

Отчет по лабораторной работе №6

Информационная безопасность

Астафьева Анна Андреевна НПИбд-01-18

Содержание

1	Цель работы	4
2	Теоретическое описание	5
3	Подготовка лабораторного стенда:	6
4	Выполнение лабораторной работы	8
5	Выводы	20

List of Figures

3.1	Параметр ServerName	6
3.2	Отключение фильтра	7
3.3	Добавление разрешающих правил	7
4.1	Проверка	8
4.2	Обращение через браузер	9
4.3	Проверка	9
4.4	веб-сервер Apache	10
4.5	Просмотр состояние переключателей SELinux для Apache	11
4.6	Получение информации	12
4.7	Получение информации	12
4.8	Создание файла	13
4.9	Проверка	13
4.10	Получение доступа к файлу через браузер	14
4.11	Получение доступа к файлу через браузер	14
4.12	Просмотр системного лог-файла	15
4.13	Просмотр системного лог-файла	15
4.14	Изменение порта 80 на 81	16
4.15	Анализ лог-файла	16
4.16	Анализ файла	17
4.17	Анализ файла	17
4.18	Выполнение и проверка	17
4.19	Возвращение контекста	18
4.20	Получение доступа к файлу через браузер	18
4.21	Исправление конфигурационного файл apache	18
4.22	Удаление привязки http_port_t к 81 порту	19
4.23	Удаление файла /var/www/html/test.html	19

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 Теоретическое описание

SELinux — набор технологий расширения системы безопасности Linux. Сегодня основу набора составляют три технологии: мандатный контроль доступа, ролевой доступ RBAC и система типов (доменов). Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

3 Подготовка лабораторного стенда:

1. В конфигурационном файле `/etc/httpd/httpd.conf` задала параметр `ServerName`. (рис. 3.1).

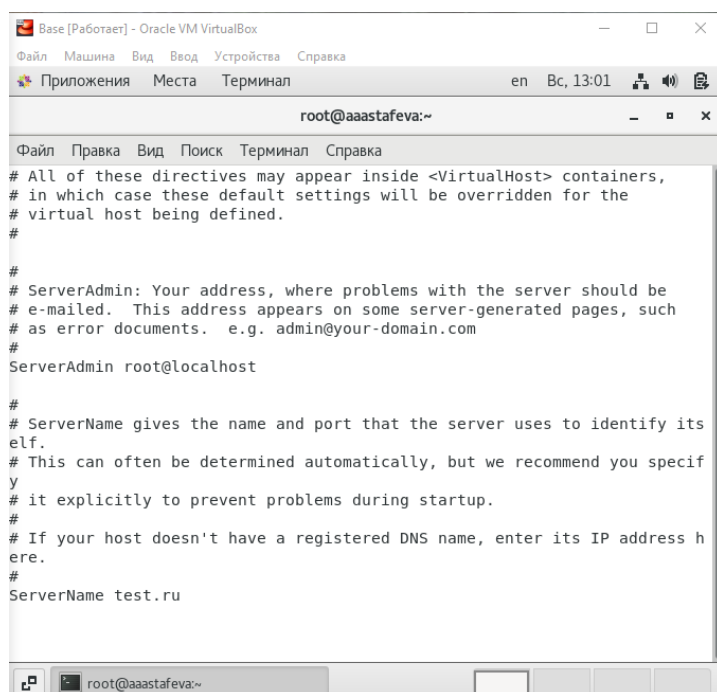


Figure 3.1: Параметр `ServerName`

2. Также проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола `tcp`. Отключила фильтр командами: `iptables -F`, `iptables -P INPUT ACCEPT`, `iptables -P OUTPUT ACCEPT`. Так же добавила разрешающие правила. (рис. 3.2), (рис. 3.3).

```
[root@aaastafeva ~]# iptables -F  
[root@aaastafeva ~]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
```

Figure 3.2: Отключение фильтра

```
[root@aaastafeva ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
[root@aaastafeva ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
[root@aaastafeva ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
[root@aaastafeva ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT  
[root@aaastafeva ~]#
```

Figure 3.3: Добавление разрешающих правил

4 Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 4.1).

```
[root@aaaastafeva ~]# getenforce
Enforcing
[root@aaaastafeva ~]# 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
Max kernel policy version:     31
[root@aaaastafeva ~]#
```

Figure 4.1: Проверка

2. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: `service httpd status` (рис. 4.2), (рис. 4.3).

