

Отчет по лабораторной работе №6

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	18
	Список литературы	19

Список иллюстраций

2.1	Проверка статуса	6
2.2	Проверка статуса	7
2.3	Переключатели	7
2.4	Статистика по политике	8
2.5	Типы файлов и поддиректории	8
2.6	Файл	9
2.7	Контекст	9
2.8	Проверка отображения файла	10
2.9	Изменение контекста	11
2.10	Проверка отображения файла	11
2.11	Лог-файл	12
2.12	/var/log/audit/audit.log	12
2.13	Замана порта	13
2.14	Лог-файл	13
2.15	/var/log/httpd/error_log	14
2.16	/var/log/httpd/access_log	14
2.17	/var/log/audit/audit.log	15
2.18	Контекст	15
2.19	Проверка отображения файла	16
2.20	Возвращение исходной конфигурации	16
2.21	Удаление привязки к порту и файла	17

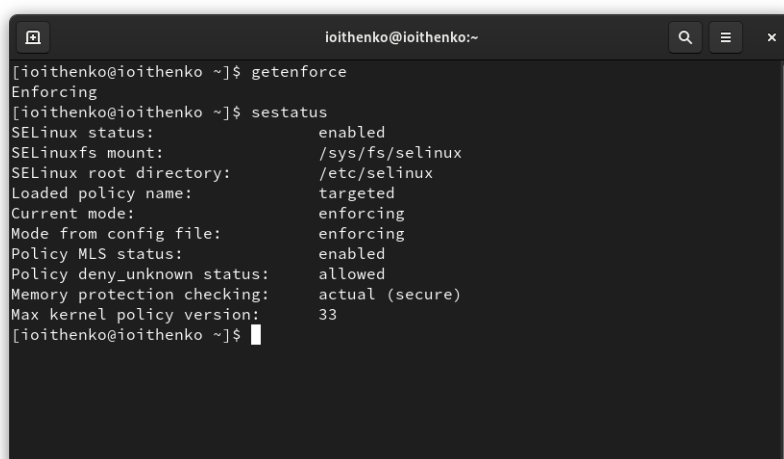
Список таблиц

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux [1]. Проверить работу SELinux на практике совместно с веб-сервером Apache.

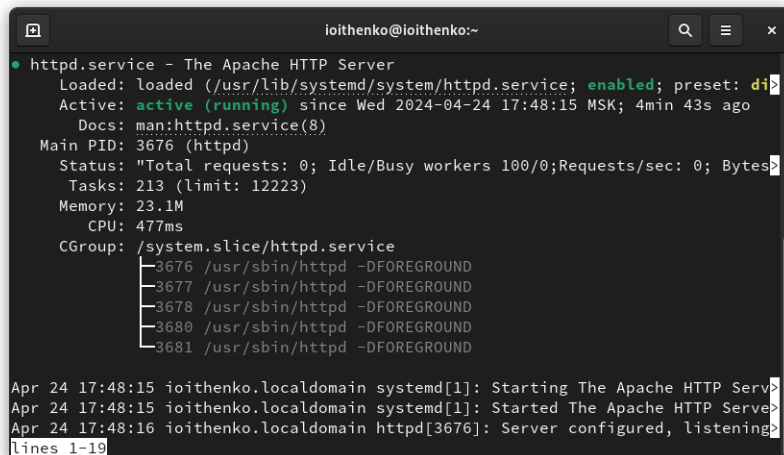
2 Выполнение лабораторной работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. Обратимся с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедимся, что последний работает (рис. 2.1) и (рис. 2.2): `service httpd status`



```
ioithenko@ioithenko:~  
[ioithenko@ioithenko ~]$ getenforce  
Enforcing  
[ioithenko@ioithenko ~]$ 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  
[ioithenko@ioithenko ~]$
```

