

Отчет по лабораторной работе №6

по дисциплине: Информационная безопасность

Ким Михаил Алексеевич

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	7
5	Анализ результатов	22
6	Выводы	23
	Список литературы	24

Список иллюстраций

4.1	Проверка getenforce и sestatus	7
4.2	Установка и проверка статуса httpd	8
4.3	Запуск httpd	8
4.4	Контекст безопасности httpd	9
4.5	Текущее состояние переключателей SELinux для Apache	10
4.6	Статистика по политике	12
4.7	Определение параметров и создание простого html-файла	13
4.8	Контекст созданного файла	13
4.9	Отображение файла test.html	14
4.10	Проверка контекста файла test.html	14
4.11	Изменение контекста файла test.html. Попытка получения доступа	15
4.12	Log-файлы	15
4.13	Запуск веб-сервера Apache на TCP-порт 81	16
4.14	Список прослушиваемых портов	17
4.15	Обратное изменение контекста файла	17
4.16	Файл открывается	18
4.17	Обратное изменение порта	20
4.18	Попытка удаления привязки TCP-порта 81	21
4.19	Удаление файла text.html	21

1 Цель работы

Развитие навыков администрирования ОС Linux. Получение первого практического знакомства с технологией SELinux. Проверка работы SELinux на практике совместно с веб-сервером Apache.

2 Задание

1. Произвести эксперименты с дополнительными атрибутами прав доступа.

3 Теоретическое введение

- Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями [1].
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами [2].
- В UNIX-системах, кроме стандартных прав доступа, существуют также дополнительные или специальные атрибуты файлов, которые поддерживает файловая система [3].
- SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра [4].
- Apache («Апачи», Apache HTTP Server) — это открытое кросс-платформенное программное обеспечение для размещения и поддержки веб-сервера [5].

4 Выполнение лабораторной работы

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

```
[makim@makim ~]$ getenforce
Enforcing
[makim@makim ~]$ 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
[makim@makim ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
```

Рис. 4.1: Проверка `getenforce` и `sestatus`

2. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает: `service httpd status`. Предварительно установим пакет: `sudo yum install httpd`. Если не работает, запустим его так же, но с параметром `start`. (рис. 4.2, 4.3).

```
[makim@makim ~]$ sudo yum install httpd
Last metadata expiration check: 0:05:07 ago on Sat 21 Oct 2023 07:55:36 PM MSK.
Package httpd-2.4.53-11.el9_2.5.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[makim@makim ~]$ 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: d>
   Active: inactive (dead)
   Docs: man:httpd.service(8)
```

Рис. 4.2: Установка и проверка статуса httpd

```
[makim@makim ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[makim@makim ~]$ 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 Sat 2023-10-21 20:12:31 MSK; 11s ago
   Docs: man:httpd.service(8)
  Main PID: 6261 (httpd)
  Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 50371)
  Memory: 49.6M
    CPU: 70ms
  CGroup: /system.slice/httpd.service
          └─6261 /usr/sbin/httpd -DFOREGROUND
            └─6269 /usr/sbin/httpd -DFOREGROUND
              └─6270 /usr/sbin/httpd -DFOREGROUND
                └─6271 /usr/sbin/httpd -DFOREGROUND
                  └─6273 /usr/sbin/httpd -DFOREGROUND

Oct 21 20:12:31 makim.localdomain systemd[1]: Starting The Apache HTTP Server...
Oct 21 20:12:31 makim.localdomain httpd[6261]: Server configured, listening on: port 80
Oct 21 20:12:31 makim.localdomain systemd[1]: Started The Apache HTTP Server.
```

Рис. 4.3: Запуск httpd

3. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности и занесем эту информацию в отчет. Например, можно использовать команды: `ps auxZ | grep httpd`, `ps -eZ | grep httpd` (рис. 4.4).


```

[makim@makim ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      6261  0.0  0.1 20328 11636 ?        Ss   20:12   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  6269  0.0  0.0 21664 7500 ?        S    20:12   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  6270  0.0  0.2 2521332 19304 ?       SL   20:12   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  6271  0.0  0.2 2324660 21344 ?       SL   20:12   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  6273  0.0  0.2 2324660 21344 ?       SL   20:12   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 makim 6551  0.0  0.0 221664 2248 pts/0 S+  20:16   0:00 grep --color=auto httpd
[makim@makim ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      6261 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      6269 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      6270 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      6271 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      6273 ?          00:00:00 httpd

