

Отчет по лабораторной работе №6

Дисциплина: Информационная безопасность

Выполнила Дяченко Злата Константиновна, НФИбд-03-18

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Шаг 1	6
3.2	Шаг 2	6
3.3	Шаг 3	7
3.4	Шаг 4	8
3.5	Шаг 5	8
3.6	Шаг 6	9
3.7	Шаг 7	9
3.8	Шаг 8	9
3.9	Шаг 9	10
3.10	Шаг 10	11
3.11	Шаг 11	11
3.12	Шаг 12	12
3.13	Шаг 13	13
3.14	Шаг 14	14
3.15	Шаг 15	14
3.16	Шаг 16	14
3.17	Шаг 17	15
3.18	Шаг 18	15
4	Выводы	16

List of Figures

3.1	Список процессов	6
3.2	Состояния переключателей SELinux для Apache	7
3.3	seinfo	8
3.4	Информация о поддиректориях /var/www	8
3.5	Содержание файла test.html	9
3.6	Контекст файла	9
3.7	Отображение файла	9
3.8	Справка man httpd_selinux	10
3.9	Изменение контекста файла	11
3.10	Ошибка	11
3.11	Файл /var/log/messages	12
3.12	Файл /var/log/audit/audit.log	12
3.13	Замена строки в файле	13
3.14	Перезапуск веб-сервера Apache	13
3.15	Просмотр файлов	13
3.16	Список портов	14
3.17	Перезапуск веб-сервера Apache	14
3.18	Получение доступа к файлу через веб-браузер	15
3.19	Исправление файла	15
3.20	Попытка удалить привязку http_port_t к 81 порту и удаление файла	15

1 Цель работы

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

2 Задание

Выполнить все пункты указания к лабораторной работе, чтобы достигнуть цель.

3 Выполнение лабораторной работы

3.1 Шаг 1

Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted. Обратилась с помощью браузера к веб-серверу и запустила его. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности: `system_u:system_r:httpd_t:s0`. Использовала команду `ps auxZ | grep httpd`, результат представлен на Рисунке 1 (рис. 3.1)

```
[zkdyachenko@zkdyachenko ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      4381  0.0  0.4 224084  5008 ?        Ss   13:18   0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4386  0.0  0.3 226168  3092 ?        S    13:18   0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4387  0.0  0.3 226168  3092 ?        S    13:18   0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4388  0.0  0.3 226168  3092 ?        S    13:18   0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4389  0.0  0.3 226168  3092 ?        S    13:18   0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache  4390  0.0  0.3 226168  3092 ?        S    13:18   0:00 /usr/sbin/httpd
-DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 zkdyach+ 4509  0.0  0.0 112832  968 pts/0  S+   13:22   0:00 gre
p --color=auto httpd
```

Figure 3.1: Список процессов

3.2 Шаг 2

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис. 3.2). Многие из них находятся в положении «off».

```
[zkdyachenko@zkdyachenko ~]$ 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_mythtv off
httpd_can_connect_zabbix 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_avahi 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 on
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
zkdyachenko@zkdyachenko ~1$ █
```

Figure 3.2: Состояния переключателей SELinux для Apache

3.3 Шаг 3

Посмотрела статистику по политике с помощью команды seinfo (рис. 3.3).

```
[zkdyachenko@zkdyachenko ~]$ seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:       272
Sensitivities:    1        Categories:       1024
Types:            4793     Attributes:        253
Users:            8        Roles:            14
Booleans:         316     Cond. Expr.:      362
Allow:            107834   Neverallow:        0
Auditallow:       158     Dontaudit:         10022
Type_trans:       18153   Type_change:       74
Type_member:      35      Role_allow:        37
Role_trans:       414     Range_trans:       5899
Constraints:      143     Validatetrans:     0
Initial SIDs:     27      Fs_use:            32
Genfscon:         103     Portcon:           614
Netifcon:         0       Nodecon:            0
Permissives:      0       Polcap:             5
```

Figure 3.3: seinfo

3.4 Шаг 4

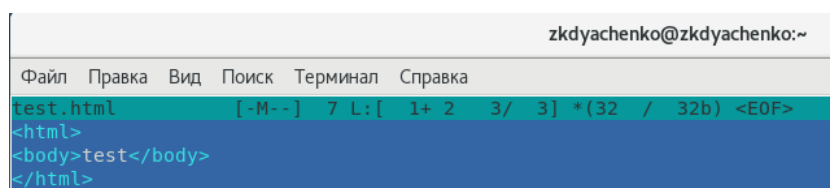
Определите тип файлов и поддиректорий, находящихся в директории /var/www - там находятся только две поддиректории (рис. 3.4). Директория /var/www/html пуста. Создавать файлы в директории /var/www/html может только владелец директории - root.

```
[zkdyachenko@zkdyachenko ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[zkdyachenko@zkdyachenko ~]$ ls -lZ /var/www/html
```

Figure 3.4: Информация о поддиректориях /var/www

3.5 Шаг 5

Создала от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис. 3.5).