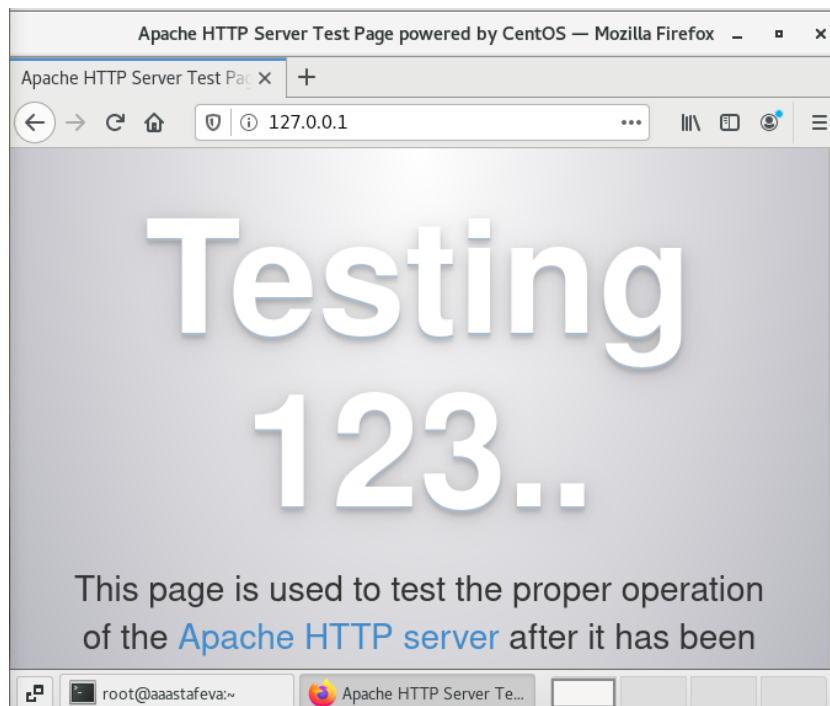


Figure 4.2: Обращение через браузер

```
[root@aaastafeva ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@aaastafeva ~]# 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 Бс 2021-11-21 13:18:24 MSK; 2s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 4100 (httpd)
    Status: "Processing requests..."
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─4100 /usr/sbin/httpd -DFOREGROUND
              4105 /usr/sbin/httpd -DFOREGROUND
              4106 /usr/sbin/httpd -DFOREGROUND
              4107 /usr/sbin/httpd -DFOREGROUND
              4109 /usr/sbin/httpd -DFOREGROUND
              4110 /usr/sbin/httpd -DFOREGROUND

ноя 21 13:18:20 aaastafeva.localdomain systemd[1]: Starting The Apa...
ноя 21 13:18:24 aaastafeva.localdomain systemd[1]: Started The Apac...
Hint: Some lines were ellipsized, use -l to show in full.
[root@aaastafeva ~]#
```

Figure 4.3: Проверка

3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (рис. 4.4).

```
root@aaastafeva:~  
Файл Правка Вид Поиск Терминал Справка  
ноя 21 13:18:20 aaastafeva.localdomain systemd[1]: Starting The Apa...  
ноя 21 13:18:24 aaastafeva.localdomain systemd[1]: Started The Apac...  
Hint: Some lines were ellipsized, use -l to show in full.  
[root@aaastafeva ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 4100 0.2 0.4 224084 4904 ?  
Ss 13:18 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4105 0.0 0.3 226304 3724 ?  
S 13:18 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4106 0.0 0.3 226304 3752 ?  
S 13:18 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4107 0.0 0.3 226304 3752 ?  
S 13:18 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4109 0.0 0.2 226168 3016 ?  
S 13:18 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4110 0.0 0.2 226168 3016 ?  
S 13:18 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4184 0.0 0.3 226168 3096 ?  
S 13:19 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4186 0.0 0.3 226168 3096 ?  
S 13:19 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 4187 0.0 0.3 226168 3096 ?  
S 13:19 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4199 0.0 0.0  
112832 972 pts/0 R+ 13:19 0:00 grep --color=auto httpd  
[root@aaastafeva ~]#
```

Figure 4.4: веб-сервер Apache

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратила внимание, что многие из них находятся в положении «off». (рис. 4.5).