```

Рис. 4.4: Контекст безопасности httpd

4. Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис. 4.5).

```

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

Policy booleans:
abrt_anon_write                 off
abrt_handle_event               off
abrt_upload_watch_anon_write    on
antivirus_can_scan_system       off
antivirus_use_jit               off
auditadm_exec_content           on
authlogin_nsswitch_use_ldap     off
authlogin_radius                off
authlogin_yubikey               off
awstats_purge_apache_log_files  off
boinc_execmem                   on
cdrecord_read_content           off
cluster_can_network_connect     off
cluster_manage_all_files        off
cluster_use_execmem             off
cobbler_anon_write              off
cobbler_can_network_connect     off
cobbler_use_cifs                off
cobbler_use_nfs                 off
collectd_tcp_network_connect    off
colord_use_nfs                  off
condor_tcp_network_connect      off
conman_can_network              off
conman_use_nfs                  off
container_connect_any           off
container_manage_cgroup         off
container_use_cephfs            off
container_use_devices           off
container_use_ecryptfs          off
cron_can_relabel                off
cron_system_cronjob_use_shares  off
cron_userdomain_transition      on
cups_execmem                    off
cvs_read_shadow                 off
daemons_dontaudit_scheduling   on
daemons_dump_core              off
daemons_enable_cluster_mode    off
daemons_use_tcp_wrapper        off
daemons_use_tty                off

```

Рис. 4.5: Текущее состояние переключателей SELinux для Apache

5. Посмотрим статистику по политике с помощью команды `seinfo` (предварительно установив необходимый пакет), также определим множество пользователей, ролей, типов. (рис. 4.6).

```

[makim@makim ~]$ seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] y

* Waiting in queue...
The following packages have to be installed:
setools-console-4.4.1-1.el9.x86_64      Policy analysis command-line tools for SELinux
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:      33 (MLS enabled)
Target Policy:       selinux
Handle unknown classes: allow
Classes:             135      Permissions:          457
Sensitivities:       1        Categories:          1024
Types:               5100     Attributes:           258
Users:               8        Roles:                14
Booleans:            353     Cond. Expr.:         384
Allow:               65008    Neverallow:           0
Auditallow:          170     Dontaudit:            8572
Type_trans:          265344   Type_change:          87
Type_member:         35      Range_trans:          6164
Role allow:          38      Role_trans:           420
Constraints:         70      Validatetrans:        0
MLS Constrain:       72      MLS Val. Tran:        0
Permissives:         2       Polcap:               6
Defaults:            7       Typebounds:           0
Allowxperm:          0       Neverallowxperm:      0
Auditallowxperm:     0       Dontauditxperm:       0
Ibendportcon:        0       Ibpkeycon:            0
Initial SIDs:        27      Fs_use:               35
Genfscon:            109     Portcon:              660
Netifcon:            0       Nodecon:              0

[makim@makim ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:      33 (MLS enabled)
Target Policy:       selinux
Handle unknown classes: allow
Classes:             135      Permissions:          457
Sensitivities:       1        Categories:          1024
Types:               5100     Attributes:           258
Users:               8        Roles:                14
Booleans:            353     Cond. Expr.:         384
Allow:               65008    Neverallow:           0
Auditallow:          170     Dontaudit:            8572
Type_trans:          265344   Type_change:          87
Type_member:         35      Range_trans:          6164
Role allow:          38      Role_trans:           420
Constraints:         70      Validatetrans:        0
MLS Constrain:       72      MLS Val. Tran:        0
Permissives:         2       Polcap:               6
Defaults:            7       Typebounds:           0
Allowxperm:          0       Neverallowxperm:      0
Auditallowxperm:     0       Dontauditxperm:       0
Ibendportcon:        0       Ibpkeycon:            0
Initial SIDs:        27      Fs_use:               35
Genfscon:            109     Portcon:              660
Netifcon:            0       Nodecon:              0

