

Лабораторная работа №6

Мандатное разграничение прав в Linux

Монастырская Кристина Владимировна

Содержание

Цель работы	4
Выполнение лабораторной работы	5
Выводы	16
Список литературы	17

Список иллюстраций

1	Режим SELinux	5
2	Проверка работы веб-сервера	6
3	Список процессов	6
4	Состояние переключателей SELinux	7
5	Статистика SELinux	8
6	Тип поддиректорий в директории /var/www	8
7	Директория /var/www/html	9
8	Право на создание файлов	9
9	HTML-файл /var/www/html/test.html	9
10	Контекст файла	10
11	Отображение файла test.html	10
12	Изменение контекста файла	11
13	Доступ через веб-сервер	11
14	log-файл	12
15	Системный log-файл	12
16	Включение прослушивания 81 порта	13
17	Лог-файл /var/log/messages	13
18	Лог-файл /var/log/http/error_log	13
19	Лог-файл /var/log/http/access_log	14
20	Лог-файл /var/log/audit/audit.log	14
21	Список портов	14
22	Конфигурационный файл Apache	15
23	Удаление порта из списка	15
24	Удаление файла	15

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache. [1]

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. 1)

```
[root@kvmonastyrskaya ~]# getenforce
bash: getenforce: command not found...
Similar command is: 'getenforce'
[root@kvmonastyrskaya ~]# getenforce
Enforcing
[root@kvmonastyrskaya ~]# 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
[root@kvmonastyrskaya ~]#
```

Рис. 1: Режим SELinux

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

```
[root@kvmonastyrskaya ~]# 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 pre
   Active: active (running) since Sun 2022-12-18 15:51:22 MSK; 53min ago
     Docs: man:httpd.service(8)
   Main PID: 3508 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
      Tasks: 213 (limit: 10804)
     Memory: 35.2M
        CPU: 4.472s
   CGroup: /system.slice/httpd.service
           └─3508 /usr/sbin/httpd -DFOREGROUND
             └─3509 /usr/sbin/httpd -DFOREGROUND
               └─3510 /usr/sbin/httpd -DFOREGROUND
                 └─3511 /usr/sbin/httpd -DFOREGROUND
                   └─3512 /usr/sbin/httpd -DFOREGROUND

дек 18 15:51:22 kvmonastyrskaya systemd[1]: Starting The Apache HTTP Server...
дек 18 15:51:22 kvmonastyrskaya systemd[1]: Started The Apache HTTP Server.
дек 18 15:51:22 kvmonastyrskaya httpd[3508]: Server configured, listening on: p
lines 1-19/19 (FND)
```

Рис. 2: Проверка работы веб-сервера

3. Нашла веб-сервер Apache в списке процессов. (рис. 3).

```
[root@kvmonastyrskaya ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3508 0.0 0.4 20132 8656 ?
Ss 15:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3509 0.0 0.2 21608 5132 ?
S 15:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3510 0.0 0.6 2062420 12112 ?
Sl 15:51 0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3511 0.0 0.7 2193556 14004 ?
Sl 15:51 0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3512 0.0 0.6 2062420 12532 ?
Sl 15:51 0:01 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 6405 0.0 0.1 221820
2360 pts/0 S+ 16:47 0:00 grep --color=auto httpd
[root@kvmonastyrskaya ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 3508 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3509 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3510 ? 00:00:01 httpd
system_u:system_r:httpd_t:s0 3511 ? 00:00:01 httpd
system_u:system_r:httpd_t:s0 3512 ? 00:00:01 httpd
[root@kvmonastyrskaya ~]#
```

Рис. 3: Список процессов

Контекст безопасности: system_u:system_r:httpd_t:s0

4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd`. (рис. 4).

```
[root@kvmonastyrskaya ~]# 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_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 off
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
```

Рис. 4: Состояние переключателей SELinux

Многие из них находятся в положении «off»

