

# **Отчёт по лабораторной работе №6**

**Мандатное разграничение прав в Linux**

Морозов Михаил Евгеньевич

# Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	10
	Список литературы	11

## **Список иллюстраций**

## Список таблиц

# 1 Цель работы

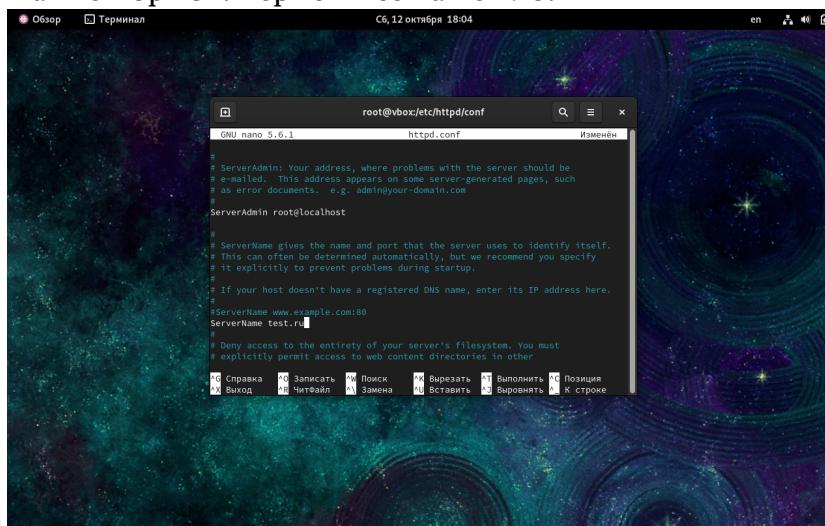
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

## 2 Теоретическое введение

В SELinux права доступа определяются самой системой при помощи специально определённых политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux: через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила SELinux «прозрачны» для приложений, и не требуется никакой их модификации. В состав некоторых дистрибутивов входят готовые политики, в которых права могут определяться на основе совпадения типов процесса (субъекта) и файла (объекта) — это основной механизм SELinux. Две других формы контроля доступа — доступ на основе ролей и на основе многоуровневой системы безопасности. [1]

### 3 Выполнение лабораторной работы

Убедимся, что SELinux работает в режиме enforcing политики targeted. Обратимся к веб-серверу и убедимся, что он работает. Найдем apache в списке процессов. Посмотрим статистику по политике. Определим тип файлов и директорий в /var/www. Посмотрим список пользователей. Создадим от имени root файл в /var/www/html. Попробуем посмотреть файл в браузере. Изменим контекст файла. Добавим на прослушивание порт 81. Вернем все как было.



Результаты работы команд 1 (рис. ??)

2 (рис. ??)

```
roo@vbox:/etc/httpd/conf$ su
bash: su: команда не найдена...
Аналогичная команда: 'su'
roo@vbox:/etc/httpd/conf$ su
Пароль:
[roo@vbox conf]$ ps auxZ | grep httpd
bash: grep: команда не найдена...
[roo@vbox conf]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3367 0.0 0.6 21312 11504 ? Ss 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3368 0.0 0.4 23044 7236 ? S 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3371 0.0 0.6 983596 11092 ? Sl 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3372 0.0 0.7 1113732 13472 ? Sl 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3374 0.0 0.6 982596 11092 ? Sl 18:12 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023 root 2648 0.0 0.5 237760 9244 pts/0 S+ 18:15 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023 root 3743 0.0 0.1 221820 2432 pts/1 S+ 18:16 0:00 grep --color=auto httpd

[roo@vbox conf]$ systemctl status -bigrep httpd
bash: systemctl: команда не найдена...
[roo@vbox conf]$ 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.
[roo@vbox conf]$ 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.
[roo@vbox conf]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
```

3 (рис. ??)

```
roo@vbox:/etc/httpd/conf$ systemctl status httpd.service
roo@vbox:/etc/httpd/conf$
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_issd 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_ftp off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ftp off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_com off
httpd_untiffed off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_verify_dns off
[roo@vbox conf]$
```