Рис. 2.1: Проверка статуса

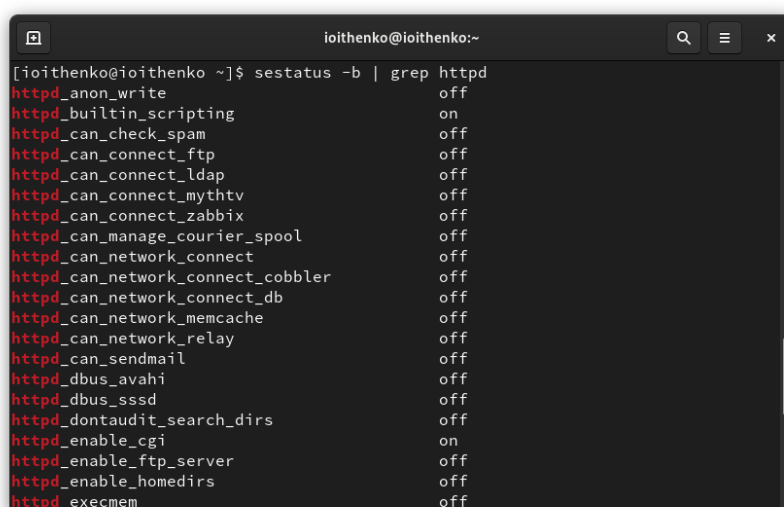


```
ioithenko@ioithenko:~  
• httpd.service - The Apache HTTP Server  
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)  
  Active: active (running) since Wed 2024-04-24 17:48:15 MSK; 4min 43s ago  
    Docs: man:httpd.service(8)  
 Main PID: 3676 (httpd)  
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0; CPU usage: 0.0%"  
  Tasks: 213 (limit: 12223)  
 Memory: 23.1M  
    CPU: 477ms  
   CGroup: /system.slice/httpd.service  
           └─3676 /usr/sbin/httpd -DFOREGROUND  
             └─3677 /usr/sbin/httpd -DFOREGROUND  
               └─3678 /usr/sbin/httpd -DFOREGROUND  
                 └─3680 /usr/sbin/httpd -DFOREGROUND  
                   └─3681 /usr/sbin/httpd -DFOREGROUND  
  
Apr 24 17:48:15 ioithenko.localdomain systemd[1]: Starting The Apache HTTP Server: OK  
Apr 24 17:48:15 ioithenko.localdomain systemd[1]: Started The Apache HTTP Server: OK  
Apr 24 17:48:16 ioithenko.localdomain httpd[3676]: Server configured, listening on: OK  
lines 1-19
```

Рис. 2.2: Проверка статуса

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности `ps auxZ | grep httpd`

Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды (рис. 2.3). `sestatus -b | grep httpd`



```
[ioithenko@ioithenko ~]$ 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_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
```

Рис. 2.3: Переключатели

Посмотрим статистику по политике с помощью команды `seinfo`, также определим множество пользователей, ролей, типов (рис. 2.4).

```
ioithenko@ioithenko:~$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:            selinux
Handle unknown classes:  allow
Classes:                  135
Sensitivities:            1
Types:                    5100
Users:                    8
Booleans:                 353
Allow:                    65009
Auditallow:               170
Type_trans:               265337
Type_member:              35
Role allow:               38
Constraints:               70
MLS Constrains:           72
Permissives:              2
Defaults:                 7
Allowxperm:               0
Permissions:              457
Categories:               1024
Attributes:               258
Roles:                    14
Cond. Expr.:              384
Neverallow:               0
Dontaudit:                8572
Type_change:              87
Range_trans:              6164
Role_trans:               420
Validatetrans:            0
MLS Val. Tran:            0
Polcap:                   6
Typebounds:               0
Neverallowxperm:          0
```

Рис. 2.4: Статистика по политике

Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды (рис. 2.5). `ls -lZ /var/www`

