

Отчёт по лабораторной работе №6. Мандатное разграничение прав в Linux

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Вывод	18
5	Библиография	19

List of Figures

3.1	getenforce и sestatus	6
3.2	Веб-сервер	7
3.3	Apache	7
3.4	Состояние переключателей	8
3.5	seinfo	9
3.6	тип	9
3.7	тип	10
3.8	круг пользователей	10
3.9	файл	10
3.10	контекст	11
3.11	http://127.0.0.1/test.html	11
3.12	Проверка	11
3.13	Смена контекста	12
3.14	Ошибка	12
3.15	log-файлы	13
3.16	Замена	14
3.17	/var/log/messages	15
3.18	/var/log/http/access_log	15
3.19	/var/log/http/error_log	15
3.20	81	15
3.21	«test»	16
3.22	«test»	16
3.23	Listen 80	17
3.24	81	17
3.25	Удалите файл	17

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. [1]

2 Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

3 Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 3.1)

```
[root@asbaklashov ~]# getenforce
Enforcing
[root@asbaklashov ~]# 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@asbaklashov ~]#
```

Figure 3.1: `getenforce` и `sestatus`

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (рис. 3.2)

```

[root@asbaklashov ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@asbaklashov ~]# 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 pr
   Active: active (running) since Fri 2022-10-14 22:37:29 MSK; 2s ago
     Docs: man:httpd.service(8)
    Main PID: 40085 (httpd)
   Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12212)
    Memory: 23.0M
       CPU: 57ms
    CGroup: /system.slice/httpd.service
           └─40085 /usr/sbin/httpd -DFOREGROUND
             40086 /usr/sbin/httpd -DFOREGROUND
             40090 /usr/sbin/httpd -DFOREGROUND
             40091 /usr/sbin/httpd -DFOREGROUND
             40093 /usr/sbin/httpd -DFOREGROUND

Oct 14 22:37:29 asbaklashov.localadmin systemd[1]: Starting The Apache HTTP Ser
Oct 14 22:37:29 asbaklashov.localadmin systemd[1]: Started The Apache HTTP Serv
Oct 14 22:37:29 asbaklashov.localadmin httpd[40085]: Server configured, listeni
lines 1-19/19 (END)
[2]+  Stopped                  service httpd status
[root@asbaklashov ~]#

```

Figure 3.2: Веб-сервер

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. (рис. 3.3)

```

[root@asbaklashov ~]# ps auxZ | grep httpd-
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40344 0.0  0.1 221668 2248 pts/0 S+ 22:38  0
:00 grep --color=auto httpd-
[root@asbaklashov ~]# ps -eZ | grep httpd-
[root@asbaklashov ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      40085 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      40086 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      40090 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      40091 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      40093 ?          00:00:00 httpd
[root@asbaklashov ~]#

```

Figure 3.3: Apache

httpd_sys_content_t

4. Посмотрите текущее состояние переключателей SELinux для Apache. (рис. 3.4)

```

[root@asbaklashov ~]# 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
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_opencryptoki off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
[root@asbaklashov ~]#

```

Figure 3.4: Состояние переключателей

5. Посмотрите статистику по политике с помощью команды `seinfo`, также

определите множество пользователей, ролей, типов. (рис. 3.5)

```
[root@asbaklashov ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  133      Permissions:              454
Sensitivities:            1        Categories:              1024
Types:                    4995     Attributes:              254
Users:                    8         Roles:                   14
Booleans:                 347      Cond. Expr.:            382
Allow:                    63727    Neverallow:              0
Auditallow:              163      Dontaudit:              8391
Type_trans:              251060   Type_change:             87
Type_member:              35       Range_trans:            5958
Role_allow:              38       Role_trans:             418
Constraints:             72       Validatetrans:          0
MLS Constrain:           72       MLS Val. Tran:          0
Permissives:             0        Polcap:                 5
Defaults:                7        Typebounds:             0
Allowxperm:              0        Neverallowxperm:        0
Auditallowxperm:         0        Dontauditxperm:         0
Ibendportcon:            0        Ibpkeycon:              0
Initial SIDs:            27       Fs_use:                 33
Genfscon:                106      Portcon:                651
Netifcon:                0        Nodecon:                0
[root@asbaklashov ~]#
```

Figure 3.5: seinfo

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www (рис. 3.6)

```
[root@asbaklashov ~]# 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 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0    6 May 16 15:10 html
[root@asbaklashov ~]#
```

Figure 3.6: тип

7. Определите тип файлов, находящихся в директории /var/www/html (рис. 3.7)

```
[root@asbaklashov ~]# ls -lZ /var/www/html
total 0
[root@asbaklashov ~]#
```

Figure 3.7: тип

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 3.8)

```
[root@asbaklashov ~]# 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 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 May 16 15:10 html
```