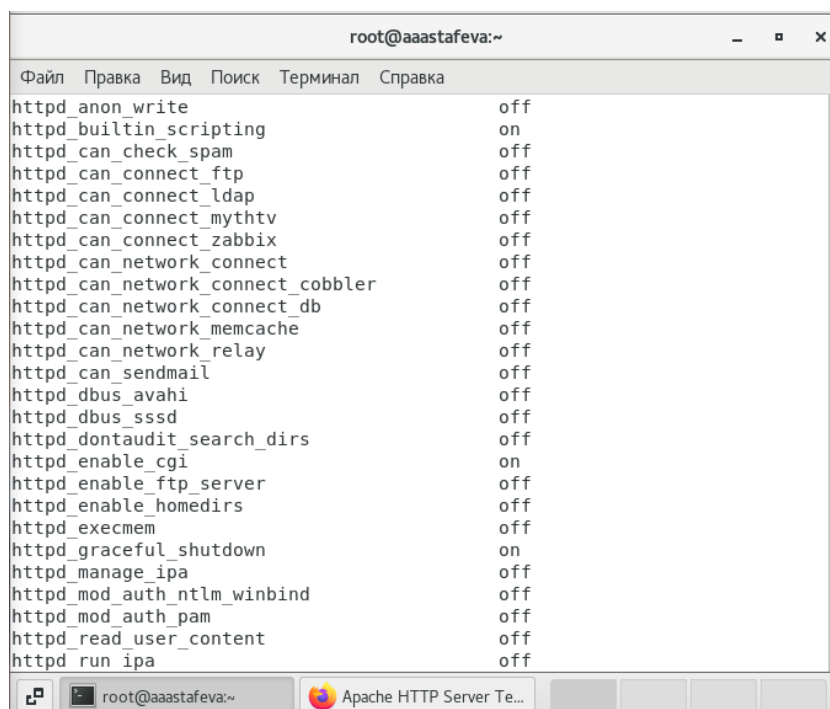


Figure 4.5: Просмотр состояние переключателей SELinux для Apache

5. Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей(8), ролей(14), типов(4793). Определила тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды: `ls -lZ /var/www`. Определила тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. Определила круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. (рис. 4.6), (рис. 4.7).

```
[root@aaaastafeva ~]# 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

[root@aaaastafeva ~]#
```

Figure 4.6: Получение информации

```
[root@aaaastafeva ~]# 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
[root@aaaastafeva ~]# ls -lZ /var/www/html
[root@aaaastafeva ~]# ls /var/www/html
```

Figure 4.7: Получение информации

6. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 4.8).

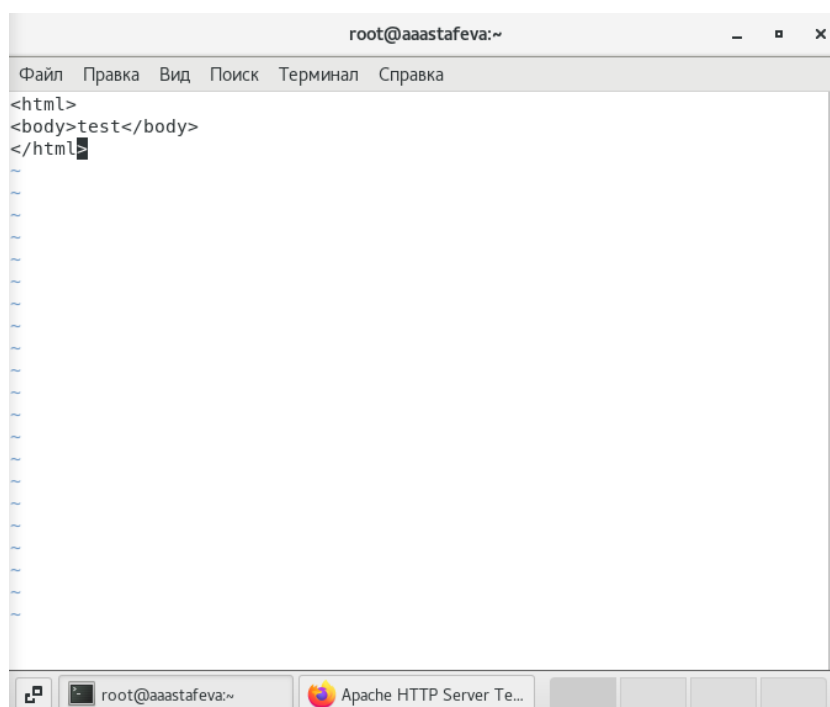


Figure 4.8: Создание файла

7. Проверила контекст созданного файла. `httpd_sys_content_t` (рис. 4.9).