```

Рис. 4.6: Статистика по политике

6. Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`. Определим тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html: `ll /var/www/html`. Создадим от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис. 4.7):
- ```
html <html> <body>test</body>
</html>
```

```
[makim@makim ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 23:21 html
[makim@makim ~]$ ls -lZ /var/www/html
total 0
[makim@makim ~]$ ll /var/www/html
total 0
[makim@makim ~]$ sudo nano /var/www/html/test.html
```

Рис. 4.7: Определение параметров и создание простого html-файла

7. Проверим контекст созданного файла: `ls -Z /var/www/html`. (рис. 4.8).

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

Рис. 4.8: Контекст созданного файла

8. Обратимся к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедимся, что файл был успешно отображён. (рис. 4.9).

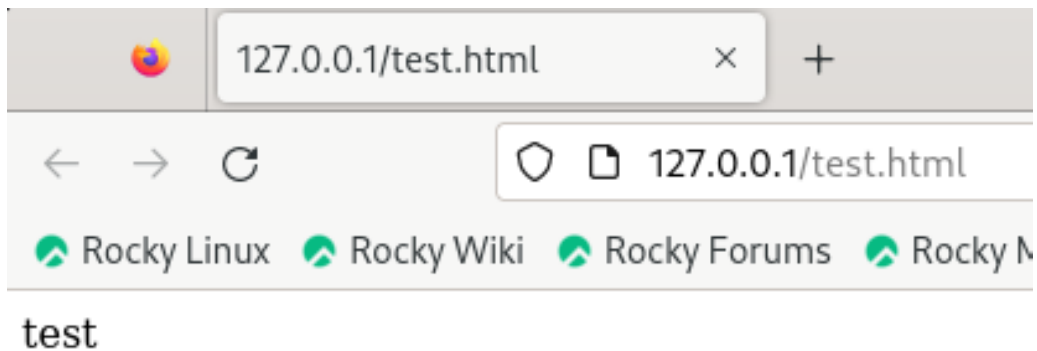


Рис. 4.9: Отображение файла test.html

9. Проверим контекст файла командой: `ls -Z /var/www/html/test.html` (рис. 4.10).

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

Рис. 4.10: Проверка контекста файла test.html

10. 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:chcon -t samba_share_t /var/www/html/test.html`, `ls -Z /var/www/html/test.html`. После этого проверим, что контекст поменялся. При попытку получить доступ к файлу получаем сообщение об ошибке (рис. 4.11).

```
[makim@makim ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] password for makim:
[makim@makim ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[makim@makim ~]$ wget ls -Z /var/www/html/test.html
wget: invalid option -- 'Z'
Usage: wget [OPTION]... [URL]...

Try 'wget --help' for more options.
[makim@makim ~]$ wget http://127.0.0.1/test.html
--2023-10-21 20:22:35-- http://127.0.0.1/test.html
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2023-10-21 20:22:35 ERROR 403: Forbidden.
```

