /usr/sbin/httpd
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33631 0.0 0.1 22096 7248 ? S 23:31 0:00 /usr/sbin/httpd
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33636 0.0 0.5 1112656 21596 ? Sl 23:31 0:00 /usr/sbin/httpd
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33637 0.0 0.2 981520 11160 ? Sl 23:31 0:00 /usr/sbin/httpd
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33638 0.0 0.2 981520 11160 ? Sl 23:31 0:00 /usr/sbin/httpd
pd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 mrshche+ 41858 0.0 0.0 221820 2432 pts/0 S+ 23:35 0:00
grep --color=auto httpd
[mrshcherbak@mrshcherbak ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0:c1023 mrshche+ 41864 0.0 0.0 221688 2304 pts/0 S+ 23:35 0:00
grep --color=auto httpd-
[mrshcherbak@mrshcherbak ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 33537 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33631 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33636 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33637 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33638 ? 00:00:00 httpd
[mrshcherbak@mrshcherbak ~]$
```

Рис. 3: Веб-сервер Apache

Выполнение лабораторной работы

Посмотрела текущее состояние переключателей SELinux для Apache.



The screenshot shows a terminal window titled "mrshcherbak@mrshcherbak:~" with the command `sestatus -b | grep httpd` executed. The output lists various SELinux booleans for the httpd process, most of which are set to "off". Below the terminal window, a portion of a file listing command is visible.