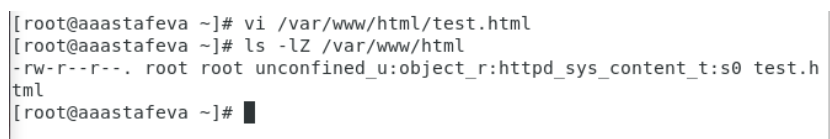


Figure 4.9: Проверка

8. Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедилась, что файл был успешно отображён. (рис. 4.10).

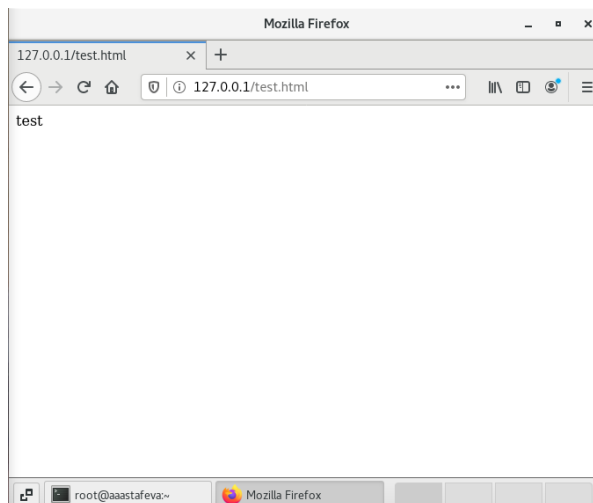


Figure 4.10: Получение доступа к файлу через браузер

9. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверила, что контекст поменялся. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получили сообщение об ошибке. (рис. 4.11).

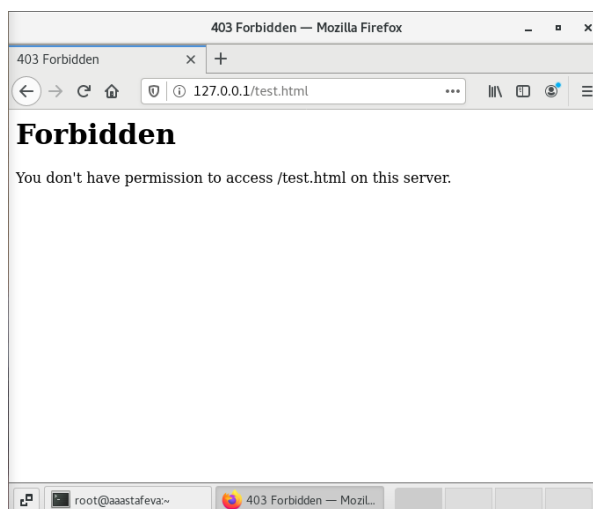
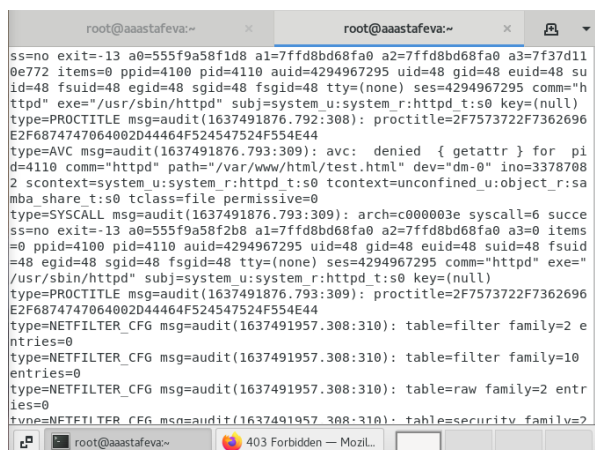