A screenshot of a file editor window. The title bar shows the username 'zkdyachenko@zkdyachenko:~'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The main text area shows the content of a file named 'test.html'. The first line is a metadata line: 'test.html [-M--] 7 L:[1+ 2 3/ 3] *(32 / 32b) <EOF>'. The second line is '<html>'. The third line is '<body>test</body>'. The fourth line is '</html>'.

```
zkdyachenko@zkdyachenko:~
Файл  Правка  Вид  Поиск  Терминал  Справка
test.html  [-M--] 7 L:[ 1+ 2 3/ 3] *(32 / 32b) <EOF>
<html>
<body>test</body>
</html>
```

Figure 3.5: Содержание файла test.html

3.6 Шаг 6

Проверила контекст созданного файла. По умолчанию это `unconfined_u:object_r:httpd_sys_content` (рис. 3.6).

A screenshot of a terminal window. The prompt is '[zkdyachenko@zkdyachenko ~]\$. The command entered is 'ls -lZ /var/www/html'. The output shows the file 'test.html' with permissions '-rw-r--r--', owner 'root', group 'root', and context 'unconfined_u:object_r:httpd_sys_content_t:s0'.

```
[zkdyachenko@zkdyachenko ~]$ ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

Figure 3.6: Контекст файла

3.7 Шаг 7

Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Файл был успешно отображён (рис. 3.7).

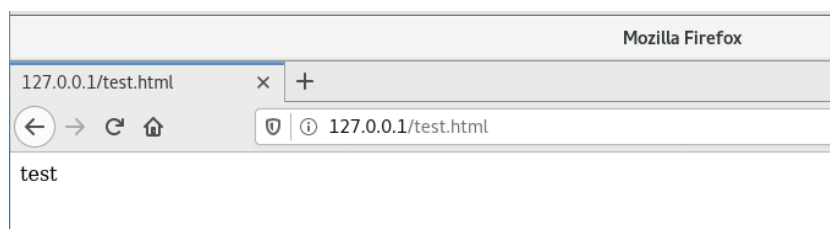


Figure 3.7: Отображение файла

3.8 Шаг 8

Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd` (рис. 3.8). Так как по умолчанию пользователи CentOS являются

свободными от типа, созданному файлу test.html был сопоставлен SELinux, пользователь unconfined_u. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. Тип httpd_sys_content_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа возможно получить доступ к файлу при обращении к нему через браузер.

```

httpd_selinux(8)                                SELinux Policy httpd                                httpd_selinux(8)

NAME
    httpd_selinux - Security Enhanced Linux Policy for the httpd processes

DESCRIPTION
    Security-Enhanced Linux secures the httpd processes via flexible mandatory access control.

    The httpd processes execute with the httpd_t SELinux type. You can check if you have these processes
    running by executing the ps command with the -Z qualifier.

    For example:

    ps -eZ | grep httpd_t

ENTRYPOINTS
    The httpd_t SELinux type can be entered via the httpd_exec_t file type.

    The default entrypoint paths for the httpd_t domain are the following:

    /usr/sbin/httpd(.worker)?, /usr/sbin/apache(2)?, /usr/lib/apache-ssl/., /usr/sbin/apache-ssl(2)?,
    /usr/share/jetty/bin/jetty.sh, /usr/sbin/nginx, /usr/sbin/thttpd, /usr/sbin/php-fpm, /usr/sbin/cherokee,
    /usr/sbin/lighttpd, /usr/sbin/httpd.event, /usr/bin/mongrel_rails, /usr/sbin/htcacheclean

PROCESS TYPES
    SELinux defines process types (domains) for each process running on the system

    You can see the context of a process using the -Z option to ps

    Policy governs the access confined processes have to files. SELinux httpd policy is very flexible
    allowing users to setup their httpd processes in as secure a method as possible.