Рис. 4.11: Изменение контекста файла test.html. Попытка получения доступа

## 11. Просмотрим log-файлы (рис. 4.12).

```
[makim@makim ~]$ ll /var/www/html/test.html
-rw-r--r-- 1 root root 33 Oct 21 20:06 /var/www/html/test.html
[makim@makim ~]$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[makim@makim ~]$ sudo tail /var/log/messages
Oct 21 20:23:13 makim setroubleshoot[7790]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For comp
lete SELinux messages run: sealert -l c12c83d7-a61a-4542-a846-61b1f7c488c1
Oct 21 20:23:13 makim setroubleshoot[7790]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012*
**** Plugin restorecon (92.2 confidence) suggests ****#012#012If you want to fix the label, #012/var/www/html/test.html defa
ult label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions t
o access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#0
12#012**** Plugin public_content (7.83 confidence) suggests ****#012#012If you want to treat test.html as public content#012The
n 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/w
ww/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 the test.html file by default.#012Then you should report this as a bug.#012
You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audi
t2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 21 20:23:15 makim firefox.desktop[7553]: [ERROR viaduct::backend::ffi] Missing HTTP status
Oct 21 20:23:15 makim firefox.desktop[7553]: [ERROR viaduct::backend::ffi] Missing HTTP status
Oct 21 20:23:16 makim systemd[3165]: app-gnome-firefox-7553.scope: Consumed 9.949s CPU time.
Oct 21 20:23:23 makim systemd[1]: dbus-1.1-0-rg.fedoraproject.SetroubleshootPrivileged@l.service: Deactivated successfully.
Oct 21 20:23:23 makim systemd[1]: dbus-1.1-0-rg.fedoraproject.SetroubleshootPrivileged@l.service: Consumed 1.180s CPU time.
Oct 21 20:23:23 makim systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 21 20:23:50 makim gnome-shell[3305]: Window manager warning: last_user_time (2401159) is greater than comparison timestamp (2401158). This mos
t likely represents a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 21 20:23:50 makim gnome-shell[3305]: Window manager warning: W1 appears to be one of the offending windows with a timestamp of 2401159. Workin
g around...
[makim@makim ~]$ cat /var/log/audit/audit.log
cat: /var/log/audit/audit.log: Permission denied
[makim@makim ~]$ sudo cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1694286262.889:8843): op=start ver=3.0.7 format=enriched kernel=5.14.0-284.25.1.el9_2.x86_64 audit=4294967295 pid=805 ui
d=0 ses=4294967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1694286262.897:5): pid=1 uid=0 audit=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journ
al-catalog-update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=CONFIG_CHANGE msg=audit(1694286262.915:6): op=set audit_backlog_limit=8192 old=64 audit=4294967295 ses=4294967295 subj=system_u:system_r:unconf
ined_service_t:s0 res=IAUID="unset"
type=SYSCALL msg=audit(1694286262.915:6): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffcb1493710 a2=3c a3=0 items=0 ppid=810 pid=820 au
id=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system
_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EG
ID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1694286262.915:6): proctitle=2F7362696E2F617564697463746C002052002F6574632F61756469742F61756469742E72756C6573
type=CONFIG_CHANGE msg=audit(1694286262.915:7): op=set audit_failure=1 old=1 audit=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_servi
ce_t:s0 res=IAUID="unset"
type=SYSCALL msg=audit(1694286262.915:7): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffcb1493710 a2=3c a3=0 items=0 ppid=810 pid=820 au
id=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=system
_u:system_r:unconfined_service_t:s0 key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EG
ID="root" SGID="root" FSGID="root"
```

Рис. 4.12: Log-файлы

## 12. 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 найдем строчку Listen 80 и заменим её на Listen 81 (рис. 4.13).

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
This is the main Apache HTTP server configuration file. It contains the
configuration directives that give the server its instructions.
See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
In particular, see
<URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
for a discussion of each configuration directive.
#
See the httpd.conf(5) man page for more information on this configuration,
and httpd.service(8) on using and configuring the httpd service.
#
Do NOT simply read the instructions in here without understanding
what they do. They're here only as hints or reminders. If you are unsure
consult the online docs. You have been warned.
#
Configuration and logfile names: If the filenames you specify for many
of the server's control files begin with "/" (or "drive:/" for Win32), the
server will use that explicit path. If the filenames do *not* begin
with "/", the value of ServerRoot is prepended -- so 'log/access_log'
with ServerRoot set to '/www' will be interpreted by the
server as '/www/log/access_log', where as '/log/access_log' will be
interpreted as '/log/access_log'.
#
ServerRoot: The top of the directory tree under which the server's
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 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.
#
File Name to Write: /etc/httpd/conf/httpd.conf
^G Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend M-T Browse
```

Рис. 4.13: Запуск веб-сервера Apache на TCP-порт 81

13. Запустить веб-сервер удалось, т.к. TCP-порт 81 уже находится в списке прослушиваемых портов (рис. 4.14).



