

# **Отчёт по лабораторной работе №6**

**Знакомство с SELinux**

Ласурия Данил

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Подготовка . . . . .	5
2.2	Изучение механики SetUID . . . . .	5
<b>3</b>	<b>Выводы</b>	<b>13</b>
	<b>Список литературы</b>	<b>14</b>

# List of Figures

2.1	запуск http . . . . .	6
2.2	контекст безопасности http . . . . .	6
2.3	переключатели SELinux для http . . . . .	7
2.4	создание html-файла и доступ по http . . . . .	8
2.5	ошибка доступа после изменения контекста . . . . .	9
2.6	лог ошибок . . . . .	10
2.7	переключение порта . . . . .	11
2.8	доступ по http на 81 порт . . . . .	12

# 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

### 2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

### 2.2 Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`.

```
lasuriyadr@localhost:/etc
File Edit View Search Terminal Help
[root@localhost etc]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost etc]# 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 preset: enabled)
   Active: active (running) since Sat 2022-10-15 20:45:33 MSK; 4s ago
     Docs: man:httpd.service(8)
   Main PID: 39918 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 23517)
    Memory: 25.6M
    CGroup: /system.slice/httpd.service
            └─39918 /usr/sbin/httpd -DFOREGROUND
              └─39920 /usr/sbin/httpd -DFOREGROUND
                └─39921 /usr/sbin/httpd -DFOREGROUND
                  └─39922 /usr/sbin/httpd -DFOREGROUND
                    └─39923 /usr/sbin/httpd -DFOREGROUND

Oct 15 20:45:33 localhost.localdomain systemd[1]: Starting The Apache HTTP Server:
Oct 15 20:45:33 localhost.localdomain httpd[39918]: AH00558: httpd: Could not r
Oct 15 20:45:33 localhost.localdomain systemd[1]: Started The Apache HTTP Server:
Oct 15 20:45:33 localhost.localdomain httpd[39918]: Server configured, listenin
lines 1-19/19 (END)
```

Figure 2.1: запуск http

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`

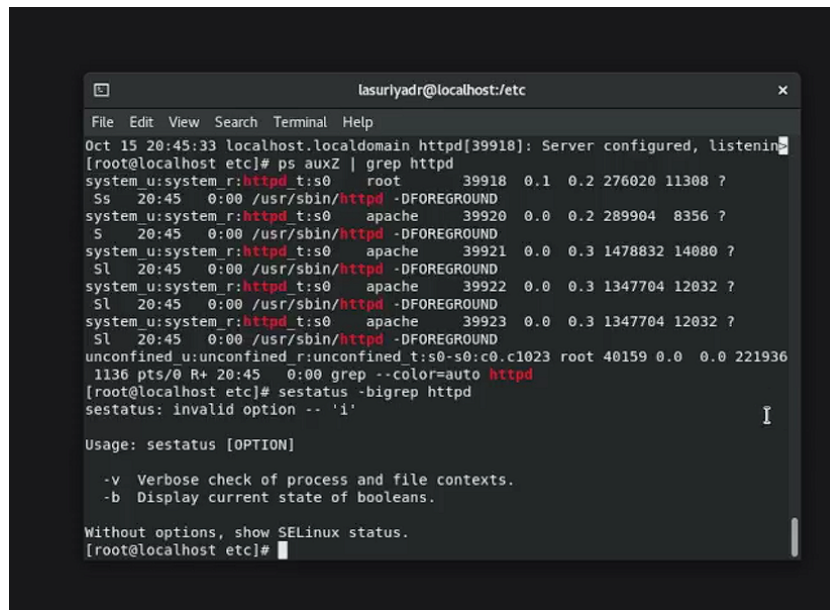
```
lasuriyadr@localhost:/etc
File Edit View Search Terminal Help
└─39918 /usr/sbin/httpd -DFOREGROUND
└─39920 /usr/sbin/httpd -DFOREGROUND
└─39921 /usr/sbin/httpd -DFOREGROUND
└─39922 /usr/sbin/httpd -DFOREGROUND
└─39923 /usr/sbin/httpd -DFOREGROUND

Oct 15 20:45:33 localhost.localdomain systemd[1]: Starting The Apache HTTP Server:
Oct 15 20:45:33 localhost.localdomain httpd[39918]: AH00558: httpd: Could not r
Oct 15 20:45:33 localhost.localdomain systemd[1]: Started The Apache HTTP Server:
Oct 15 20:45:33 localhost.localdomain httpd[39918]: Server configured, listenin
[root@localhost etc]# ps auxZ | grep httpd
system u:system r:httpd t:s0 root 39918 0.1 0.2 276020 11308 ?
Ss 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 39920 0.0 0.2 289904 8356 ?
S 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 39921 0.0 0.3 1478832 14080 ?
Sl 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 39922 0.0 0.3 1347704 12032 ?
Sl 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 39923 0.0 0.3 1347704 12032 ?
Sl 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 40159 0.0 0.0 221936
1136 pts/0 R+ 20:45 0:00 grep --color=auto httpd
[root@localhost etc]#
```