5. Посмотрела статистику по политике с помощью команды seinfo. (рис. 5).

```

[root@kvmonastyrskaya ~]# 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:                   5095  Attributes:              256
Users:                   8     Roles:                  14
Booleans:                351   Cond. Expr.:            383
Allow:                   65187  Neverallow:              0
Auditallow:              165   Dontaudit:              8564
Type_trans:              257951 Type_change:              87
Type_member:              35   Range_trans:            6164
Role allow:              38   Role_trans:              419
Constraints:             70   Validatetrans:           0
MLS Constrains:          72   MLS Val. Tran:           0
Permissives:             0    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
[root@kvmonastyrskaya ~]#

```

Рис. 5: Статистика SELinux

Множество пользователей - 8

Ролей - 14 Типов - 5002

6. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. 6).

```

[root@kvmonastyrskaya ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 июл 22 14
:43 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 июл 22 14
:43 html
[root@kvmonastyrskaya ~]#

```

Рис. 6: Тип поддиректорий в директории /var/www

7. Определила тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` (рис. 7).

```
[root@kvmonastyrskaya ~]# ls -lZ /var/www/html
итого 0
```

Рис. 7: Директория /var/www/html

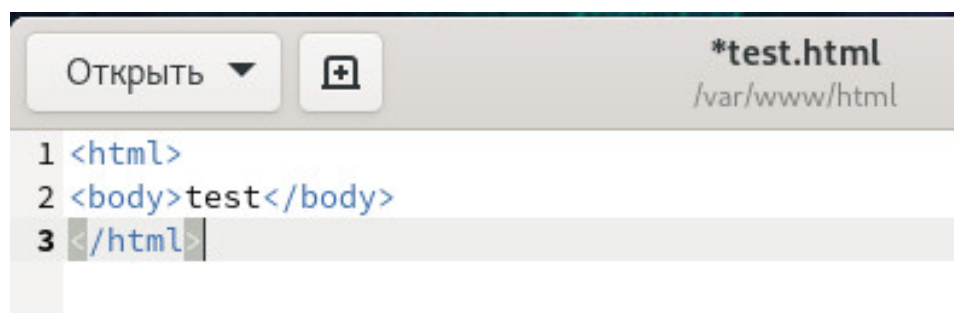
8. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 8).

```
[root@kvmonastyrskaya ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 июл 22 14
:43 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 июл 22 14
:43 html
```

Рис. 8: Право на создание файлов

Создавать файлы в директории может только её владелец.

9. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания: (рис. 9).



```
*test.html
/var/www/html

1 <html>
2 <body>test</body>
3 </html>
```

Рис. 9: HTML-файл /var/www/html/test.html

10. Проверила контекст созданного файла. (рис. 10).

```
[root@kvmonastyrskaya ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@kvmonastyrskaya ~]#
```

Рис. 10: Контекст файла

Контекст безопасности (по умолчанию для новых файлов в директории):
unconfined_u:object_r:httpd_sys_content_t:s0

11. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.
(рис. 11).

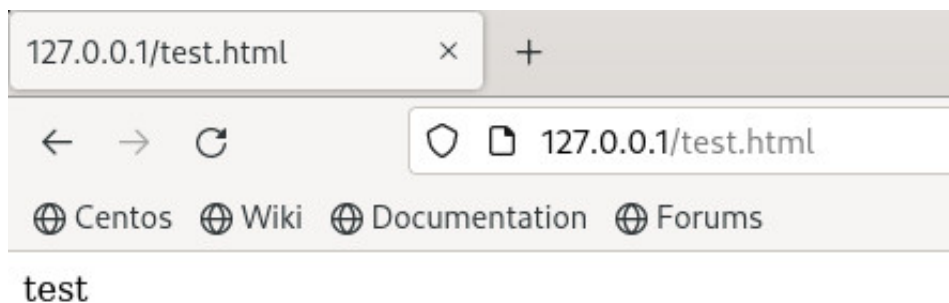


Рис. 11: Отображение файла test.html

12. Изучила справку `man httpd_selinux` (рис. 12).

13. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на тот, к которому процесс `httpd` не имеет доступ (`samba_share_t`) (рис. 13).

```
[root@kvmonastyrskaya ~]# chcon -t samba_share_t /var/www/html/test.html
[root@kvmonastyrskaya ~]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@kvmonastyrskaya ~]#
```

Рис. 12: Изменение контекста файла

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

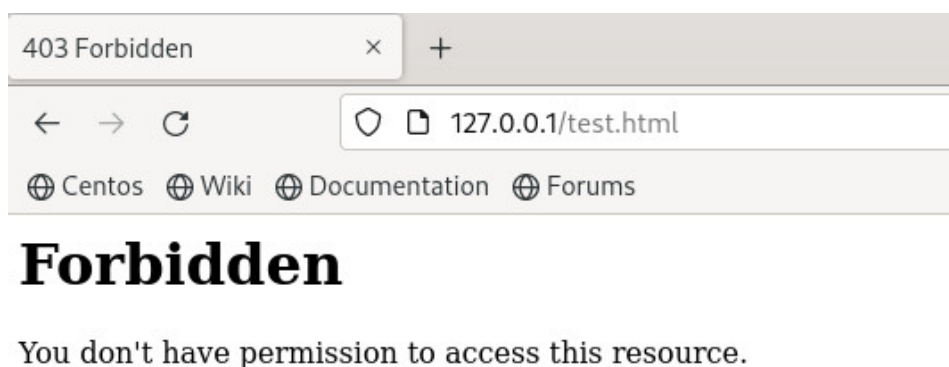


Рис. 13: Доступ через веб-сервер

Файл не отображен, так как к заданному типу контекста `httpd` не имеет доступа.

15. Просмотрела log-файлы веб-сервера Apache. (рис. 15)

```
[root@kvmonastyrskaya ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 дек 18 16:56 /var/www/html/test.html
[root@kvmonastyrskaya ~]# tail /var/log/messages
Dec 18 17:04:36 kvmonastyrskaya systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Dec 18 17:04:38 kvmonastyrskaya setroubleshoot[7503]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
test.html. Для выполнения всех сообщений SELinux: sealert -l 00505e2e-980e-4fc6-a0f7-9db17343b02d
Dec 18 17:04:38 kvmonastyrskaya setroubleshoot[7503]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите испра
вить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, по
пытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайт
есь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012+
**** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html как общ
едоступный контент#012То необходимо изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# sema
nage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012**** Мо
дуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разреше
но getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, мож
но создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Dec 18 17:04:38 kvmonastyrskaya setroubleshoot[7503]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
test.html. Для выполнения всех сообщений SELinux: sealert -l 00505e2e-980e-4fc6-a0f7-9db17343b02d
Dec 18 17:04:38 kvmonastyrskaya setroubleshoot[7503]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите испра
вить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, по
пытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайт
есь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012+
**** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html как общ
едоступный контент#012То необходимо изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# sema
nage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012**** Мо
дуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разреше
но getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, мож
но создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw |
audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Dec 18 17:04:48 kvmonastyrskaya systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated succ
essfully.
Dec 18 17:04:48 kvmonastyrskaya systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.693s
CPU time.
Dec 18 17:04:48 kvmonastyrskaya systemd[1]: setroubleshootd.service: Deactivated successfully.
Dec 18 17:04:48 kvmonastyrskaya systemd[1]: setroubleshootd.service: Consumed 1.378s CPU time.
Dec 18 17:05:12 kvmonastyrskaya journal[5531]: Source ID 15989 was not found when attempting to remove it
[root@kvmonastyrskaya ~]#
```

Рис. 14: log-файл

Посмотрела системный лог-файл (рис. 16).

```
[root@kvmonastyrskaya ~]# tail /var/log/audit/audit.log
type=AVC msg=audit(1671372275.164:399): avc: denied { getattr } for pid=3512 comm="httpd" path="/var/www/html/test.html"
dev="dm-0" ino=71300109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file pe
rmisive=0
type=SYSCALL msg=audit(1671372275.164:399): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f6f4c00caa8 a2=7f6
f68fe98b0 a3=0 items=0 ppid=3508 pid=3512 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tt
y=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=n
ewfstatat AUDID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGI
D="apache"
type=PROCTITLE msg=audit(1671372275.164:399): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=AVC msg=audit(1671372275.165:400): avc: denied { getattr } for pid=3512 comm="httpd" path="/var/www/html/test.html"
dev="dm-0" ino=71300109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file pe
rmisive=0
type=SYSCALL msg=audit(1671372275.165:400): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f6f4c00cb88 a2=7f6
f68fe98b0 a3=100 items=0 ppid=3508 pid=3512 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="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=
newfstatat AUDID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FS
GID="apache"
type=PROCTITLE msg=audit(1671372275.165:400): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1671372276.228:401): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg="unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success"UID="root"
AUDID="unset"
type=SERVICE_START msg=audit(1671372276.785:402): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg="unit=dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?
addr=? terminal=? res=success"UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1671372288.820:403): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg="unit=dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?
addr=? terminal=? res=success"UID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1671372288.859:404): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg="unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success"UID="root"
AUDID="unset"
[root@kvmonastyrskaya ~]#
```