    The following process types are defined for httpd:

    httpd_t, httpd_helper_t, httpd_php_t, httpd_rotatelog_t, httpd_suexec_t, httpd_sys_script_t, httpd_user_s
    cript_t, httpd_passwd_t, httpd_unconfined_script_t

    Note: semanage permissive -a httpd_t can be used to make the process type httpd_t permissive. SELinux
    does not deny access to permissive process types, but the AVC (SELinux denials) messages are still gen-
    erated.

Manual page httpd_selinux(8) line 1 (press h for help or q to quit)

```

Figure 3.8: Справка man httpd_selinux

3.9 Шаг 9

Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t, к которому процесс httpd не имеет доступа. После этого проверила, что контекст поменялся (рис. 3.9).

```
[zkdyachenko@zkdyachenko ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для zkdyachenko:
[zkdyachenko@zkdyachenko ~]$ ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[zkdyachenko@zkdyachenko ~]$
```

Figure 3.9: Изменение контекста файла

3.10 Шаг 10

Попробовала ещё раз получить доступ к файлу через веб-сервер, но получила сообщение об ошибке (рис. 3.10).



Figure 3.10: Ошибка

3.11 Шаг 11

Просмотрела лог-файл `tail /var/log/messages` (рис. 3.11) и `/var/log/audit/audit.log` (рис. 3.12).

```
[zkdyachenko@zkdyachenko ~]$ sudo tail /var/log/messages
Nov 24 14:36:57 zkdyachenko dbus[694]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Nov 24 14:36:59 zkdyachenko dbus[694]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Nov 24 14:37:01 zkdyachenko setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Nov 24 14:37:01 zkdyachenko setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For complet
e SELinux messages run: sealert -l a7e56dbc-648a-41d8-b38a-cfd641e5917f
Nov 24 14:37:01 zkdyachenko python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html.#012#012***** Plugi
n restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default
label should be httpd.sys.content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permission
s to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/t
est.html#012#012***** Plugin public content (7.83 confidence) suggests *****#012#012If you want to treat test.html as publ
ic content#012Then you need to change the label on test.html to public.content.t or public.content.rw.t.#012Do#012# semanage fcontext -a -t
public.content.t /var/www/html/test.html.#012# restorecon -v /var/www/html/test.html.#012#012***** Plugin catchall (1.41 confidence) sugg
ests *****#012#012If you believe that httpd should be allowed getatrr access on the test.html file by default.#012The
n you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by exe
cuting:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Nov 24 14:37:16 zkdyachenko setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For complet
e SELinux messages run: sealert -l a7e56dbc-648a-41d8-b38a-cfd641e5917f
Nov 24 14:37:16 zkdyachenko python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html.#012#012***** Plugi
n restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default
label should be httpd.sys.content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permission
s to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/t
est.html#012#012***** Plugin public content (7.83 confidence) suggests *****#012#012If you want to treat test.html as publ
ic content#012Then you need to change the label on test.html to public.content.t or public.content.rw.t.#012Do#012# semanage fcontext -a -t
public.content.t /var/www/html/test.html.#012# restorecon -v /var/www/html/test.html.#012#012***** Plugin catchall (1.41 confidence) sugg
ests *****#012#012If you believe that httpd should be allowed getatrr access on the test.html file by default.#012The
n you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by exe
cuting:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
[zkdyachenko@zkdyachenko ~]$
```

Figure 3.11: Файл /var/log/messages