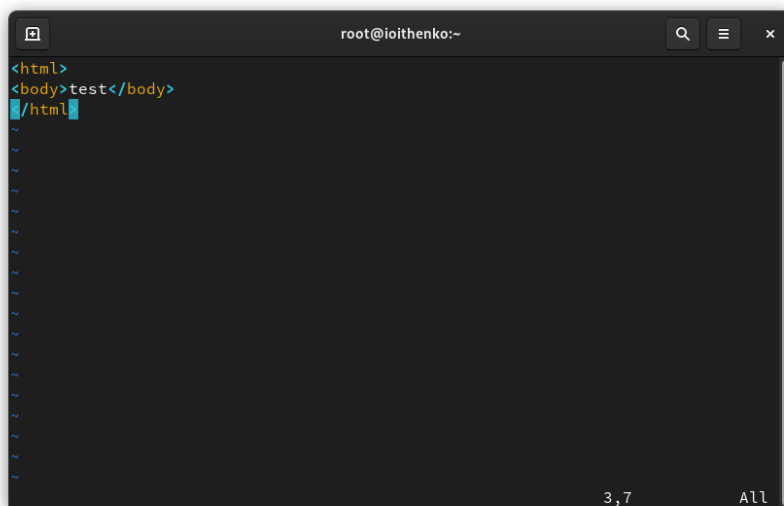
```
ioithenko@ioithenko:~$ seinfo
Allow:                    65009
Auditallow:               170
Type_trans:               265337
Type_member:              35
Role allow:               38
Constraints:               70
MLS Constrains:           72
Permissives:              2
Defaults:                 7
Allowxperm:               0
Auditallowxperm:          0
Ibendportcon:             0
Initial SIDs:             27
Genfscon:                 109
Netifcon:                  0
Neverallow:               0
Dontaudit:                8572
Type_change:              87
Range_trans:              6164
Role_trans:               420
Validatetrans:            0
MLS Val. Tran:            0
Polcap:                   6
Typebounds:               0
Neverallowxperm:          0
Dontauditxperm:           0
Ibpkeycon:                0
Fs_use:                   35
Portcon:                  660
Nodecon:                  0

ioithenko@ioithenko:~$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 1
2:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 1
2:35 html
ioithenko@ioithenko:~$
```

Рис. 2.5: Типы файлов и поддиректории

Определим тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создадим от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в ди-

ректорию) html-файл /var/www/html/test.html следующего содержания (рис. 2.6):



Проверим контекст созданного вами файла (рис. 2.7).

Обратимся к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедимся, что файл был успешно отображён (рис. 2.8).

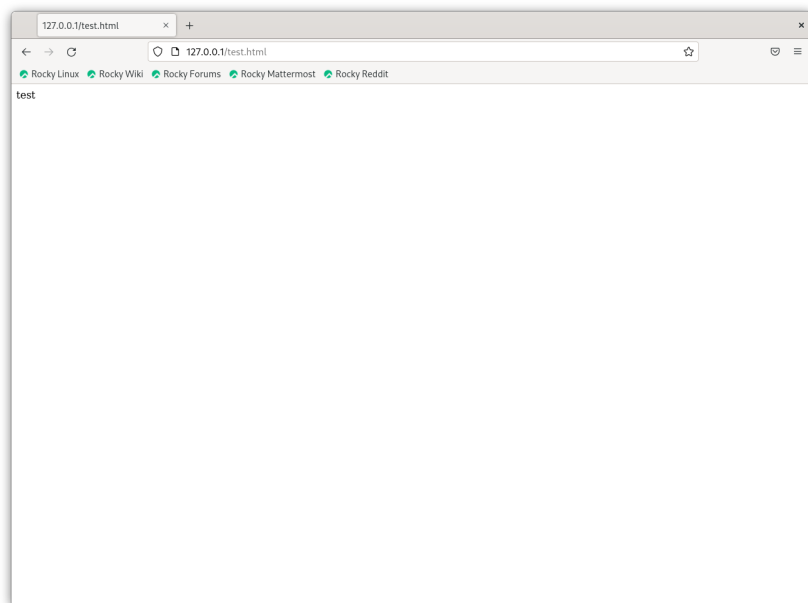
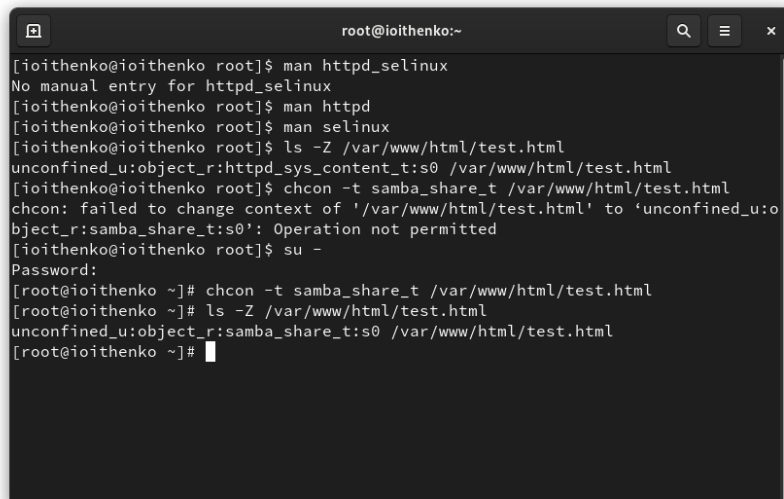