Figure 4.11: Получение доступа к файлу через браузер

12. Проанализировала ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также

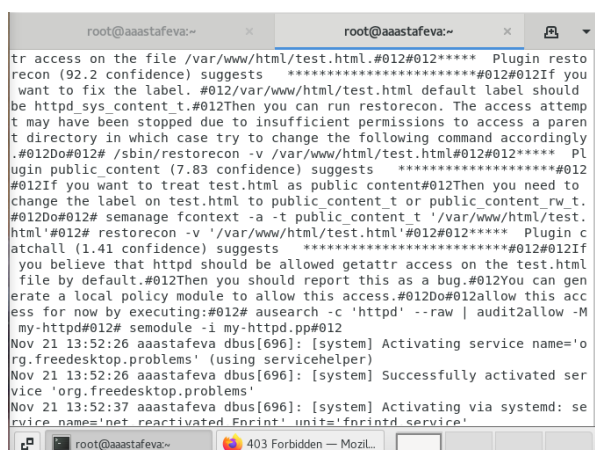
просмотрела системный лог-файл: tail /var/log/messages (рис. 4.12), (рис. 4.13).



```
root@aaastafeva:~  
ss=no exit=-13 a0=555f9a58f1d8 a1=7ffd8bd68fa0 a2=7ffd8bd68fa0 a3=7f37d11  
0e772 items=0 ppid=4100 pid=4110 auid=4294967295 uid=48 gid=48 euid=48 su  
id=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="h  
ttpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)  
type=PROCTITLE msg=audit(1637491876.792:308): proctitle=2F7573722F7362696  
E2F6874747064002D44464F524547524F554E44  
type=AVC msg=audit(1637491876.793:309): avc: denied { getattr } for pi  
d=4110 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=3378708  
2 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:sa  
mba_share_t:s0 tclass=file permissive=0  
type=SYSCALL msg=audit(1637491876.793:309): arch=c000003e syscall=6 succe  
ss=no exit=-13 a0=555f9a58f2b8 a1=7ffd8bd68fa0 a2=7ffd8bd68fa0 a3=0 items  
=0 ppid=4100 pid=4110 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid  
=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="<div data-bbox="285 366 710 384" data-label="Caption">

Figure 4.12: Просмотр системного лог-файла

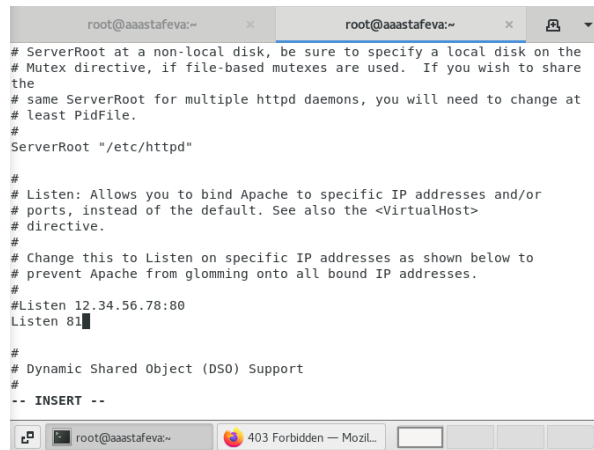

```



```
root@aaastafeva:~  
tr access on the file /var/www/html/test.html.#012#012**** Plugin resto  
recon (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  
t may have been stopped due to insufficient permissions to access a paren  
t directory in which case try to change the following command accordingly  
.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Pl  
ugin public_content (7.83 confidence) suggests *****#012#012If  
you want to treat test.html as public 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 c  
atchall (1.41 confidence) suggests *****#012#012If  
you believe that httpd should be allowed getattr access on the test.html  
file by default.#012Then you should report this as a bug.#012You can gen  
erate a local policy module to allow this access.#012Do#012allow this acc  
ess for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M  
my-httpd#012# semodule -i my-httpd.pp#012  
Nov 21 13:52:26 aaastafeva dbus[696]: [system] Activating service name='o  
rg.freedesktop.problems' (using servicehelper)  
Nov 21 13:52:26 aaastafeva dbus[696]: [system] Successfully activated ser  
vice 'org.freedesktop.problems'  
Nov 21 13:52:37 aaastafeva dbus[696]: [system] Activating via systemd: se  
rvice name='org.freedesktop.problems' unit='fprintd.service'
```