```
zkdyachenko@zkdyachenko:~
Файл Правка Ввод Поиск Терминал Справка
type=USER_END msg=audit(1637754061.851:545): pid=11544 uid=0 auid=0 ses=17 subj=system_u:system_r:crond:t:s0-s0:c0.c1023 msg=op=PAM:session
close grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=/dev/pts/0 res=succ
s'
type=USER_ACCT msg=audit(1637754066.156:546): pid=11631 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg=op=PAM:accounting grantors=pam_unix,pam_localuser acct="zkdyachenko" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succ
ess'
type=USER_CMD msg=audit(1637754066.156:547): pid=11631 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 m
sg=cwd="/home/zkdyachenko" cmd=636174202f7661722f6c6f672f61756469742f61756469742e6c6f67 terminal=pts/0 res=success'
type=CRED_REFR msg=audit(1637754066.156:548): pid=11631 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
type=USER_START msg=audit(1637754066.172:549): pid=11631 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:session open grantors=pam_keyinit,pam_keyinit,pam_limits,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? te
rминал=/dev/pts/0 res=success'
[zkdyachenko@zkdyachenko ~]$ sudo tail /var/log/audit/audit.log
type=USER_ACCT msg=audit(1637754066.156:546): pid=11631 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg=op=PAM:accounting grantors=pam_unix,pam_localuser acct="zkdyachenko" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succ
ess'
type=USER_CMD msg=audit(1637754066.156:547): pid=11631 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 m
sg=cwd="/home/zkdyachenko" cmd=636174202f7661722f6c6f672f61756469742f61756469742e6c6f67 terminal=pts/0 res=success'
type=CRED_REFR msg=audit(1637754066.156:548): pid=11631 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
type=USER_START msg=audit(1637754066.172:549): pid=11631 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:session open grantors=pam_keyinit,pam_keyinit,pam_limits,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? te
rминал=/dev/pts/0 res=success'
type=USER_END msg=audit(1637754066.719:550): pid=11631 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:session close grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? te
rминал=/dev/pts/0 res=success'
type=CRED_DTSP msg=audit(1637754066.719:551): pid=11631 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
type=USER_ACCT msg=audit(1637754113.420:552): pid=11687 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg=op=PAM:accounting grantors=pam_unix,pam_localuser acct="zkdyachenko" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=succ
ess'
type=USER_CMD msg=audit(1637754113.420:553): pid=11687 uid=1000 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 m
sg=cwd="/home/zkdyachenko" cmd=7461696c202f7661722f6c6f672f61756469742f61756469742e6c6f67 terminal=pts/0 res=success'
type=CRED_REFR msg=audit(1637754113.420:554): pid=11687 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
type=USER_START msg=audit(1637754113.420:555): pid=11687 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:session open grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? te
rминал=/dev/pts/0 res=success'
type=USER_END msg=audit(1637754113.420:556): pid=11687 uid=0 auid=1000 ses=2 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 ms
g=op=PAM:session close grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? te
rминал=/dev/pts/0 res=success'
```

Figure 3.12: Файл /var/log/audit/audit.log

3.12 Шаг 12

Попробую запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81 (рис. 3.13).

```
#
# 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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
```

1Помощь2Сохранить3Блок4Замена5Копия

Figure 3.13: Замена строки в файле

3.13 Шаг 13

Выполнила перезапуск веб-сервера Apache. Сбоя не произошло (рис. 3.14). Следуя указаниям к лабораторной, посмотрела файлы `tail -nl /var/log/messages`, `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` (рис. 3.15)

```
[zkdyachenko@zkdyachenko ~]$ sudo mcedit /etc/httpd/conf/httpd.conf

[zkdyachenko@zkdyachenko ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[zkdyachenko@zkdyachenko ~]$ █
```

Figure 3.14: Перезапуск веб-сервера Apache

```
[zkdyachenko@zkdyachenko ~]$ sudo tail -n 10 /var/log/messages
Nov 24 14:40:01 zkdyachenko systemd: Created slice User Slice of root.
Nov 24 14:40:01 zkdyachenko systemd: Started Session 17 of user root.
Nov 24 14:40:01 zkdyachenko systemd: Removed slice User Slice of root.
Nov 24 14:47:46 zkdyachenko systemd: Stopping The Apache HTTP Server...
Nov 24 14:47:48 zkdyachenko systemd: Stopped The Apache HTTP Server.
Nov 24 14:47:48 zkdyachenko systemd: Starting The Apache HTTP Server...
Nov 24 14:47:48 zkdyachenko systemd: Started The Apache HTTP Server.
Nov 24 14:50:01 zkdyachenko systemd: Created slice User Slice of root.
Nov 24 14:50:01 zkdyachenko systemd: Started Session 18 of user root.
Nov 24 14:50:02 zkdyachenko systemd: Removed slice User Slice of root.
[zkdyachenko@zkdyachenko ~]$ sudo tail -n 10 /var/log/httpd/error_log
[Wed Nov 24 13:18:26.425178 2021] [lbmethod:heartbeat:notice] [pid 4381] AH02282: No slotmem from mod_heartbeat
[Wed Nov 24 13:18:26.427686 2021] [mpm_prefork:notice] [pid 4381] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Wed Nov 24 13:18:26.427727 2021] [core:notice] [pid 4381] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Wed Nov 24 14:36:54.790709 2021] [core:error] [pid 4388] (13)Permission denied: [client 127.0.0.1:60908] 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 Nov 24 14:47:46.957198 2021] [mpm_prefork:notice] [pid 4381] AH00170: caught SIGINCH, shutting down gracefully
[Wed Nov 24 14:47:48.096783 2021] [core:notice] [pid 12091] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Wed Nov 24 14:47:48.098969 2021] [suexec:notice] [pid 12091] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Nov 24 14:47:48.114808 2021] [lbmethod:heartbeat:notice] [pid 12091] AH02282: No slotmem from mod_heartbeat
[Wed Nov 24 14:47:48.116822 2021] [mpm_prefork:notice] [pid 12091] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Wed Nov 24 14:47:48.116861 2021] [core:notice] [pid 12091] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[zkdyachenko@zkdyachenko ~]$ sudo tail -n 10 /var/log/httpd/access_log
127.0.0.1 - - [24/Nov/2021:13:45:11 +0300] "GET /test.html HTTP/1.1" 200 32 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [24/Nov/2021:13:45:12 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [24/Nov/2021:14:36:54 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Figure 3.15: Просмотр файлов