4 (рис. ??)

```
roo@vbox:/etc/httpd/conf$ systemctl status httpd.service
roo@vbox:/etc/httpd/conf$
Type: members: 37 Range: trans: 5931
Role: allow: 40 Role: trans: 417
Constraints: 70 Validatetrans: 0
MLS Constraint: 72 MLS Val. Trans: 0
Permissives: 1 PolCap: 6
Defaults: 7 Typebounds: 0
Allowperms: 0 Neverallowperms: 0
Auditallowperms: 0 Dontauditperms: 0
Ibendportcon: 0 Ibkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 189 Portcon: 665
Netifcon: 0 Nodecon: 0

[roo@vbox conf]$ 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: 5169 Attributes: 259
Users: 8 Roles: 15
Booleans: 358 Cond. Expr.: 390
Allow: 65833 Neverallow: 0
Auditallow: 176 Dontaudit: 8703
Type_trans: 271851 Type_change: 94
Type_member: 37 Range_trans: 5931
Role_allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constraint: 72 MLS Val. Trans: 0
Permissives: 1 PolCap: 6
Defaults: 7 Typebounds: 0
Allowperms: 0 Neverallowperms: 0
Auditallowperms: 0 Dontauditperms: 0
Ibendportcon: 0 Ibkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 189 Portcon: 665
Netifcon: 0 Nodecon: 0

[roo@vbox conf]$
```



5 (рис. ??)

```

roo@vbox:/etc/httpd/conf — /bin/systemctl status httpd.service
roo@vbox:/etc/httpd/conf

Permissives: 1 PolCap: 6
Defaults: 7 Typebounds: 0
Allowperm: 0 Neverallowperm: 0
Auditallowperm: 0 Dontauditperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[roo@vbox conf]# 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: 5169 Attributes: 259
Users: 8 Roles: 15
Booleans: 358 Cond. Expr.: 390
Allow: 65633 Neverallow: 0
Auditallow: 176 Dontaudit: 8703
Type_trans: 271851 Type_change: 94
Type_member: 37 Range_trans: 5931
Role_allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constrains: 72 MLS Val. Tran: 0
Permissives: 1 PolCap: 6
Defaults: 7 Typebounds: 0
Allowperm: 0 Neverallowperm: 0
Auditallowperm: 0 Dontauditperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[roo@vbox conf]# ls -lZ /var/www
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 апр 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр 12 16:20 html
[roo@vbox conf]#

```

6 (рис. ??)

```

roo@vbox:/var/www/html
roo@vbox:/var/www/html

Type_members: 37 Range_trans: 5931
Role_allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constrains: 72 MLS Val. Tran: 0
Permissives: 1 PolCap: 6
Defaults: 7 Typebounds: 0
Allowperm: 0 Neverallowperm: 0
Auditallowperm: 0 Dontauditperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0

[roo@vbox conf]# ls -lZ /var/www
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 апр 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр 12 16:20 html
[roo@vbox conf]# ls -lZ /var/www/html
ls: невозможно получить доступ к '/var/www/html': Нет такого файла или каталога
[roo@vbox conf]# ls -lZ /var/www/html
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 апр 12 16:20 html
[roo@vbox conf]# cd /var/www/html
[roo@vbox html]# nano test.html
[roo@vbox html]# ls -lZ /var/www/test.html
ls: невозможно получить доступ к '/var/www/test.html': Нет такого файла или каталога
[roo@vbox html]# ls
test.html
[roo@vbox html]# ls -lZ test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 окт 12 18:23 test.html
[roo@vbox html]# secon --file var/www/html/test.html
secon: couldn't get security context for file var/www/html/test.html: No such file or directory
[roo@vbox html]# secon --file test.html
user: unconfined_u
role: object_r
type: httpd_sys_content_t
sensitivity: s0
clearance: s0
mls-range: s0
[roo@vbox html]#

```

## 4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Sticky bit [Электронный ресурс]. Wikimedia Foundation, 2024. URL: [https://ru.wikipedia.org/wiki/Sticky\\_bit](https://ru.wikipedia.org/wiki/Sticky_bit).