```
mrshcherbak@mrshcherbak:~$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mysqld off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avaahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipp off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipp off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
```

1. Определите тип файлов, находящихся в директории /var/www/html.
ls -lZ /var/www/html

Рис. 4: Состояние переключателей

Выполнение лабораторной работы

Посмотрела статистику по политике с помощью команды `seinfo`.

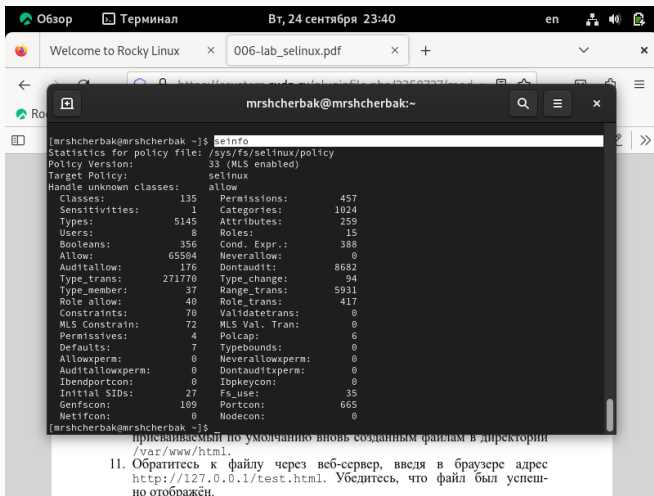


Рис. 5: Статистика по политике с помощью команды `seinfo`

Выполнение лабораторной работы

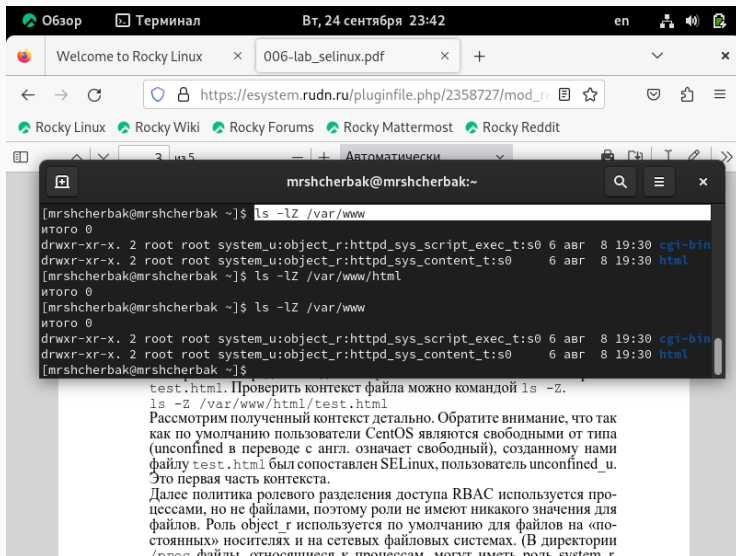


Рис. 6: Просмотр типов файлов и поддиректорий

Выполнение лабораторной работы

Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания. А также проверила контекст созданного файла - httpd_sys_content_t.

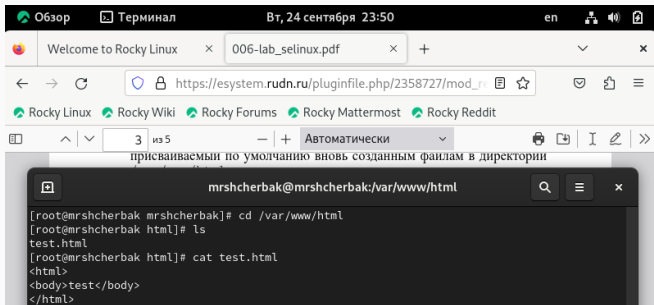


Рис. 7: Содержимое файла

Выполнение лабораторной работы

Проверила контекст созданного файла. Обратилась к файлу через веб-сервер.

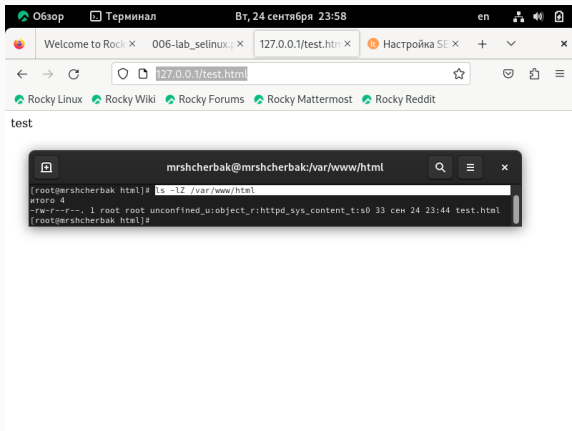


Рис. 8: Контекст и отображение файла

Выполнение лабораторной работы

Проверила контекст файла командой `ls -Z`. Изменила контекст файла с `httpd_sys_content_t` на `samba_share_t`.

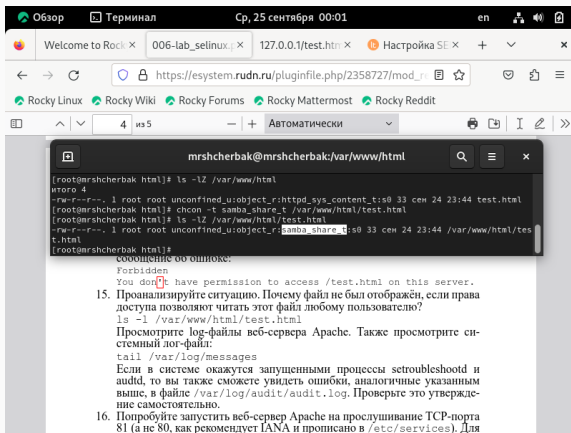


Рис. 9: Проверка контекста и его изменение

Выполнение лабораторной работы

Попробовала ещё раз получить доступ к файлу через веб-сервер. Получила сообщение об ошибке.

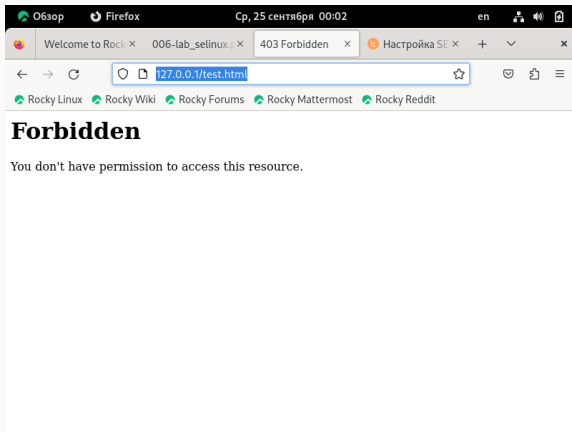
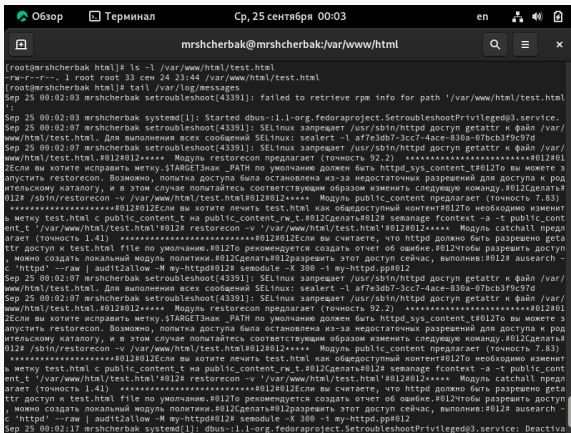


Рис. 10: Ошибка

Выполнение лабораторной работы

Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: tail /var/log/messages.

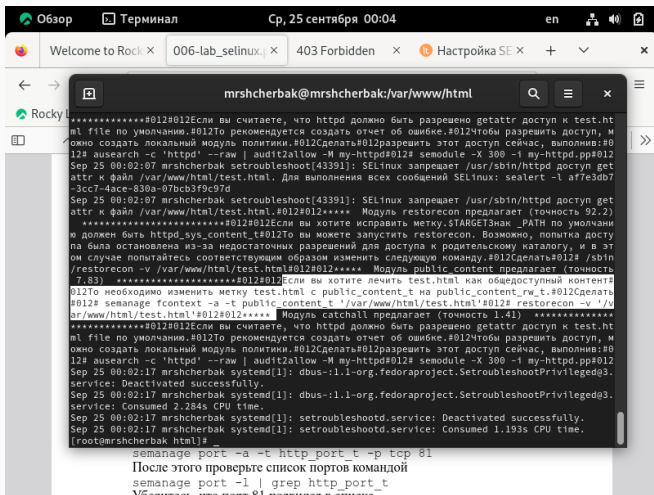