Рис. 2.8: Проверка отображения файла

Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html`. Проверим контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html` Изменим 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` (рис. 2.9): `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html`



```
root@ioithenko:~  
[ioithenko@ioithenko root]$ man httpd_selinux  
No manual entry for httpd_selinux  
[ioithenko@ioithenko root]$ man httpd  
[ioithenko@ioithenko root]$ man selinux  
[ioithenko@ioithenko root]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[ioithenko@ioithenko root]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted  
[ioithenko@ioithenko root]$ su -  
Password:  
[root@ioithenko ~]# chcon -t samba_share_t /var/www/html/test.html  
[root@ioithenko ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@ioithenko ~]#
```

Рис. 2.9: Изменение контекста

После этого проверим, что контекст поменялся. Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 2.10).

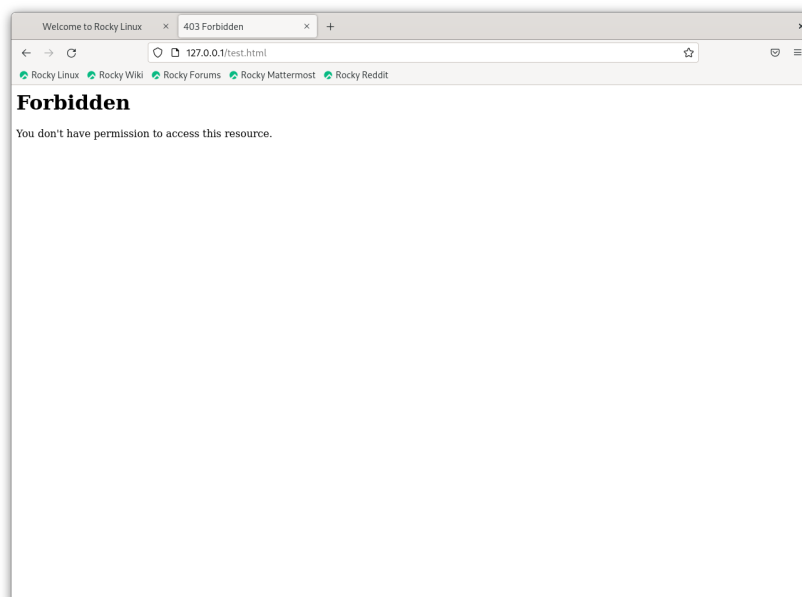


Рис. 2.10: Проверка отображения файла

`ls -l /var/www/html/test.html` Просмотрим log-файлы веб-сервера Apache. Также посмотрим системный лог-файл (рис. 2.11): `tail /var/log/messages`

```
root@ioithenko:~  
[root@ioithenko ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@ioithenko ~]# ls -l /var/www/html/test.html  
-rw-r--r--. 1 root root 33 Apr 24 17:58 /var/www/html/test.html  
[root@ioithenko ~]# tail /var/log/messages  
Apr 24 18:07:42 ioithenko setroubleshoot[5589]: SELinux is preventing /usr/sbin  
/httpd from getattr access on the file /var/www/html/test.html.#012#012***** P  
lugin restorecon (92.2 confidence) suggests *****#012#012I  
f you want to fix the label. #012/var/www/html/test.html default label should b  
e httpd_sys_content_t.#012Then you can run restorecon. The access attempt may h  
ave been stopped due to insufficient permissions to access a parent directory i  
n which case try to change the following command accordingly.#012Do#012# /sbin/  
restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83  
confidence) suggests *****#012#012If you want to treat test.h  
tml as public content#012Then you need to change the label on test.html to publ  
ic_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) suggests *****  
*****#012#012If you believe that httpd should be allowed getattr access on t  
he test.html file by default.#012Then you should report this as a bug.#012You c  
an generate 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-ht
```