Figure 4.13: Просмотр системного лог-файла

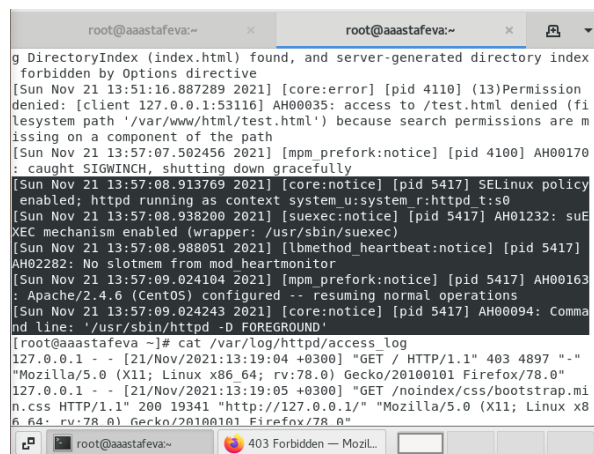
13. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81.(рис. 4.14).



```
root@aaastafeva:~  
# ServerRoot at a non-local disk, be sure to specify a local disk on the  
# Mutex directive, if file-based mutexes are used. If you wish to share  
# the  
# same ServerRoot for multiple httpd daemons, you will need to change at  
# least PidFile.  
#  
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 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  
#  
-- INSERT --
```

Figure 4.14: Изменение порта 80 на 81

14. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log. (рис. 4.15), (рис. 4.16), (рис. 4.17).



```
root@aaastafeva:~  
g DirectoryIndex (index.html) found, and server-generated directory index  
forbidden by Options directive  
[Sun Nov 21 13:51:16.887289 2021] [core:error] [pid 4110] (13)Permission  
denied: [client 127.0.0.1:53116] AH00035: access to /test.html denied (fi  
lesystem path '/var/www/html/test.html') because search permissions are m  
issing on a component of the path  
[Sun Nov 21 13:57:07.502456 2021] [mpm_prefork:notice] [pid 4100] AH00170  
: caught SIGWINCH, shutting down gracefully  
[Sun Nov 21 13:57:08.913769 2021] [core:notice] [pid 5417] SELinux policy  
enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Sun Nov 21 13:57:08.938200 2021] [suexec:notice] [pid 5417] AH01232: suE  
XEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Sun Nov 21 13:57:08.988051 2021] [lbmethod_heartbeat:notice] [pid 5417]  
AH02282: No slotmem from mod_heartbeat  
[Sun Nov 21 13:57:09.024104 2021] [mpm_prefork:notice] [pid 5417] AH00163  
: Apache/2.4.6 (CentOS) configured -- resuming normal operations  
[Sun Nov 21 13:57:09.024243 2021] [core:notice] [pid 5417] AH00094: Comma  
nd line: '/usr/sbin/httpd -D FOREGROUND'  
[root@aaastafeva ~]# cat /var/log/httpd/access_log  
127.0.0.1 - - [21/Nov/2021:13:19:04 +0300] "GET / HTTP/1.1" 403 4897 "-"  
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"  
127.0.0.1 - - [21/Nov/2021:13:19:05 +0300] "GET /noindex/css/bootstrap.mi  
n.css HTTP/1.1" 200 19341 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x8  
6_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Figure 4.15: Анализ лог-файла


```

root@aaastafeva:~
vice 'org.freedesktop.problems'
Nov 21 13:52:37 aaastafeva dbus[696]: [system] Activating via systemd: se
vice name='net.reactivated.Fprint' unit='fprintd.service'
Nov 21 13:52:37 aaastafeva systemd: Starting Fingerprint Authentication D
aemon...
Nov 21 13:52:37 aaastafeva dbus[696]: [system] Successfully activated ser
vice 'net.reactivated.Fprint'
Nov 21 13:52:37 aaastafeva systemd: Started Fingerprint Authentication Da
emon.
Nov 21 13:52:39 aaastafeva su: (to root) aaastafeva on pts/1
[root@aaastafeva ~]# vi /etc/httpd/conf/httpd.conf
[root@aaastafeva ~]# tail -n1 /var/log/messages
Nov 21 13:57:08 aaastafeva systemd: Started The Apache HTTP Server.
[root@aaastafeva ~]# cat /var/log/http/error_log
cat: /var/log/http/error_log: Нет такого файла или каталога
[root@aaastafeva ~]# ls /var/log/http
ls: невозможно получить доступ к /var/log/http: Нет такого файла или ката
лога
[root@aaastafeva ~]# ls /var/log/
anaconda          grubby_prune_debug  secure-20211109
audit             httpd               secure-20211121
boot.log          lastlog             speech-dispatcher
boot.log-20211016 libvirt             spooler
boot.log-20211109 maillog             spooler-20211016

```

Figure 4.16: Анализ файла