```
Обзор Терминал Ср, 25 сентября 00:03 en
mrshcherbak@mrshcherbak:/var/www/html

[root@mrshcherbak html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 сен 24 23:44 /var/www/html/test.html
[root@mrshcherbak html]# tail /var/log/messages
Sep 25 00:02:03 mrshcherbak setroubleshoot[43391]: failed to retrieve rpm info for path '/var/www/html/test.html'
Sep 25 00:02:03 mrshcherbak systemd[1]: Started dbus-1.1-1-org.fedoraproject.SetroubleshootPrivileged03.service.
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l a7fe3db7-3cc7-4ace-83ba-07bcb3f9c97d
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/
www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#012*****
Если вы хотите исправить метку.$TARGETзнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете з
апустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к род
ительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83)
*****#012#012***** Если вы хотите решить test.html как общедоступный контент#012То необходимо изменить
метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_cont
ent_t '/var/www/html/test.html'#012#012 restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предл
агает (точность 1.41) *****#012#012***** Если вы считаете, что httpd должно быть разрешено geta
ttr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ
, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l a7fe3db7-3cc7-4ace-83ba-07bcb3f9c97d
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/
www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#012*****
Если вы хотите исправить метку.$TARGETзнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете з
апустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к род
ительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83)
*****#012#012***** Если вы хотите решить 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_cont
ent_t '/var/www/html/test.html'#012#012 restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предл
агает (точность 1.41) *****#012#012***** Если вы считаете, что httpd должно быть разрешено geta
ttr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ
, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:02:17 mrshcherbak systemd[1]: dbus-1.1-1-org.fedoraproject.SetroubleshootPrivileged03.service: Deactiva
```

Рис. 11: log-файлы

Выполнение лабораторной работы



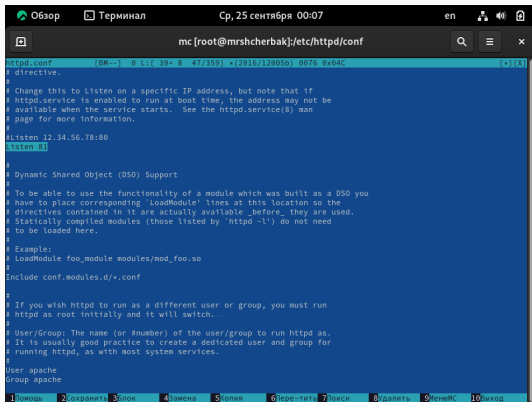
The screenshot shows a terminal window with the title bar "Обзор Терминал Ср, 25 сентября 00:04". The terminal output displays the following commands and their results:

