

Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Исаев Булат Абубакарович НПИбд-01-22

Содержание

1	Цель работы	1
2	Выполнение лабораторной работы.....	1
3	Выводы	9
Список литературы		Ошибка! Закладка не определена.

1 Цель работы

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

2 Выполнение лабораторной работы

1. Убеждаюсь, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus*. Запускаю веб-сервер командой *service httpd start* и проверяю его статус командой *service httpd status* (рис. 1)

```
baisaev@localhost:~ — /bin/systemctl status httpd.service
[baisaev@localhost ~]$ getenforce
Enforcing
[baisaev@localhost ~]$ 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
[baisaev@localhost ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2024-04-27 16:51:48 +04; 45s ago
     Docs: man:httpd.service(8)
   Main PID: 98842 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
   Tasks: 213 (limit: 65577)
  Memory: 23.2M
    CPU: 85ms
   CGroup: /system.slice/httpd.service
           └─98842 /usr/sbin/httpd -DFOREGROUND
```

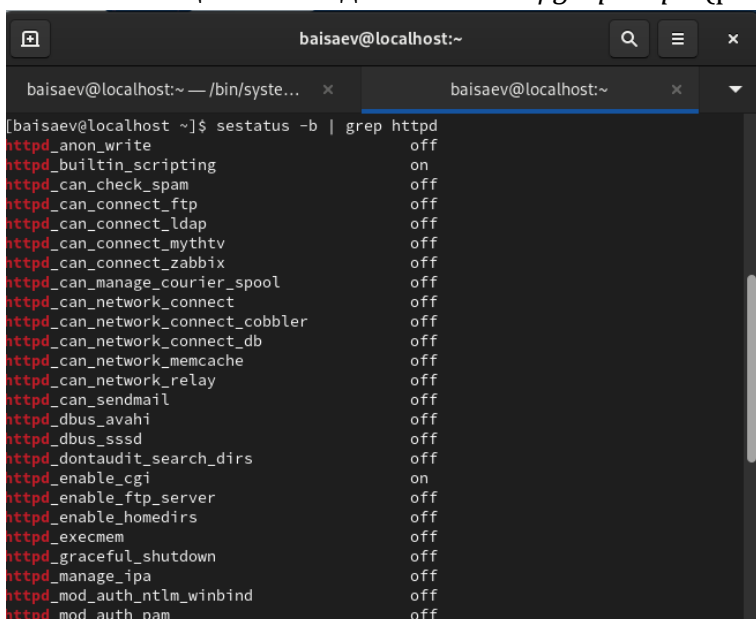
Рис. 1: Запуск и проверка веб-сервера

2. Определяю контекст безопасности веб-сервера с помощью команды `ps auxZ | grep httpd` (рис. 2)

```
baisaev@localhost:~ — /bin/systemctl status httpd.service
[baisaev@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 98842 0.0 0.1 20128 11468 ?
Ss 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98843 0.0 0.0 21612 7268 ?
S 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98844 0.0 0.1 1538136 10940 ?
Sl 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98845 0.0 0.1 1538136 10940 ?
Sl 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 98846 0.0 0.1 1669272 12988 ?
Sl 16:51 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 baisaev 99101 0.0 0.0 236
232 9076 pts/1 S+ 16:52 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 baisaev 99175 0.0 0.0 221
688 2392 pts/0 S+ 16:56 0:00 grep --color=auto httpd
[baisaev@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 98842 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98843 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98844 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98845 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 98846 ? 00:00:00 httpd
[baisaev@localhost ~]$
```