```
[makim@makim ~]$ semanage port -l | grep http_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
[makim@makim ~]$ 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
```

Рис. 4.14: Список прослушиваемых портов

14. Вернем 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 попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. (рис. 4.15, 4.16).

```
[makim@makim ~]$ chcon -t httpd_sys_content_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:httpd_sys_content_t:s0': Operation not permitted
[makim@makim ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html
[makim@makim ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[makim@makim ~]$ wget http://127.0.0.1:81/test.html
--2023-10-21 20:33:17-- http://127.0.0.1:81/test.html
Connecting to 127.0.0.1:81... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [text/html]
Saving to: 'test.html'

test.html 100%[=====] 33 --KB/s in 0s
2023-10-21 20:33:17 (7.41 MB/s) - 'test.html' saved [33/33]

[makim@makim ~]$ lynx http://127.0.0.1:81/test.html.
[makim@makim ~]$ lynx http://127.0.0.1:81/test.html
```

Рис. 4.15: Обратное изменение контекста файла

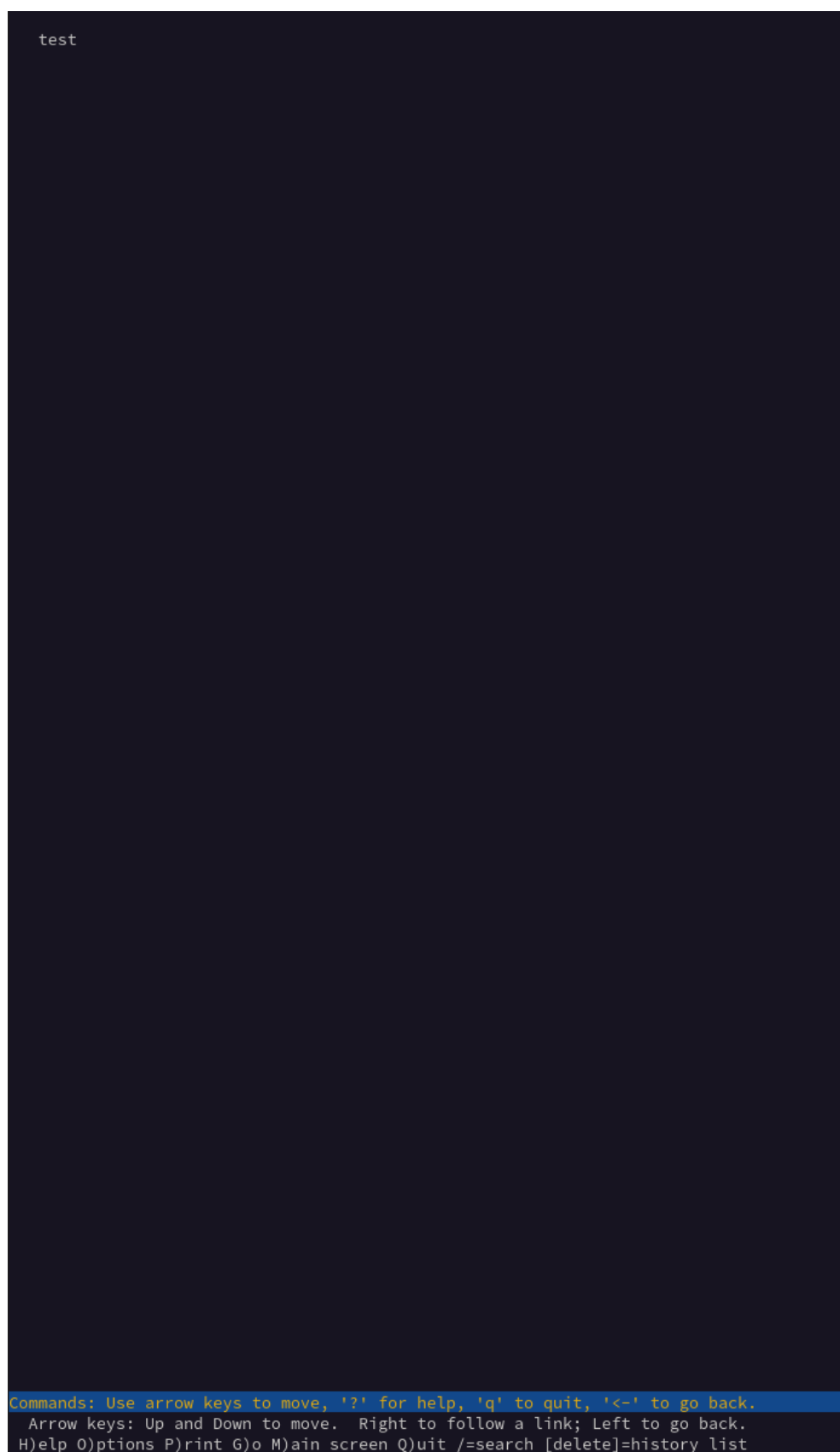


Рис. 4.16: Файл открывается

15. Исправим обратно конфигурационный файл apache, вернув Listen 80. (рис. 4.17).