Рис. 2.11: Лог-файл

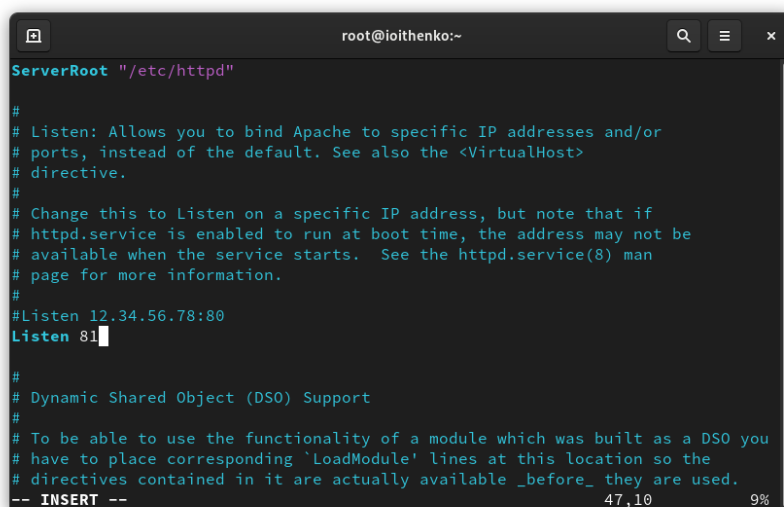
Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверим это утверждение самостоятельно (рис. 2.12).

```
root@ioithenko:~  
stem_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset"  
" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="ap  
ache" SGID="apache" FSGID="apache"  
type=PROCTITLE msg=audit(1713971256.509:301): proctitle=2F7573722F7362696E2F687  
4747064002D44464F524547524F554E44  
type=SERVICE_START msg=audit(1713971258.456:302): pid=1 uid=0 auid=4294967295 s  
es=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="s  
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=succes  
s'UID="root" AUID="unset"  
type=SERVICE_START msg=audit(1713971259.756:303): pid=1 uid=0 auid=4294967295 s  
es=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedorapro  
ject.SetroubleshootPrivileged@1 comm="systemd" exe="/usr/lib/systemd/systemd"  
hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713971273.506:304): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedorapro  
ject.SetroubleshootPrivileged@1 comm="systemd" exe="/usr/lib/systemd/systemd" h  
ostname=? addr=? terminal=? res=success'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713971273.589:305): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="s  
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success  
'UID="root" AUID="unset"  
[root@ioithenko ~]#
```

Рис. 2.12: /var/log/audit/audit.log

Попробуем 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 заменим её на Listen 81 (рис.

2.13).

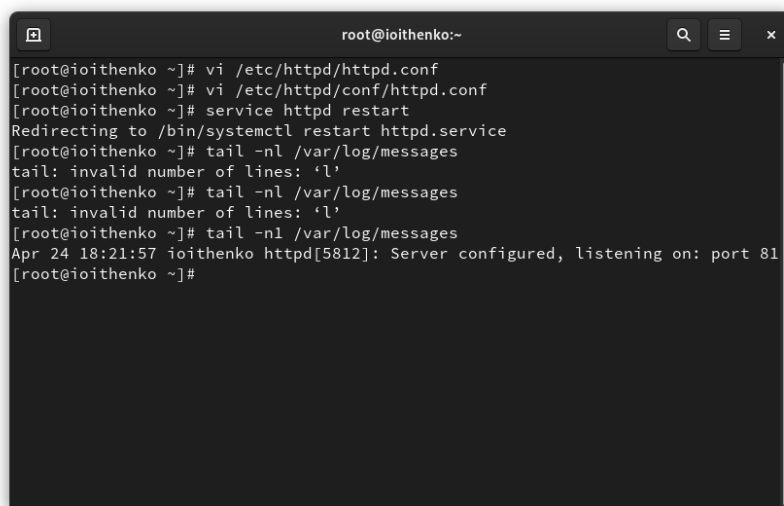


```
root@ioithenko:~  
ServerRoot "/etc/httpd"  
  
#  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default. See also the <VirtualHost>  
# directive.  
#  
# Change this to Listen on a specific IP address, but note that if  
# httpd.service is enabled 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  
  
#  
# 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.  
-- INSERT --
```

Рис. 2.13: Замана порта

Выполним перезапуск веб-сервера Apache. Сбой не произошел, так как порт существует.

Проанализируем лог-файлы (рис. 2.14): `tail -n1 /var/log/messages`



```
root@ioithenko:~  
[root@ioithenko ~]# vi /etc/httpd/httpd.conf  
[root@ioithenko ~]# vi /etc/httpd/conf/httpd.conf  
[root@ioithenko ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ioithenko ~]# tail -n1 /var/log/messages  
tail: invalid number of lines: 'l'  
[root@ioithenko ~]# tail -n1 /var/log/messages  
tail: invalid number of lines: 'l'  
[root@ioithenko ~]# tail -n1 /var/log/messages  
Apr 24 18:21:57 ioithenko httpd[5812]: Server configured, listening on: port 81  
[root@ioithenko ~]#
```

