

# **Лабораторная работа №6**

**Мандатное разграничение прав в Linux**

Аскеров Александр Эдуардович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>3</b>	<b>Выводы</b>	<b>14</b>
	<b>Список литературы</b>	<b>15</b>

## Список иллюстраций

2.1	Проверка SELinux . . . . .	5
2.2	Проверка работы веб-сервера . . . . .	5
2.3	Контекст безопасности веб-сервера . . . . .	6
2.4	Переключатели SELinux . . . . .	6
2.5	Статистика по политике . . . . .	7
2.6	Тип файлов и поддиректорий . . . . .	7
2.7	Тип файлов . . . . .	7
2.8	Круг пользователей с разрешением . . . . .	8
2.9	html-файл . . . . .	8
2.10	Контекст файла . . . . .	8
2.11	Изменение контекста . . . . .	8
2.12	Проверка контекста . . . . .	9
2.13	Системный лог-файл . . . . .	9
2.14	Файл audit.log . . . . .	10
2.15	Изменение порта . . . . .	10
2.16	Файл messages . . . . .	11
2.17	Файл access_log . . . . .	11
2.18	Файл audit.log . . . . .	11
2.19	Управление портами . . . . .	12
2.20	Управление портами . . . . .	12
2.21	Возврат контекста . . . . .	12
2.22	Изменение порта . . . . .	12
2.23	Удаление привязки . . . . .	12
2.24	Удаление файла . . . . .	13

# 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

Войдём в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.

```
[aeaskerov@aeaskerov ~]$ getenforce
Enforcing
[aeaskerov@aeaskerov ~]$ 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
[aeaskerov@aeaskerov ~]$
```

Рис. 2.1: Проверка SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает.

```
[aeaskerov@aeaskerov ~]$ 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 Wed 2024-04-24 14:54:46 MSK; 34min ago
     Docs: man:httpd.service(8)
   Main PID: 1441 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served: 0"
   Tasks: 213 (limit: 23035)
```

Рис. 2.2: Проверка работы веб-сервера

Найдём веб-сервер Apache в списке процессов, определим его контекст безопасности.

```
[aeaskerov@aeaskerov ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 1441 0.0 0.3 20340 11700 ?
Ss 14:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1565 0.0 0.2 21676 7644 ?
S 14:54 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1566 0.1 0.2 1538248 11176 ?
Sl 14:54 0:02 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1567 0.1 0.3 1669384 13220 ?
Sl 14:54 0:02 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 1568 0.1 0.2 1538248 11172 ?
Sl 14:54 0:02 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aeasker+ 4594 0.0 0.0 221
796 2372 pts/0 S+ 15:30 0:00 grep --color=auto httpd
[aeaskerov@aeaskerov ~]$
```

Рис. 2.3: Контекст безопасности веб-сервера

Посмотрим текущее состояние переключателей SELinux для Apache.

```
[aeaskerov@aeaskerov ~]$ 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
```

Рис. 2.4: Переключатели SELinux

Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей, типов.

```

[aeaskerov@aeaskerov ~]$ 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
Ibendportcon:            0        Ibpkeycon:            0
Initial SIDs:            27       Fs_use:               35
Genfscon:                109      Portcon:              665
Netifcon:                0        Nodecon:              0
[aeaskerov@aeaskerov ~]$

```

Рис. 2.5: Статистика по политике

Определим тип файлов и поддиректорий, находящихся в директории /var/www.

```

[aeaskerov@aeaskerov ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12
:35 html
[aeaskerov@aeaskerov ~]$

```

Рис. 2.6: Тип файлов и поддиректорий

Определим тип файлов, находящихся в директории /var/www/html.

```

[aeaskerov@aeaskerov ~]$ ls -lZ /var/www/html
total 0
[aeaskerov@aeaskerov ~]$

```

Рис. 2.7: Тип файлов

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[aeaskerov@aeaskerov ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Oct 28 12
:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Oct 28 12
:35 html
[aeaskerov@aeaskerov ~]$
```

Рис. 2.8: Круг пользователей с разрешением

Создадим от имени суперпользователя html-файл /var/www/html/test.html следующего содержания.

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

Рис. 2.9: html-файл

Проверим контекст созданного файла. Запишем контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

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

Рис. 2.10: Контекст файла

Обратимся к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.

Изучим справку `man httpd_selinux`.

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`.