```
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.ht
ml file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, м
ожно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#0
12# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ get
attr к файлу /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l af7e3db7
-3cc7-4ace-830a-07bcb3f9c97d
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ get
attr к файлу /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2)
*****#012#012Если вы хотите исправить метку.$TARGETЗнак _PATH по умолчанию
о должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка досту
па была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в эт
ом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin
/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность
7.83) *****#012#012Если вы хотите лечить 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 '/v
ar/www/html/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.ht
ml file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, м
ожно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#0
12# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:02:17 mrshcherbak systemd[1]: dbus-1.11-org.fedoraproject.SetroubleshootPrivileged@3.
service: Deactivated successfully.
Sep 25 00:02:17 mrshcherbak systemd[1]: dbus-1.11-org.fedoraproject.SetroubleshootPrivileged@3.
service: Consumed 2.284s CPU time.
Sep 25 00:02:17 mrshcherbak systemd[1]: setroubleshoot.service: Deactivated successfully.
Sep 25 00:02:17 mrshcherbak systemd[1]: setroubleshoot.service: Consumed 1.193s CPU time.
[root@mrshcherbak html]#
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
```

Рис. 12: log-файлы

Выполнение лабораторной работы

Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81.



```
Обзор Терминал Ср, 25 сентября 00:07 en
mc [root@mrshcherbak]:/etc/httpd/conf
httpd.conf (BM~) 0 L: (39* 8 47/359) *(2016/12005b) 0070 0x04C (*)
# 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
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
# Include conf.modules.d/*.conf
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch...
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User apache
Group apache
```

Рис. 13: Замена порта в файле

Выполнение лабораторной работы

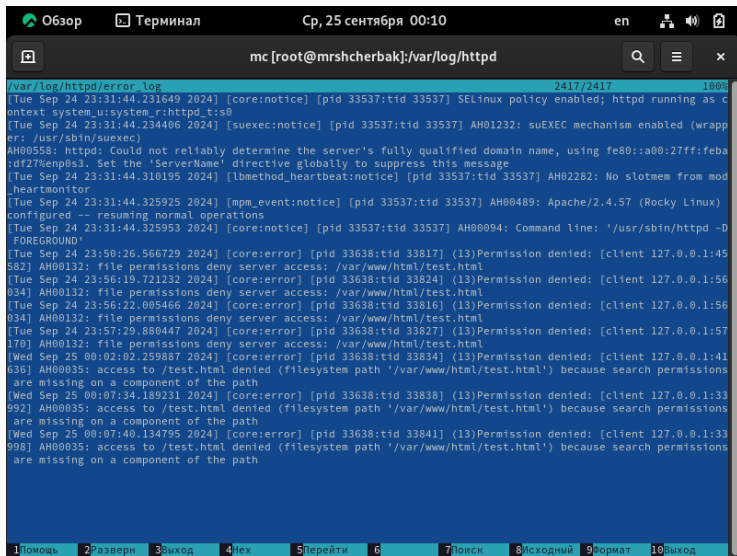
```
Обзор Терминал Ср, 25 сентября 00:10 en [root@mrshcherbak]:/var/log/httpd

/var/log/httpd/access_log 1593/1593 100%
127.0.0.1 - - [24/Sep/2024:23:50:26 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:50:27 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Moz
illa/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:56:19 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:56:22 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:57:29 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:58:08 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64;
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:02:02 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:02:02 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Moz
illa/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:07:34 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:07:40 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64
; rv:109.0) Gecko/20100101 Firefox/115.0"

1 Помощь 2 Разверн 3 Выход 4 Нех 5 Перейти 6 7 Поиск 8 Исходный 9 Формат 10 Выход
```

Рис. 15: /var/log/http/access_log

Выполнение лабораторной работы