Рис. 2.14: Лог-файл

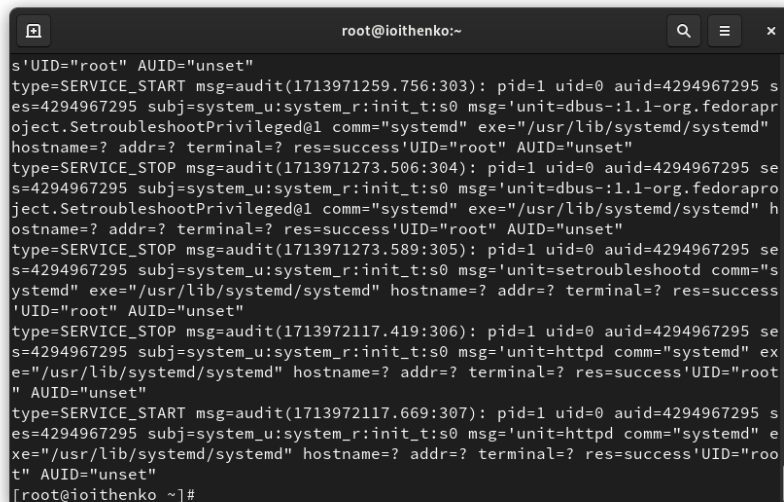
Посмотрим файлы `/var/log/http/error_log` (рис. 2.15), `/var/log/httpd/access_log` (рис. 2.16) и `/var/log/audit/audit.log` (рис. 2.17).

```
root@ioithenko:~  
[root@ioithenko ~]# cat /var/log/httpd/error.log  
cat: /var/log/httpd/error.log: No such file or directory  
[root@ioithenko ~]# cat /var/log/httpd/error_log  
[Wed Apr 24 17:48:15.773828 2024] [core:notice] [pid 3676:tid 3676] SELinux pol  
icy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Wed Apr 24 17:48:15.821740 2024] [suexec:notice] [pid 3676:tid 3676] AH01232:  
suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Wed Apr 24 17:48:15.980794 2024] [lbmethod_heartbeat:notice] [pid 3676:tid 367  
6] AH02282: No slotmem from mod_heartbeat  
[Wed Apr 24 17:48:16.032418 2024] [mpm_event:notice] [pid 3676:tid 3676] AH0048  
9: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations  
[Wed Apr 24 17:48:16.032493 2024] [core:notice] [pid 3676:tid 3676] AH00094: Co  
mmand line: '/usr/sbin/httpd -D FOREGROUND'  
[Wed Apr 24 18:06:56.557482 2024] [core:error] [pid 3681:tid 3887] (13)Permissi  
on denied: [client 127.0.0.1:41866] AH00035: access to /test.html denied (files  
ystem path '/var/www/html/test.html') because search permissions are missing on  
a component of the path  
[Wed Apr 24 18:07:36.511145 2024] [core:error] [pid 3681:tid 3890] (13)Permissi  
on denied: [client 127.0.0.1:50910] AH00035: access to /test.html denied (files  
ystem path '/var/www/html/test.html') because search permissions are missing on  
a component of the path  
[Wed Apr 24 18:21:56.329008 2024] [mpm_event:notice] [pid 3676:tid 3676] AH0049
```

Рис. 2.15: /var/log/httpd/error_log

```
root@ioithenko:~  
9: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations  
[Wed Apr 24 18:21:57.691712 2024] [core:notice] [pid 5812:tid 5812] AH00094: Co  
mmand line: '/usr/sbin/httpd -D FOREGROUND'  
[root@ioithenko ~]# cat /var/log/httpd/access_log  
127.0.0.1 - - [24/Apr/2024:18:01:29 +0300] "GET /test.html HTTP/1.1" 200 33 "-"  
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:02:08 +0300] "GET /test.html HTTP/1.1" 200 33 "-"  
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:02:12 +0300] "GET /test.html HTTP/1.1" 200 33 "-"  
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:02:22 +0300] "GET /test.html HTTP/1.1" 404 196 "  
-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:02:31 +0300] "GET /test.html HTTP/1.1" 200 33 "-"  
"Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:02:41 +0300] "GET /favicon.ico HTTP/1.1" 404 196  
"http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/2  
0100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:06:56 +0300] "GET /test.html HTTP/1.1" 403 199 "-  
" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
127.0.0.1 - - [24/Apr/2024:18:07:36 +0300] "GET /test.html HTTP/1.1" 403 199 "-  
" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"  
[root@ioithenko ~]#
```