```
[root@aeaskerov html]# chcon -t samba_share_t /var/www/html/test.html
[root@aeaskerov html]#
```

Рис. 2.11: Изменение контекста



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

Рис. 2.12: Проверка контекста

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получено сообщение об ошибке.

Проанализируем ситуацию. Просмотрим log-файлы веб-сервера Apache. Также посмотрим системный лог-файл.

```
[root@aeaskerov html]# tail /var/log/messages
Apr 24 15:39:59 aeaskerov systemd[3308]: Started Portal service.
Apr 24 15:40:01 aeaskerov rtkit-daemon[938]: Successfully made thread 43087 of p
rocess 42845 (/usr/lib64/firefox/firefox) owned by '1000' RT at priority 10.
Apr 24 15:41:56 aeaskerov firefox.desktop[42845]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:41:56 aeaskerov firefox.desktop[42845]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:41:57 aeaskerov systemd[3308]: app-gnome-firefox-42845.scope: Consumed
48.141s CPU time.
Apr 24 15:46:53 aeaskerov systemd[3308]: Started Application launched by gnome-s
hell.
Apr 24 15:46:55 aeaskerov rtkit-daemon[938]: Successfully made thread 43458 of p
rocess 43346 (/usr/lib64/firefox/firefox) owned by '1000' RT at priority 10.
Apr 24 15:47:33 aeaskerov firefox.desktop[43346]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:47:33 aeaskerov firefox.desktop[43346]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:47:34 aeaskerov systemd[3308]: app-gnome-firefox-43346.scope: Consumed
19.510s CPU time.
[root@aeaskerov html]#
```

Рис. 2.13: Системный лог-файл

Посмотрим файл `/var/log/audit/audit.log`.

```
[root@aeaskerov html]# tail /var/log/audit/audit.log
type=CRED_ACQ msg=audit(1713962220.439:203): pid=42759 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred g
rantors=pam_unix acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/p
ts/0 res=success'UID="aeaskerov" AUID="aeaskerov"
type=USER_START msg=audit(1713962220.498:204): pid=42759 uid=1000 auid=1000 ses=
3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session
_open grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask
,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 r
es=success'UID="aeaskerov" AUID="aeaskerov"
type=BPF msg=audit(1713962220.526:205): prog-id=40 op=LOAD
type=BPF msg=audit(1713962220.526:206): prog-id=41 op=LOAD
type=SERVICE_START msg=audit(1713962220.582:207): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="
systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1713962247.069:208): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" ex
e="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=BPF msg=audit(1713962247.103:209): prog-id=39 op=UNLOAD
type=SERVICE_STOP msg=audit(1713962250.621:210): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="s
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
UID="root" AUID="unset"
type=BPF msg=audit(1713962250.659:211): prog-id=41 op=UNLOAD
type=BPF msg=audit(1713962250.659:212): prog-id=40 op=UNLOAD
[root@aeaskerov html]#
```

Рис. 2.14: Файл audit.log

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 найдём строчку Listen 80 и заменим её на Listen 81.



Рис. 2.15: Изменение порта

Выполним перезапуск веб-сервера Apache. Произошёл сбой из-за изменения порта.

Проанализируем лог-файлы.