3.14 Шаг 14

Выполнила команду `semanage port -a -t http_port_t -p tcp 81`, после этого проверила список портов. Порт 81 есть в списке (рис. 3.16).

```
[zkdyachenko@zkdyachenko ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[zkdyachenko@zkdyachenko ~]$ 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
[zkdyachenko@zkdyachenko ~]$
```

Figure 3.16: Список портов

3.15 Шаг 15

Попробовала запустить веб-сервер Apache ещё раз. Он запустился (рис. 3.17).

```
[zkdyachenko@zkdyachenko ~]$ 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
[zkdyachenko@zkdyachenko ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[zkdyachenko@zkdyachenko ~]$ 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; vendor preset: disabled)
   Active: active (running) since Cp 2021-11-24 14:55:26 MSK; 17s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 12664 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 12672 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           └─12672 /usr/sbin/httpd -DFOREGROUND
             └─12673 /usr/sbin/httpd -DFOREGROUND
               └─12674 /usr/sbin/httpd -DFOREGROUND
                 └─12675 /usr/sbin/httpd -DFOREGROUND
                   └─12676 /usr/sbin/httpd -DFOREGROUND
                     └─12677 /usr/sbin/httpd -DFOREGROUND

ноя 24 14:55:26 zkdyachenko.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 24 14:55:26 zkdyachenko.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 24 14:55:26 zkdyachenko.localdomain systemd[1]: Started The Apache HTTP Server.
```

Figure 3.17: Перезапуск веб-сервера Apache

3.16 Шаг 16

Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. После этого попробовала получить доступ к файлу через веб-сервер и увидела содержимое файла — слово «test». (рис. 3.18)

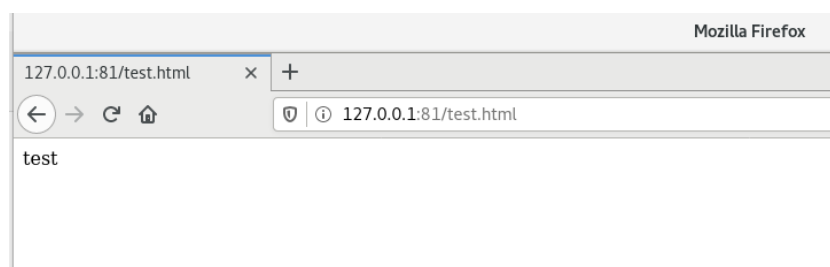


Figure 3.18: Получение доступа к файлу через веб-браузер

3.17 Шаг 17

Исправила обратно конфигурационный файл apache, вернув Listen 80 (рис. 3.19).

```
#  
# 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 specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
#  
#Listen 12.34.56.78:80  
Listen 80
```

Figure 3.19: Исправление файла

3.18 Шаг 18

Попыталась удалить привязку http_port_t к 81 порту, но сделать это не удалось. Затем удалила файл /var/www/html/test.html (рис. 3.20).

```
[zkdyachenko@zkdyachenko ~]$ sudo semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален  
[zkdyachenko@zkdyachenko ~]$ sudo rm /var/www/html/test.html  
[zkdyachenko@zkdyachenko ~]$ sudo ls /var/www/html  
[zkdyachenko@zkdyachenko ~]$
```

Figure 3.20: Попытка удалить привязку http_port_t к 81 порту и удаление файла

4 Выводы

В результате работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux. Также я проверила работу SELinux на практике совместно с веб-сервером Apache. Результаты работы находятся в репозитории на GitHub, а также есть скринкаст выполнения лабораторной работы.