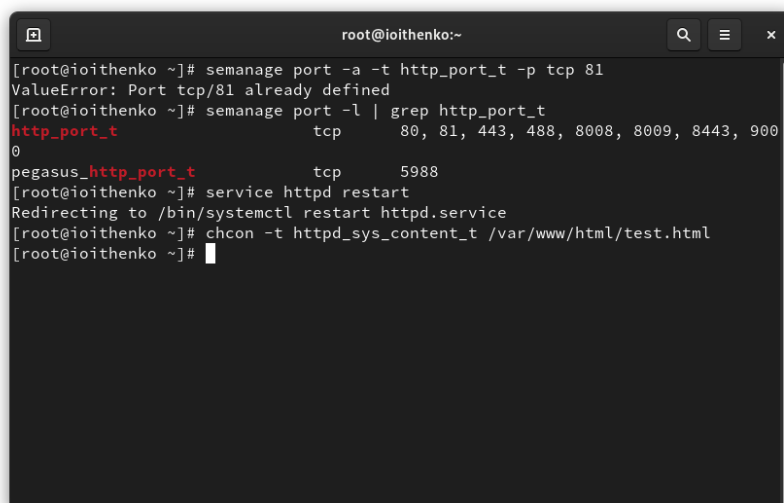
Рис. 2.16: /var/log/httpd/access_log



```
root@ioithenko:~  
s'UID="root" AUID="unset"  
type=SERVICE_START msg=audit(1713971259.756:303): pid=1 uid=0 auid=4294967295 s  
es=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedorapro  
ject.SetroubleshootPrivileged@1 comm="systemd" exe="/usr/lib/systemd/systemd" h  
ostname=? addr=? terminal=? res=success'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713971273.506:304): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dbus-:1.1-org.fedorapro  
ject.SetroubleshootPrivileged@1 comm="systemd" exe="/usr/lib/systemd/systemd" h  
ostname=? addr=? terminal=? res=success'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713971273.589:305): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=setroubleshootd comm="s  
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success  
'UID="root" AUID="unset"  
type=SERVICE_STOP msg=audit(1713972117.419:306): pid=1 uid=0 auid=4294967295 se  
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe  
="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root  
" AUID="unset"  
type=SERVICE_START msg=audit(1713972117.669:307): pid=1 uid=0 auid=4294967295 s  
es=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" e  
xe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="roo  
t" AUID="unset"  
[root@ioithenko ~]#
```

Рис. 2.17: /var/log/audit/audit.log

Выполним команду `semanage port -a -t http_port_t -p tcp 81` После этого про-
верим список портов командой `semanage port -l | grep http_port_t` Попробуем
запустить веб-сервер Apache ещё раз. Вернем контекст `httpd_sys_content_t`
к файлу `/var/www/html/ test.html` (рис. 2.18): `chcon -t httpd_sys_content_t`
`/var/www/html/test.html`



```
root@ioithenko:~  
[root@ioithenko ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[root@ioithenko ~]# semanage port -l | grep http_port_t  
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 900  
0  
pegasus_http_port_t  tcp      5988  
[root@ioithenko ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ioithenko ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@ioithenko ~]#
```

Рис. 2.18: Контекст

После этого попробуем получить доступ к файлу через веб-сервер, введя в бра-

узере адрес `http://127.0.0.1:81/test.html` (рис. 2.19).