Рис. 15: Системный log-файл

Можем видеть как отображаются ошибки.

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

(рис. 17).

```
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
```

Рис. 16: Включение прослушивания 81 порта

17. Выполнила перезапуск веб-сервера Apache и посмотрела лог-файлы (рис. 17-рис. 20).

```
[root@kvmonastyrskaya ~]# tail -l /var/log/messages
Dec 18 17:09:47 kvmonastyrskaya systemd[1]: Stopping The Apache HTTP Server...
Dec 18 17:09:48 kvmonastyrskaya systemd[1]: httpd.service: Deactivated successfully.
Dec 18 17:09:48 kvmonastyrskaya systemd[1]: Stopped The Apache HTTP Server.
Dec 18 17:09:48 kvmonastyrskaya systemd[1]: httpd.service: Consumed 6.183s CPU time.
Dec 18 17:09:48 kvmonastyrskaya systemd[1]: Starting The Apache HTTP Server...
Dec 18 17:09:48 kvmonastyrskaya systemd[1]: Started The Apache HTTP Server.
Dec 18 17:09:48 kvmonastyrskaya httpd[7638]: Server configured, listening on: port 81
Dec 18 17:09:58 kvmonastyrskaya systemd[1]: Stopping The Apache HTTP Server...
Dec 18 17:09:59 kvmonastyrskaya systemd[1]: httpd.service: Deactivated successfully.
Dec 18 17:09:59 kvmonastyrskaya systemd[1]: Stopped The Apache HTTP Server.
[root@kvmonastyrskaya ~]#
```

Рис. 17: Лог-файл /var/log/messages

```
[root@kvmonastyrskaya ~]# tail /var/log/httpd/error_log
[Sun Dec 18 15:51:22.702565 2022] [mpm_event:notice] [pid 3508:tid 3508] AH00489: Apache/2.4.53 (CentOS Stream) configured
- resuming normal operations
[Sun Dec 18 15:51:22.702686 2022] [core:notice] [pid 3508:tid 3508] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sun Dec 18 17:04:35.166914 2022] [core:error] [pid 3512:tid 3686] (13)Permission denied: [client 127.0.0.1:58114] AH00035:
access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a compone
nt of the path
[Sun Dec 18 17:09:47.269096 2022] [mpm_event:notice] [pid 3508:tid 3508] AH00492: caught SIGWINCH, shutting down gracefully
[Sun Dec 18 17:09:48.448864 2022] [core:notice] [pid 7638:tid 7638] SELinux policy enabled; httpd running as context system
u:system_r:httpd_t:s0
[Sun Dec 18 17:09:48.450996 2022] [suexec:notice] [pid 7638:tid 7638] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin
suexec)
[Sun Dec 18 17:09:48.464389 2022] [lbmethod_heartbeat:notice] [pid 7638:tid 7638] AH02282: No slotmem from mod_heartbeat
[Sun Dec 18 17:09:48.469478 2022] [mpm_event:notice] [pid 7638:tid 7638] AH00489: Apache/2.4.53 (CentOS Stream) configured
- resuming normal operations
[Sun Dec 18 17:09:48.469517 2022] [core:notice] [pid 7638:tid 7638] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sun Dec 18 17:09:58.668341 2022] [mpm_event:notice] [pid 7638:tid 7638] AH00492: caught SIGWINCH, shutting down gracefully
[root@kvmonastyrskaya ~]#
```