```

GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
This is the main Apache HTTP server configuration file. It contains the
configuration directives that give the server its instructions.
See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
In particular, see
<URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
for a discussion of each configuration directive.
#
See the httpd.conf(5) man page for more information on this configuration,
and httpd.service(8) on using and configuring the httpd service.
#
Do NOT simply read the instructions in here without understanding
what they do. They're here only as hints or reminders. If you are unsure
consult the online docs. You have been warned.
#
Configuration and logfile names: If the filenames you specify for many
of the server's control files begin with "/" (or "drive:/" for Win32), the
server will use that explicit path. If the filenames do *not* begin
with "/", the value of ServerRoot is prepended -- so 'log/access_log'
with ServerRoot set to '/www' will be interpreted by the
server as '/www/log/access_log', where as '/log/access_log' will be
interpreted as '/log/access_log'.
#
ServerRoot: The top of the directory tree under which the server's
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 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 80
#
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.
#
File Name to Write: /etc/httpd/conf/httpd.conf

```

Рис. 4.17: Обратное изменение порта

16. Удалить привязку `http_port_t` к 81 порту невозможно из-за политики (рис. 4.18).

```
[makim@makim ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Рис. 4.18: Попытка удаления привязки TCP-порта 81

17. Удалим файл `/var/www/html/test.html`: `rm /var/www/html/test.html` (рис. 4.19).

```
[makim@makim ~]$ sudo nano /etc/httpd/conf/httpd.conf
[makim@makim ~]$ semanage port -d -t http_port_t -p tcp 81
ValueError: SELinux policy is not managed or store cannot be accessed.
[makim@makim ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[makim@makim ~]$ 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
[makim@makim ~]$ 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
[makim@makim ~]$ rm /var/www/html/test.html
rm: remove write-protected regular file '/var/www/html/test.html'? y
rm: cannot remove '/var/www/html/test.html': Permission denied
[makim@makim ~]$ sudo rm /var/www/html/test.html
[makim@makim ~]$ ll /var/www/html
total 0
```

Рис. 4.19: Удаление файла `test.html`

## **5 Анализ результатов**

Работа выполнена без каких-либо проблем. Работа с терминалом ОС Rocky Linux в данном случае нареканий не вызвала.

## 6 Выводы

Развиты навыки администрирования ОС Linux. Полученное первое практическое знакомство с технологией SELinux. Проверена работа SELinux на практике совместно с веб-сервером Apache.

## Список литературы

1. Терминал Linux [Электронный ресурс]. URL: [%7Bhttps://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/%7D](https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/).
2. Права доступа [Электронный ресурс]. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.
3. Дополнительные атрибуты файлов [Электронный ресурс]. Enchanted Technology, 2022. URL: [https://wiki.enchtex.info/doc/linux\\_file\\_attributes](https://wiki.enchtex.info/doc/linux_file_attributes).
4. SELinux – описание и особенности работы с системой. Часть 1 [Электронный ресурс]. Habr, 2014. URL: <https://habr.com/ru/companies/kingservers/articles/209644/>.
5. Apache [Электронный ресурс]. Skillfactory Media, 2023. URL: <https://blog.skillfactory.ru/glossary/apache/>.