Figure 3.8: круг пользователей

Только владелец

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

```
< html >
< body >test< /body >
< /html >
```

(рис. 3.9)

```
test.html [----] 7 L: [ 1+ 2 3/ 3] *(32 / 32b) <EOF>
<html>
<body>test</body>
</html>
```

Figure 3.9: файл

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. 3.10)

```
[root@asbaklashov html]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 32 Oct 14 22:54 test.html
[root@asbaklashov html]#
```

Figure 3.10: контекст

httpd_sys_content_t

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён. (рис. 3.11)

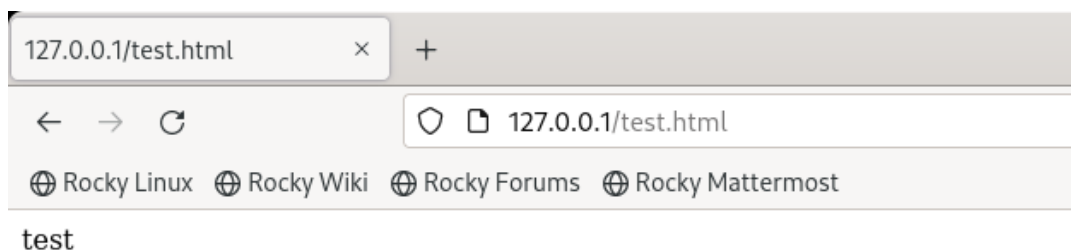


Figure 3.11: <http://127.0.0.1/test.html>

Файл был успешно отображён

12. Проверить контекст файла `/var/www/html/test.html` командой `ls -Z. ls -Z /var/www/html/test.html` (рис. 3.12)

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

Figure 3.12: Проверка

13. Измените 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. 3.13)

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

Figure 3.13: Смена контекста

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об ошибке (рис. 3.14)

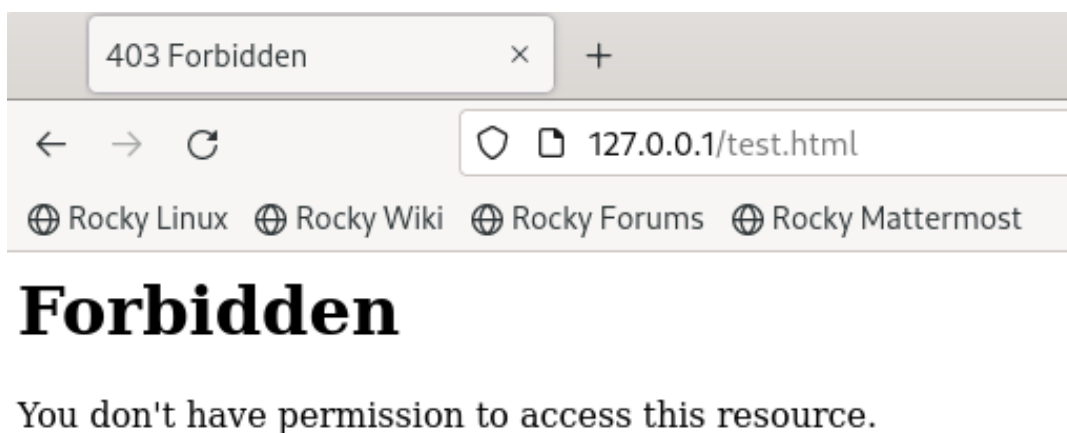


Figure 3.14: Ошибка

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` (рис. 3.15)

```

[root@asbaklashov html]# tail /var/log/messages
Oct 14 23:02:00 asbaklashov setroubleshoot[41570]: 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 default label s
*****#012#012Then you can run restorecon. The access attempt may have been stopped d
ue to insufficient permissions to access a parent directory in which case try to change the following co
mmand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public co
ntent (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.#01
2Do#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 *****#0
12#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Th
en you should report this as a bug.#012You can generate a local policy module to allow this access.#012D
o#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#01
2# semodule -X 300 -i my-httpd.pp#012
Oct 14 23:02:00 asbaklashov setroubleshoot[41570]: failed to retrieve rpm info for /var/www/html/test.ht
ml
Oct 14 23:02:00 asbaklashov setroubleshoot[41570]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l b7358313-6597-49
25-ae09-43445b33548b
Oct 14 23:02:00 asbaklashov setroubleshoot[41570]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess 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 default label s
should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped d
ue to insufficient permissions to access a parent directory in which case try to change the following co
mmand accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public co
ntent (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.#01
2Do#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 *****#0
12#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Th
en you should report this as a bug.#012You can generate a local policy module to allow this access.#012D
o#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#01
2# semodule -X 300 -i my-httpd.pp#012
Oct 14 23:02:10 asbaklashov systemd[1508]: app-gnome-firefox-41360.scope: Consumed 11.222s CPU time.
Oct 14 23:02:10 asbaklashov systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service:
Main process exited, code=killed, status=14/ALRM
Oct 14 23:02:10 asbaklashov systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service:
Failed with result 'signal'.
Oct 14 23:02:10 asbaklashov systemd[1]: dbus-:1.10-org.fedoraproject.SetroubleshootPrivileged@0.service:
Consumed 1.180s CPU time.
Oct 14 23:02:10 asbaklashov systemd[1]: dbus-:1.10-org.fedoraproject.Setroubleshootd@0.service: Main pro
cess exited, code=killed, status=14/ALRM
Oct 14 23:02:10 asbaklashov systemd[1]: dbus-:1.10-org.fedoraproject.Setroubleshootd@0.service: Failed w
ith result 'signal'.