Рис. 2: Контекст безопасности веб-сервера

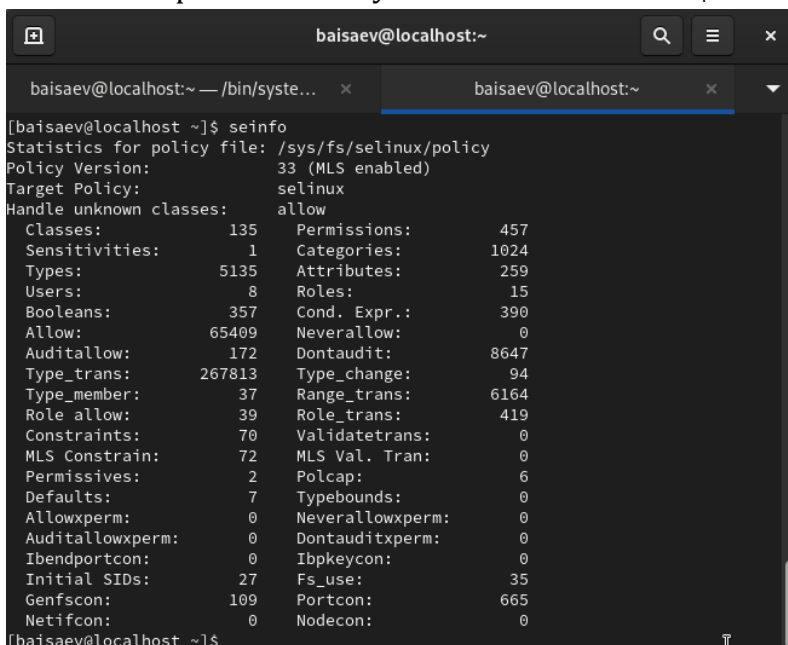
3. Просматриваю текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd` (рис. 3)



```
baisaev@localhost:~$ 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
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
```

Рис. 3: Состояние переключателей SELinux

4. Смотрю статистику по политике с помощью команды `seinfo` (рис. 4)



```
baisaev@localhost:~$ 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: 5135 Attributes: 259
Users: 8 Roles: 15
Booleans: 357 Cond. Expr.: 390
Allow: 65409 Neverallow: 0
Auditallow: 172 Dontaudit: 8647
Type_trans: 267813 Type_change: 94
Type_member: 37 Range_trans: 6164
Role_allow: 39 Role_trans: 419
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
Ibndportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0
baisaev@localhost ~$
```

Рис. 4: Статистика по политике

5. Определяю тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`. Аналогично для директории /var/www/html (рис. 5)

```
[baisaev@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 13
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 13
:35 html
[baisaev@localhost ~]$ ls -lZ /var/www/html
итого 0
[baisaev@localhost ~]$
```

Рис. 5: Определение типа файлов и папок

6. Создаю файл /var/www/html/test.html и записываю следующий html-код (рис. 6)

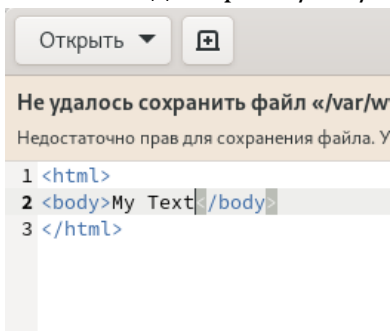


Рис. 6: test.html

7. Проверяю контекст созданного файла командой `ps auxZ | grep test.html` (рис. 7)

```
[root@localhost ~]# ps auxZ | grep myfile.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 100374 0.0 0.0 22182
4 2404 pts/0 S+ 17:42 0:00 grep --color=auto myfile.html
[root@localhost ~]#
```

Рис. 7: Контекст файла

8. Проверяю в браузере, что файл успешно отображается (рис. 8)

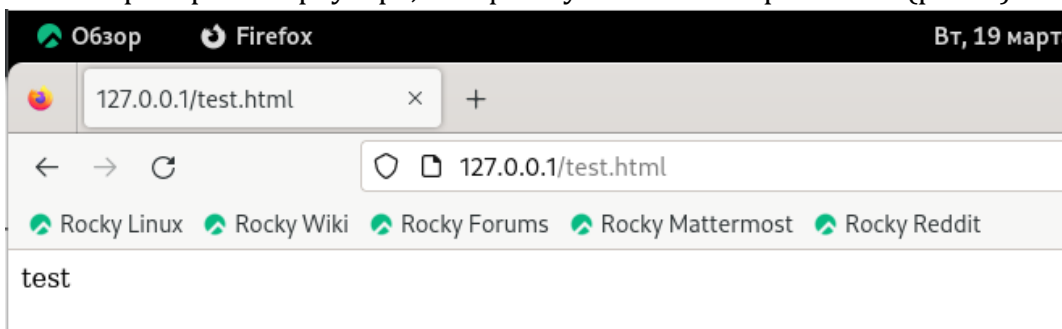


Рис. 8: Проверка в браузере

9. Изучаю справку man по командам httpd и selinux, также проверяю контекст файла командой `ls -Z /var/www/html/test.html` (рис. 9)

```
[root@localhost ~]# man httpd
[root@localhost ~]# man selinux
[root@localhost ~]# ls -Z /var/www/html/myfile.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/myfile.html
[root@localhost ~]#
```