Рис. 18: Лог-файл /var/log/http/error_log

```
[root@kvmonastyrskaya ~]# tail /var/log/httpd/access_log
127.0.0.1 - - [18/Dec/2022:16:59:15 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
ecko/20100101 Firefox/102.0"
127.0.0.1 - - [18/Dec/2022:16:59:15 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X
1; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
127.0.0.1 - - [18/Dec/2022:17:04:35 +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 - - [18/Dec/2022:17:04:35 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X
1; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
[root@kvmonastyrskaya ~]#
```

Рис. 19: Лог-файл /var/log/httpd/access_log

```
[root@kvmonastyrskaya ~]# tail /var/log/audit/audit.log
type=AVC msg=audit(1671372275.165:400): avc: denied { getattr } for pid=3512 comm="httpd" path="/var/www/html/test.html"
dev="dm-0" ino=71300109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file pe
rmisive=0
type=SYSCALL msg=audit(1671372275.165:400): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f6f4c00cb88 a2=7f6
f68fe98b0 a3=100 items=0 ppid=3508 pid=3512 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="/usr/sbin/httpd" subj=system_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="apache" SGID="apache" FS
GID="apache"
type=PROCTITLE msg=audit(1671372275.165:400): proctitle=2F7573722F7362696E2F687474064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1671372276.228:401): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=SERVICE_START msg=audit(1671372276.785:402): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=dbus-1.1-0.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?
addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1671372288.820:403): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=dbus-1.1-0.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? a
ddr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1671372288.859:404): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0
msg='unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=SERVICE_STOP msg=audit(1671372588.353:405): pid=1 uid=0 auid=4294967295 ses=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="uns
et"
type=SERVICE_START msg=audit(1671372588.466:406): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="un
set"
type=SERVICE_STOP msg=audit(1671372599.684:407): pid=1 uid=0 auid=4294967295 ses=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="uns
et"
[root@kvmonastyrskaya ~]#
```

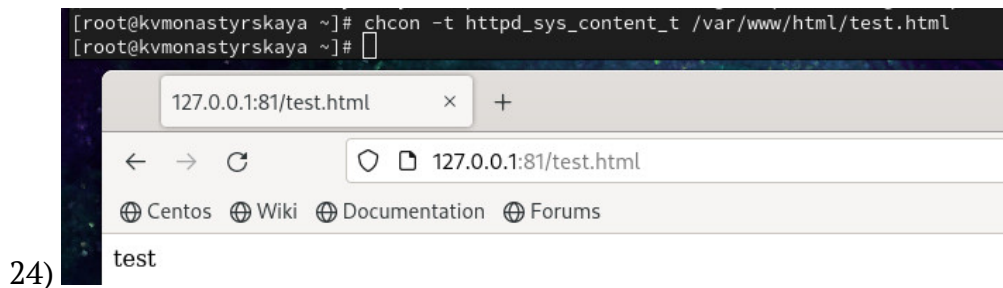
Рис. 20: Лог-файл /var/log/audit/audit.log

18. Добавила порт 81 в список портов. (рис. 21).

```
[root@kvmonastyrskaya ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kvmonastyrskaya ~]# 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
[root@kvmonastyrskaya ~]#
```

Рис. 21: Список портов

19. Вернула контекст httpd_sys_content_t к файлу /var/www/html/ test.html:..
Попробовала получить доступ к файлу через веб-сервер по 81 порту (рис.



20. Исправила обратно конфигурационный файл apache (рис. 26).

```

44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 80
48

```

Рис. 22: Конфигурационный файл Apache

21. Попробовала удалить привязку http_port_t к 81 порту (рис. 27).

```

[root@kvmonastyrskaya ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@kvmonastyrskaya ~]# 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
[root@kvmonastyrskaya ~]#

```

Рис. 23: Удаление порта из списка

22. Удалила файл /var/www/html/test.html (рис. 28).

```

[root@kvmonastyrskaya ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@kvmonastyrskaya ~]#

```

Рис. 24: Удаление файла

Выводы

Получили практическое знакомство с технологией SELinux¹. Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы

1. Основы безопасности информационных систем : Учеб. пособие для студентов вузов, обучающихся по специальностям “Компьютер. безопасность” и “Комплекс. обеспечение информ. безопасности автоматизир. систем” / Д.А. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. - 449, [2] с. : ил., табл.; 21 см.; ISBN 5-93517-018-3.