```

Figure 3.15: log-файлы

16. Попробуйте 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 замените её на Listen 81. (рис. 3.16)

```

httpd.conf      [-M--]  9 L:[ 18+36  54/360] *(2230/12024b) 0118 0x076
# 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

```

Figure 3.16: Замена

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

Сбоя нет.

18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи. (рис. 3.17, рис. 3.18, рис. 3.19)

```
[root@asbaklashov conf]# tail -n15 /var/log/messages
Oct 14 23:07:49 asbaklashov systemd[1]: Reloading The Apache HTTP Server...
Oct 14 23:07:49 asbaklashov systemd[1]: Reloaded The Apache HTTP Server.
Oct 14 23:07:49 asbaklashov httpd[40085]: Server configured, listening on: port 81
Oct 14 23:07:57 asbaklashov systemd[1]: Stopping The Apache HTTP Server...
Oct 14 23:07:58 asbaklashov systemd[1]: httpd.service: Deactivated successfully.
Oct 14 23:07:58 asbaklashov systemd[1]: Stopped The Apache HTTP Server.
Oct 14 23:08:01 asbaklashov systemd[1]: Starting The Apache HTTP Server...
Oct 14 23:08:01 asbaklashov systemd[1]: Started The Apache HTTP Server.
Oct 14 23:08:01 asbaklashov httpd[42514]: Server configured, listening on: port 81
Oct 14 23:09:13 asbaklashov systemd[1]: Stopping The Apache HTTP Server...
Oct 14 23:09:14 asbaklashov systemd[1]: httpd.service: Deactivated successfully.
Oct 14 23:09:14 asbaklashov systemd[1]: Stopped The Apache HTTP Server.
Oct 14 23:09:17 asbaklashov systemd[1]: Starting The Apache HTTP Server...
Oct 14 23:09:17 asbaklashov systemd[1]: Started The Apache HTTP Server.
Oct 14 23:09:17 asbaklashov httpd[42825]: Server configured, listening on: port 81
```

Figure 3.17: /var/log/messages

```
/var/log/httpd/access_log
127.0.0.1 - - [14/Oct/2022:22:56:00 +0300] "GET /test.html HTTP/1.1" 200 32 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:22:56:00 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:01:57 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:01:58 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:06:44 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:06:44 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:06:47 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:06:48 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:07:00 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
127.0.0.1 - - [14/Oct/2022:23:07:01 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
```