```
[root@aeaskerov html]# tail -l /var/log/messages
Apr 24 15:41:56 aeaskerov firefox.desktop[42845]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:41:57 aeaskerov systemd[3308]: app-gnome-firefox-42845.scope: Consumed
48.141s CPU time.
Apr 24 15:46:53 aeaskerov systemd[3308]: Started Application launched by gnome-s
hell.
Apr 24 15:46:55 aeaskerov rtkit-daemon[938]: Successfully made thread 43458 of p
rocess 43346 (/usr/lib64/firefox/firefox) owned by '1000' RT at priority 10.
Apr 24 15:47:33 aeaskerov firefox.desktop[43346]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:47:33 aeaskerov firefox.desktop[43346]: [ERROR viaduct::backend::ffi]
Missing HTTP status
Apr 24 15:47:34 aeaskerov systemd[3308]: app-gnome-firefox-43346.scope: Consumed
19.510s CPU time.
Apr 24 15:50:15 aeaskerov gnome-shell[3411]: Source ID 12811 was not found when
attempting to remove it
Apr 24 15:50:15 aeaskerov gnome-shell[3411]: Window manager warning: Buggy clien
t sent a _NET_ACTIVE_WINDOW message with a timestamp of 0 for 0x12000f5
Apr 24 15:54:07 aeaskerov cupsd[1232]: REQUEST localhost - - "POST / HTTP/1.1" 2
00 188 Renew-Subscription successful-ok
[root@aeaskerov html]#
```

Рис. 2.16: Файл messages

Просмотрим файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясним, в каких файлах появились записи.

```
[root@aeaskerov html]# tail /var/log/http/access_log
tail: cannot open '/var/log/http/access_log' for reading: No such file or direct
ory
[root@aeaskerov html]#
```

Рис. 2.17: Файл access\_log

```
[root@aeaskerov html]# tail /var/log/audit/audit.log
type=CRED_ACQ msg=audit(1713962220.439:203): pid=42759 uid=1000 auid=1000 ses=3
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred g
rants=pam_unix acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/p
ts/0 res=success'UID="aeaskerov" AUID="aeaskerov"
type=USER_START msg=audit(1713962220.498:204): pid=42759 uid=1000 auid=1000 ses=
3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session
_open grants=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask
,pam_xauth acct="root" exe="/usr/bin/su" hostname=? addr=? terminal=/dev/pts/0 r
es=success'UID="aeaskerov" AUID="aeaskerov"
type=BPF msg=audit(1713962220.526:205): prog-id=40 op=LOAD
type=BPF msg=audit(1713962220.526:206): prog-id=41 op=LOAD
type=SERVICE_START msg=audit(1713962220.582:207): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="
systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1713962247.069:208): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" ex
e="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=BPF msg=audit(1713962247.103:209): prog-id=39 op=UNLOAD
type=SERVICE_STOP msg=audit(1713962250.621:210): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-hostnamed comm="s
ystemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
UID="root" AUID="unset"
type=BPF msg=audit(1713962250.659:211): prog-id=41 op=UNLOAD
type=BPF msg=audit(1713962250.659:212): prog-id=40 op=UNLOAD
[root@aeaskerov html]#
```

Рис. 2.18: Файл audit.log

Выполним следующую команду.

```
[root@aeaskerov html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@aeaskerov html]#
```

Рис. 2.19: Управление портами

```
[root@aeaskerov html]# 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@aeaskerov html]#
```

Рис. 2.20: Управление портами

Порт 81 появился в списке.

Попробуем запустить веб-сервер Apache ещё раз. Теперь он запустился.

Вернём контекст httpd\_sys\_content\_t к файлу /var/www/html/test.html.

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

Рис. 2.21: Возврат контекста

После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`.

Мы видим содержимое файла – слово «test».

Исправим обратно конфигурационный файл apache, вернув Listen 80.



```
3 Listen 80|
```

Рис. 2.22: Изменение порта

Удалим привязку http\_port\_t к 81-му порту.

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

Рис. 2.23: Удаление привязки

Удалим файл /var/www/html/test.html.

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

Рис. 2.24: Удаление файла

## 3 Выводы

Развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux.

Проверена работа SELinux на практике совместно с веб-сервером Apache.

# Список литературы

1. Веб-сервер Apache