```

root@aaastafeva:~
95 ses=4294967295 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=P
AM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/cron"
hostname=? addr=? terminal=cron res=success'
type=LOGIN msg=audit(1637492461.702:328): pid=5498 uid=0 subj=system u:sy
stem r:cron t:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-s
es=4294967295 ses=13 res=1
type=USER_START msg=audit(1637492461.758:329): pid=5498 uid=0 auid=0 ses=
13 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe
="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
type=CRED_REFR msg=audit(1637492461.760:330): pid=5498 uid=0 auid=0 ses=1
3 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=PAM:setcred grant
ors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/cron" hostname=? addr
=? terminal=cron res=success'
type=CRED_DISP msg=audit(1637492462.201:331): pid=5498 uid=0 auid=0 ses=1
3 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=PAM:setcred grant
ors=pam_env,pam_fprintd acct="root" exe="/usr/sbin/cron" hostname=? addr
=? terminal=cron res=success'
type=USER_END msg=audit(1637492462.211:332): pid=5498 uid=0 auid=0 ses=13
subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=PAM:session_close
grantors=pam_loginuid,pam_keyinit,pam_limits,pam_systemd acct="root" exe
="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success'
[root@aaastafeva ~]#

```

Figure 4.17: Анализ файла

15. Выполнила команду: `semanage port -a -t http_port_t -p tcp 81`. После это-
го проверила список портов командой: `semanage port -l | grep http_port_t`.
Убедилась, что порт 81 появился в списке. (рис. 4.18).

```

[root@aaastafeva ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@aaastafeva ~]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 844
3, 9000
pegasus http_port_t      tcp      5988
[root@aaastafeva ~]#

```

Figure 4.18: Выполнение и проверка

16. Вернула 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 попро-

бовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test». (рис. 4.19), (рис. 4.20).

```
[root@aaastafeva ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@aaastafeva ~]#
```

Figure 4.19: Возвращение контекста

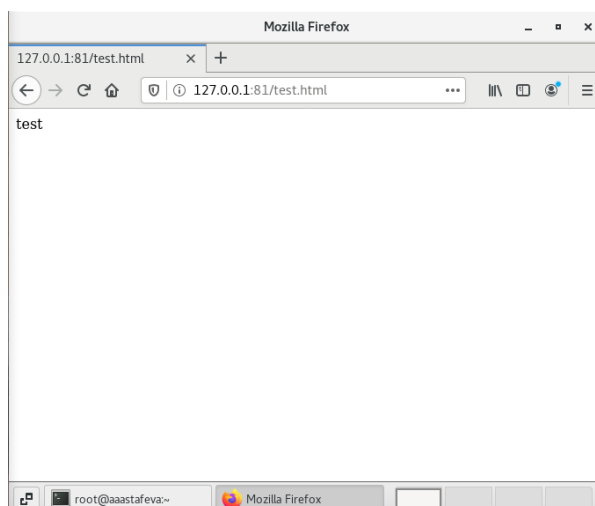


Figure 4.20: Получение доступа к файлу через браузер

17. Исправила обратно конфигурационный файл apache, вернув Listen 80. (рис. 4.21).

```
root@aaastafeva:~ root@aaastafeva:~
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share
# the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
-- INSERT --
```

Figure 4.21: Исправление конфигурационного файл apache

18. Удалила привязку http_port_t к 81 порту. (рис. 4.22).

```
[root@aaastafeva ~]# semanage port -d -t http_port_t -p tcp 81
```

Figure 4.22: Удаление привязки http_port_t к 81 порту

19. Удалила файл /var/www/html/test.html. (рис. 4.23).

```
[root@aaastafeva ~]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@aaastafeva ~]#
```

Figure 4.23: Удаление файла /var/www/html/test.html

5 Выводы

На основе проделанной работы развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.