Figure 3.18: /var/log/httpd/access_log

```
[root@asbaklashov ~]# tail -n 100 /var/log/httpd/error_log
[Fri Oct 14 22:37:29.409055 2022] [core:notice] [pid 40085:tid 40085] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 14 22:37:29.410236 2022] [suexec:notice] [pid 40085:tid 40085] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 14 22:37:29.422741 2022] [lbmethod:heartbeat:notice] [pid 40085:tid 40085] AH02282: No slotmem from mod_heartbeat
[Fri Oct 14 22:37:29.433505 2022] [mpm_event:notice] [pid 40085:tid 40085] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 14 22:37:29.433529 2022] [core:notice] [pid 40085:tid 40085] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Fri Oct 14 23:01:57.475160 2022] [core:error] [pid 40093:tid 40289] (13)Permission denied: [client 127.0.0.1:39106] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing
[Fri Oct 14 23:06:44.031824 2022] [core:error] [pid 40093:tid 40284] (13)Permission denied: [client 127.0.0.1:39108] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing
[Fri Oct 14 23:06:47.263002 2022] [core:error] [pid 40093:tid 40293] (13)Permission denied: [client 127.0.0.1:39108] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing
[Fri Oct 14 23:06:48.743588 2022] [core:error] [pid 40093:tid 40294] (13)Permission denied: [client 127.0.0.1:39108] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing
[Fri Oct 14 23:07:00.362930 2022] [core:error] [pid 40093:tid 40296] (13)Permission denied: [client 127.0.0.1:39110] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing
[Fri Oct 14 23:07:49.708039 2022] [mpm_event:notice] [pid 40085:tid 40085] AH00489: SIGHUP received. Doing graceful restart
[Fri Oct 14 23:07:49.864759 2022] [lbmethod:heartbeat:notice] [pid 40085:tid 40085] AH02282: No slotmem from mod_heartbeat
[Fri Oct 14 23:07:49.867004 2022] [mpm_event:notice] [pid 40085:tid 40085] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 14 23:07:49.867910 2022] [core:notice] [pid 40085:tid 40085] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Fri Oct 14 23:07:57.390273 2022] [mpm_event:notice] [pid 40085:tid 40085] AH00482: caught SIGHUP, shutting down gracefully
[Fri Oct 14 23:08:01.033503 2022] [core:notice] [pid 42514:tid 42514] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 14 23:08:01.034473 2022] [core:notice] [pid 42514:tid 42514] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 14 23:08:01.045339 2022] [lbmethod:heartbeat:notice] [pid 42514:tid 42514] AH02282: No slotmem from mod_heartbeat
[Fri Oct 14 23:08:01.057023 2022] [mpm_event:notice] [pid 42514:tid 42514] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 14 23:08:01.057048 2022] [core:notice] [pid 42514:tid 42514] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Fri Oct 14 23:09:13.005264 2022] [mpm_event:notice] [pid 42514:tid 42514] AH00482: caught SIGHUP, shutting down gracefully
[Fri Oct 14 23:09:17.047092 2022] [core:notice] [pid 42825:tid 42825] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri Oct 14 23:09:17.048743 2022] [suexec:notice] [pid 42825:tid 42825] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Oct 14 23:09:17.450867 2022] [lbmethod:heartbeat:notice] [pid 42825:tid 42825] AH02282: No slotmem from mod_heartbeat
[Fri Oct 14 23:09:17.469357 2022] [mpm_event:notice] [pid 42825:tid 42825] AH00489: Apache/2.4.51 (Rocky Linux) configured -- resuming normal operations
[Fri Oct 14 23:09:17.469382 2022] [core:notice] [pid 42825:tid 42825] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
```

Figure 3.19: /var/log/httpd/error_log

19. Выполните команду `semanage port -a -t http_port_t -p tcp 81`

После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке. (рис. 3.20)

```
[root@asbaklashov audit]# 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@asbaklashov audit]#
```

Figure 3.20: 81

Порт 81 был в списке до этого, поэтому сбоя не было.

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

Сервер запускался и до этого. Он бы не запустился, если бы порта 81 изначально не было в списке.

21. Верните 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`. Вы должны увидеть содержимое файла — слово «test». (рис. 3.21, рис. 3.22)

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

Figure 3.21: «test»

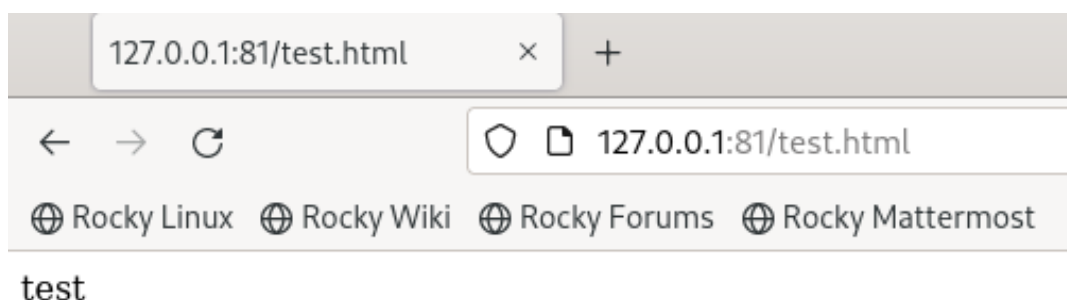


Figure 3.22: «test»

22. Исправьте обратно конфигурационный файл apache, вернув `Listen 80`. (рис. 3.23)


```
httpd.conf [----] 9 L:[ 32+15 47/360] *(2025/12024b) 0010 0x00A
# 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
```

Figure 3.23: Listen 80

23. Удалите привязку http_port_t к 81 порту: `semanage port -d -t http_port_t -p tcp 81` (рис. 3.24)

```
[root@asbaklashov conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Figure 3.24: 81

Не вышло

24. Удалите файл `/var/www/html/test.html` (рис. 3.25)

```
[root@asbaklashov conf]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@asbaklashov conf]#
```

Figure 3.25: Удалите файл

4 Вывод

В результате выполнения работы я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.

5 Библиография

1. Лабораторная работа № 6. Мандатное разграничение прав в Linux. - 5 с. [Электронный ресурс]. М. URL: Лабораторная работа №6 (Дата обращения: 15.10.2022).
2. Rocky Linux Documentation. [Электронный ресурс]. М. URL: Rocky Linux Documentation (Дата обращения: 15.10.2022).