Рис. 9: Изучение man, проверка контекста

10. Изменяю контекст файла test.html командой `chcon -t samba_share_t /var/www/html/test.html`. После, проверяю его и открываю веб-страницу - нет доступа (рис. 10)

```
[root@localhost ~]# tail /var/log/messages
Apr 27 17:29:08 localhost cupsd[896]: REQUEST localhost - - "POST / HTTP/1.1" 20
0 186 Renew-Subscription successful-ok
Apr 27 17:31:46 localhost systemd[2077]: dbus-:1.2-org.gnome.gedit@6.service: Co
nsumed 5.422s CPU time.
Apr 27 17:43:25 localhost systemd[2077]: Started dbus-:1.2-org.gnome.gedit@7.ser
vice.
Apr 27 17:43:26 localhost gnome-shell[2184]: meta_window_set_stack_position_no_s
ync: assertion 'window->stack_position >= 0' failed
Apr 27 17:43:39 localhost systemd[2077]: Started dbus-:1.2-org.gnome.gedit@8.ser
vice.
Apr 27 17:43:39 localhost gnome-shell[2184]: meta_window_set_stack_position_no_s
ync: assertion 'window->stack_position >= 0' failed
Apr 27 17:45:28 localhost systemd[2077]: Started dbus-:1.2-org.gnome.gedit@9.ser
vice.
Apr 27 17:45:29 localhost gnome-shell[2184]: meta_window_set_stack_position_no_s
ync: assertion 'window->stack_position >= 0' failed
Apr 27 17:45:42 localhost systemd[2077]: Started Application launched by gnome-s
hell.
Apr 27 17:45:45 localhost rtkit-daemon[748]: Successfully made thread 100628 of
process 100494 (/usr/lib64/firefox/firefox) owned by '1000' RT at priority 10.
[root@localhost ~]#
```

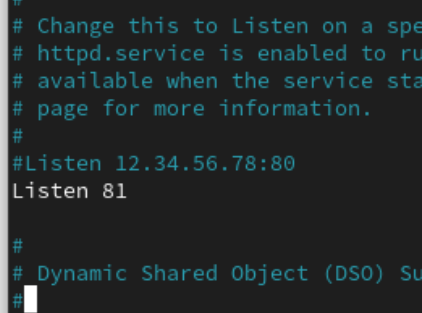
Рис. 10: Изменение контекста

11. Просматриваю системный лог-файл командой `tail /var/log/messages` (рис. 11)

```
ать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль
политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
с 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#0
12
Mar 19 18:56:40 vlbarsegyan systemd[1]: dbus-:1.1-org.fedoraproject.Setroublsh
ootPrivileged@0.service: Deactivated successfully.
Mar 19 18:56:40 vlbarsegyan systemd[1]: dbus-:1.1-org.fedoraproject.Setroublsh
ootPrivileged@0.service: Consumed 1.149s CPU time.
Mar 19 18:56:40 vlbarsegyan systemd[1]: setroublshood.service: Deactivated su
ccessfully.
[root@vlbarsegyan vlbarsegyan]#
```

Рис. 11: Системный лог-файл

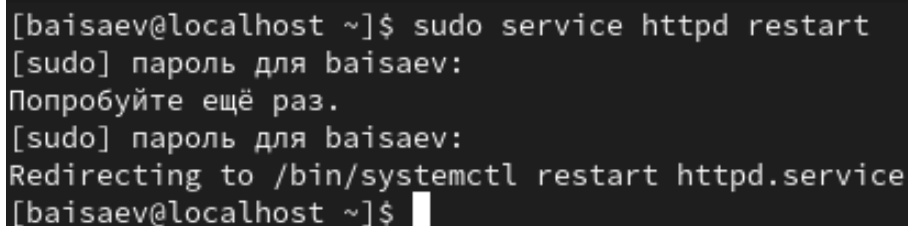
12. В файле `/etc/httpd/conf/httpd.conf` меняю порт на 81 (рис. 12)



```
# Change this to Listen on a specific IP address.  
# httpd.service is enabled to run as daemon.  
# available when the service starts.  
# page for more information.  
#  
#Listen 12.34.56.78:80  
Listen 81  
  
#  
# Dynamic Shared Object (DSO) Support
```