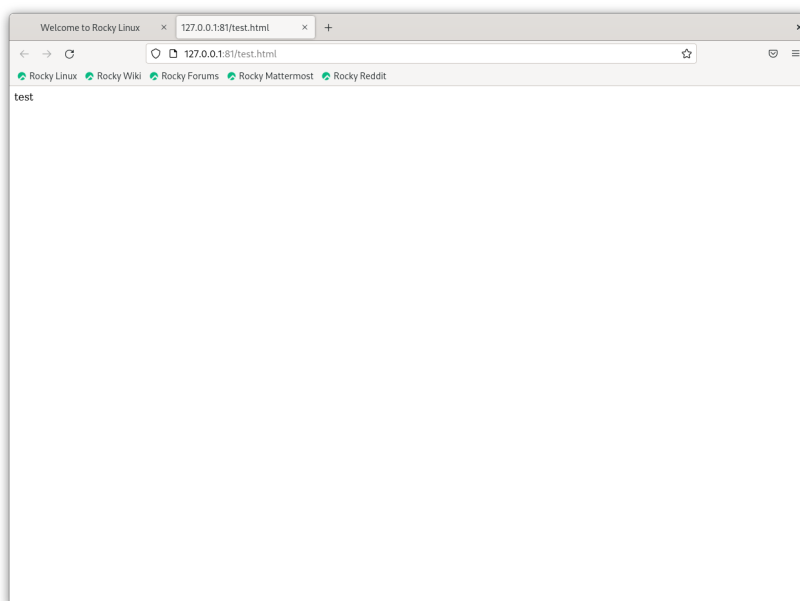


Рис. 2.19: Проверка отображения файла

Исправим обратно конфигурационный файл apache, вернув `Listen 80` (рис. 2.20).

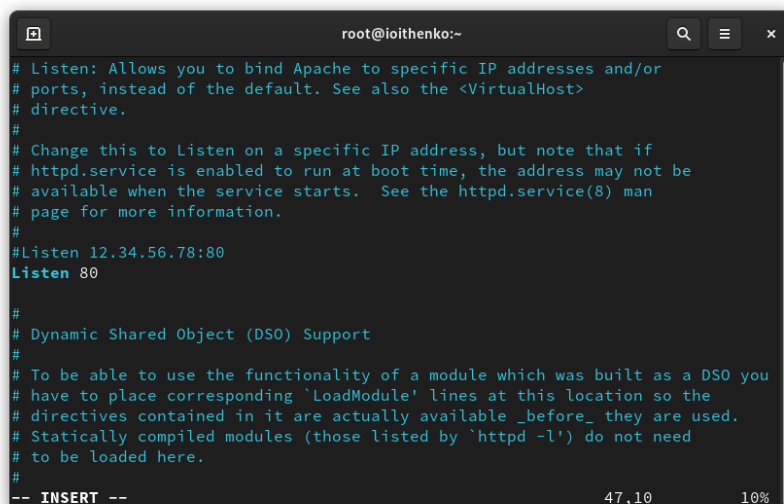
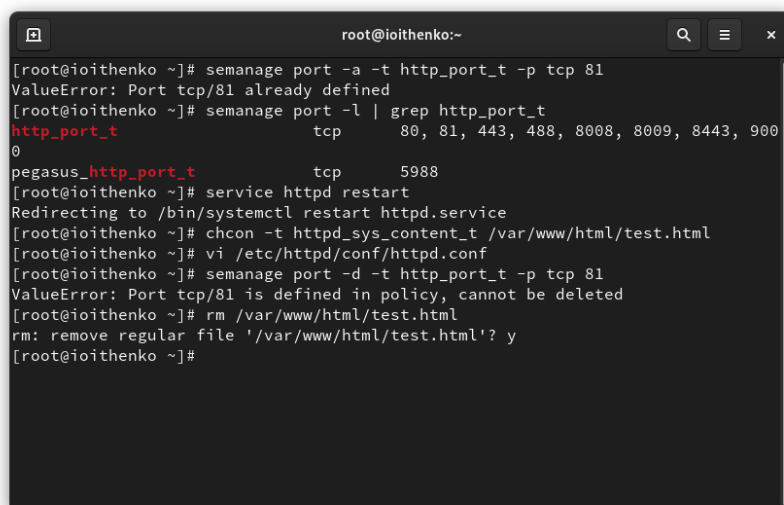


Рис. 2.20: Возвращение исходной конфигурации

Удалим привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp`

81 Удаление не произошло.

Удалим файл /var/www/html/test.html (рис. 2.21): `rm /var/www/html/test.html`



```
root@ioithenko:~  
[root@ioithenko ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Port tcp/81 already defined  
[root@ioithenko ~]# semanage port -l | grep http_port_t  
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000  
0  
pegasus_http_port_t  tcp      5988  
[root@ioithenko ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@ioithenko ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@ioithenko ~]# vi /etc/httpd/conf/httpd.conf  
[root@ioithenko ~]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Port tcp/81 is defined in policy, cannot be deleted  
[root@ioithenko ~]# rm /var/www/html/test.html  
rm: remove regular file '/var/www/html/test.html'? y  
[root@ioithenko ~]#
```

Рис. 2.21: Удаление привязки к порту и файла

3 Выводы

В ходе лабораторной работы я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.