```
mc [root@mrshcherbak]:/var/log/httpd

/var/log/httpd/error_log 2417/2417 100%
[Tue Sep 24 23:31:44.231649 2024] [core:notice] [pid 33537:tid 33537] SELinux policy enabled; httpd running as c
ontext system_u:system_r:httpd_t:s0
[Tue Sep 24 23:31:44.234406 2024] [suexec:notice] [pid 33537:tid 33537] AH01232: suEXEC mechanism enabled (wrapp
er: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:feba
:df27::enp0s3. Set the 'ServerName' directive globally to suppress this message
[Tue Sep 24 23:31:44.310195 2024] [lbmethod_heartbeat:notice] [pid 33537:tid 33537] AH02282: No slotmem from mod
_heartbeat
[Tue Sep 24 23:31:44.325925 2024] [mpm_event:notice] [pid 33537:tid 33537] AH00489: Apache/2.4.57 (Rocky Linux)
configured -- resuming normal operations
[Tue Sep 24 23:31:44.325953 2024] [core:notice] [pid 33537:tid 33537] AH00094: Command line: '/usr/sbin/httpd -D
FOREGROUND'
[Tue Sep 24 23:50:26.566729 2024] [core:error] [pid 33638:tid 33817] (13)Permission denied: [client 127.0.0.1:45
582] AH00132: file permissions deny server access: /var/www/html/test.html
[Tue Sep 24 23:56:19.721232 2024] [core:error] [pid 33638:tid 33824] (13)Permission denied: [client 127.0.0.1:56
034] AH00132: file permissions deny server access: /var/www/html/test.html
[Tue Sep 24 23:56:22.005466 2024] [core:error] [pid 33638:tid 33816] (13)Permission denied: [client 127.0.0.1:56
034] AH00132: file permissions deny server access: /var/www/html/test.html
[Tue Sep 24 23:57:29.880447 2024] [core:error] [pid 33638:tid 33827] (13)Permission denied: [client 127.0.0.1:57
170] AH00132: file permissions deny server access: /var/www/html/test.html
[Wed Sep 25 00:02:02.259887 2024] [core:error] [pid 33638:tid 33834] (13)Permission denied: [client 127.0.0.1:41
636] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Wed Sep 25 00:07:34.189231 2024] [core:error] [pid 33638:tid 33838] (13)Permission denied: [client 127.0.0.1:33
992] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Wed Sep 25 00:07:40.134795 2024] [core:error] [pid 33638:tid 33841] (13)Permission denied: [client 127.0.0.1:33
998] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path

1Помощь 2Разверн 3Выход 4Нех 5Перейти 6 7Поиск 8Исходный 9Формат 10Выход
```

Рис. 16: /var/log/httpd/error_log

Выполнение лабораторной работы

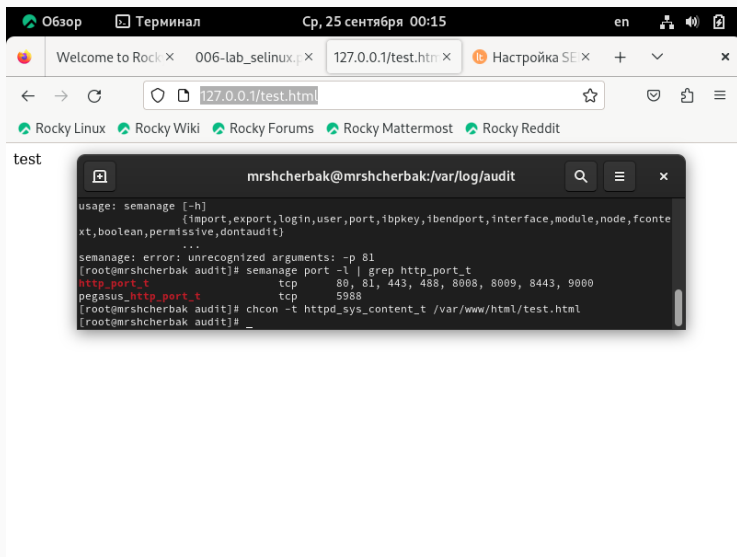


Рис. 17: Semanage и запуск веб-сервера

Выполнение лабораторной работы

Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту: `semanage port -d -t http_port_t -p tcp 81`. Удалила файл `/var/www/html/test.html` (рис. 18).

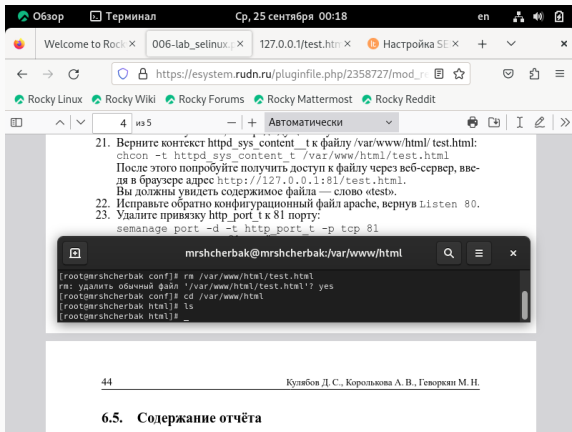


Рис. 18: Удаление файла

Таким образом, в ходе ЛР№6 я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

1. Методические материалы курса.
2. Linux Kernel Security [Электронный ресурс]: URL: <http://www.cyberciti.biz/tips/selinux-vs-apparmor-vs-grsecurity.html> (дата обращения 24.09.2024)
3. Security-Enhanced Linux [Электронный ресурс]: Официальный сайт SELinux. URL: <http://www.nsa.gov/research/selinux/index.shtml> (дата обращения 24.09.2024)