Figure 2.2: контекст безопасности http

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из

них находятся в положении «off».



```
lasuriyadr@localhost:/etc
File Edit View Search Terminal Help
Oct 15 20:45:33 localhost.localdomain httpd[39918]: Server configured, listening
[root@localhost etc]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 39918 0.1 0.2 276020 11308 ?
Ss 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39920 0.0 0.2 289904 8356 ?
S 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39921 0.0 0.3 1478832 14080 ?
Sl 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39922 0.0 0.3 1347704 12032 ?
Sl 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 39923 0.0 0.3 1347704 12032 ?
Sl 20:45 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40159 0.0 0.0 221936
1136 pts/0 R+ 20:45 0:00 grep --color=auto httpd
[root@localhost etc]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

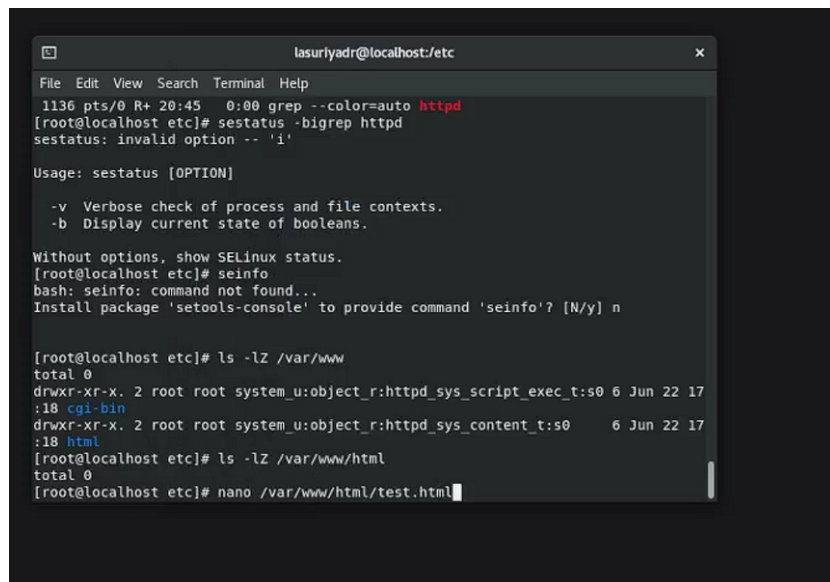
Usage: sestatus [OPTION]
  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[root@localhost etc]#
```

Figure 2.3: переключатели SELinux для http

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. В директории изначально нет файлов.
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Создавать файлы может только root.
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: Test

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`.
11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.



```
lasuriyadr@localhost/etc
File Edit View Search Terminal Help
1136 pts/0 R+ 20:45 0:00 grep --color=auto httpd
[root@localhost etc]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]
  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[root@localhost etc]# seinfo
bash: seinfo: command not found...
Install package 'setools-console' to provide command 'seinfo'? [N/y] n

[root@localhost etc]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Jun 22 17
:18 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Jun 22 17
:18 html
[root@localhost etc]# ls -lZ /var/www/html
total 0
[root@localhost etc]# nano /var/www/html/test.html
```

Figure 2.4: создание html-файла и доступ по http

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.
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`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.
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: Forbidden You don't have permission to access /test.html on this server. При изменении контекста файл стал считаться чужим для http и программа не может его прочитать.