Рис. 12: Смена порта

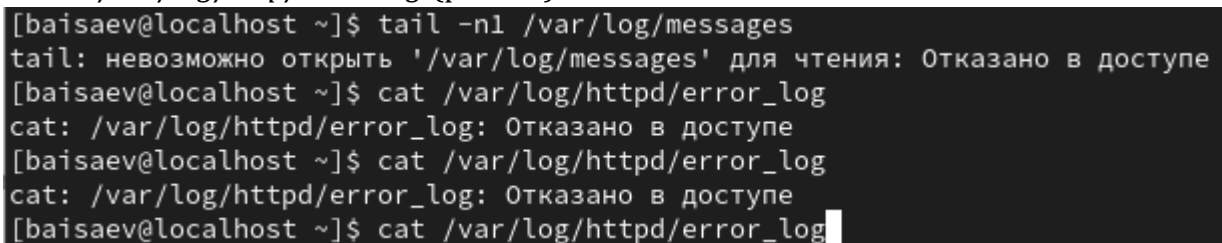
13. Перезагружаю веб-сервер - получен сбой (рис. 13)



```
[baisaev@localhost ~]$ sudo service httpd restart  
[sudo] пароль для baisaev:  
Попробуйте ещё раз.  
[sudo] пароль для baisaev:  
Redirecting to /bin/systemctl restart httpd.service  
[baisaev@localhost ~]$
```

Рис. 13: Сбой веб-сервера

14. Анализирую лог-файлы командами `tail -nl /var/log/messages` и `cat /var/log/httpd/error_log` (рис. 14)



```
[baisaev@localhost ~]$ tail -nl /var/log/messages  
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе  
[baisaev@localhost ~]$ cat /var/log/httpd/error_log  
cat: /var/log/httpd/error_log: Отказано в доступе  
[baisaev@localhost ~]$ cat /var/log/httpd/error_log  
cat: /var/log/httpd/error_log: Отказано в доступе  
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
```

Рис. 14: Проверка лог-файлов

15. Также проверяю лог-файл `/var/log/http/access_log` (рис. 15)

```
[baisaev@localhost ~]$ tail -n1 /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Отказано в доступе
[baisaev@localhost ~]$
```

Рис. 15: Проверка лог-файлов

16. Также проверяю лог-файл */var/log/audit/audit.log*. (рис. 16)

```
[baisaev@localhost ~]$ tail -n1 /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/audit.log
cat: /var/log/httpd/audit.log: Отказано в доступе
[baisaev@localhost ~]$
```

Рис. 16: Проверка лог-файлов

17. Выполняю команду *semanage port -a -t http_port_t -p tcp 81* и проверяю список портов командой *semanage port -l | grep http_port_t* - порт 81 появился в списке (рис. 17)

```
[baisaev@localhost ~]$ cat /var/log/httpd/error_log
cat: /var/log/httpd/error_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/access_log
cat: /var/log/httpd/access_log: Отказано в доступе
[baisaev@localhost ~]$ cat /var/log/httpd/audit.log
cat: /var/log/httpd/audit.log: Отказано в доступе
[baisaev@localhost ~]$ semanage port -a -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[baisaev@localhost ~]$ semanage port -l | grep httpd restart
grep: restart: Нет такого файла или каталога
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[baisaev@localhost ~]$ sudo service httpd restart
[sudo] пароль для baisaev:
Redirecting to /bin/systemctl restart httpd.service
```

Рис. 17: Добавление порта 81 в список

18. Возвращаю контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`, введя `chcon -t httpd_sys_content_t /var/www/html/test.html`. Перезапускаю веб-сервер командой `sudo service httpd restart` (рис. 18)

```
[baisaev@localhost ~]$ chcon -t httpd_sys_content_t /var/www/html/myfile.html
[baisaev@localhost ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[baisaev@localhost ~]$
```

Рис. 18: Возвращение контекста и перезапуск веб-сервера

19. Возвращаю порт 80 в конфигурационном файле (рис. 19)

```
#
# Change this to Listen on a :
# httpd.service is enabled to
# available when the service :
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO)
```

Рис. 19: Смена порта на 80

20. Удаляю привязку http_port_t к 81 порту командой *semanage port -d -t http_port_t -p tcp 81* и удаляю файл test.html командой *rm /var/www/html/test.html* (рис. 20)

```
[baisaev@localhost ~]$ semanage port -d -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[baisaev@localhost ~]$ rm /var/www/html/myfile.html
rm: удалить защищённый от записи пустой обычный файл '/var/www/html/myfile.html'
? y
rm: невозможно удалить '/var/www/html/myfile.html': Отказано в доступе
[baisaev@localhost ~]$
```

Рис. 20: Удаление привязки к 81 порту и удаление html-файла

3. Выводы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux, поработал с веб-сервером Apache