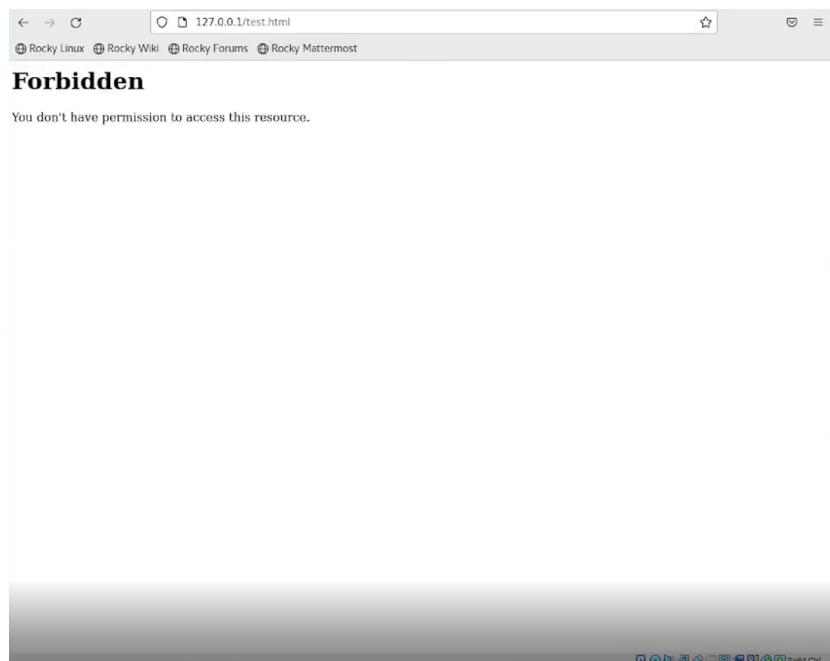


Figure 2.5: ошибка доступа после изменения контекста

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.

```
lasuriyadr@localhost:/etc
File Edit View Search Terminal Help
:system_r:httpd_t:s0 key=(null) ARCH=x86_64 SYSCALL=lstat AUID="unset" UID="apache"
GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache"
FSGID="apache"
type=PROCTITLE msg=audit(1665856238.949:208): proctitle=2F7573722F7362696E2F68747
47064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1665856259.296:209): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init t:s0 msg='unit=fprintd comm="systemd" exe
="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root"
AUID="unset"
type=USER_AUTH msg=audit(1665856261.359:210): pid=41576 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentica
tion grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdoma
in addr=? terminal=pts/1 res=success' UID="lasuriyadr" AUID="lasuriyadr"
type=USER_ACCT msg=audit(1665856261.360:211): pid=41576 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting
grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/su" hostname=localhost
.localdomain addr=? terminal=pts/1 res=success' UID="lasuriyadr" AUID="lasuriyadr"
type=CRED_ACQ msg=audit(1665856261.365:212): pid=41576 uid=1000 auid=1000 ses=3 s
ubj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred gra
ntors=pam_unix acct="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=
? terminal=pts/1 res=success' UID="lasuriyadr" AUID="lasuriyadr"
type=USER_START msg=audit(1665856261.376:213): pid=41576 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session o
pen grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask,pam_xauth acct
="root" exe="/usr/bin/su" hostname=localhost.localdomain addr=? terminal=pts/1 re
s=success' UID="lasuriyadr" AUID="lasuriyadr"
type=SERVICE_START msg=audit(1665856263.911:214): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init t:s0 msg='unit=dnf-makecache comm="system
d" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="r
oot" AUID="unset"
type=SERVICE_STOP msg=audit(1665856263.911:215): pid=1 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:init t:s0 msg='unit=dnf-makecache comm="systemd"
exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="r
oot" AUID="unset"
[root@localhost etc]#
```

Figure 2.6: лог ошибок

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.



```
GNU nano 2.9.8 /etc/httpd/httpd.conf Modified
sg=aud
u:unco ServerName test.ru
m unix Listen 81
al=pts
sg=aud
u:unco
ix,pam
r=? te

g=audi
:uncon
cct="r
res=s
msg=au
u:unc
keyin
r/bin/
lasurl
RT msg
=syste
/syste
t"
p msg=
```

Figure 2.7: переключение порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные
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.
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.
20. Попробуйте запустить веб-сервер Apache ещё раз.
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».

```

[root@localhost etc]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module
               *,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81
[root@localhost etc]# 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

```

Figure 2.8: доступ по http на 81 порт

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
23. Удалите привязку http\_port\_t к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

## **3 Выводы**

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.

# Список литературы

1. SELinux в CentOS
2. Веб-сервер Apache