

# Отчёт Лабораторной работы №6

По дисциплине Информационная безопасность

Прокошев Никита Евгеньевич

# Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	11
Список литературы	12

## Список таблиц

# Список иллюстраций

1	getenforce и sestatus. . . . .	6
2	Текущее состояние SELinux. . . . .	7
3	. . . . .	8
4	. . . . .	8
5	. . . . .	9
6	. . . . .	9
7	. . . . .	10
8	. . . . .	10
9	. . . . .	10

## Цель работы

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

# 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` (@pic:001).

```
[nikitaprokoshev@neprokoshev ~]$ su
Password:
[root@neprokoshev nikitaprokoshev]# getenforce
Enforcing
[root@neprokoshev nikitaprokoshev]# 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
```

Рис. 1: `getenforce` и `sestatus`.

2. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды (@pic:002).



```
[root@neproshech nikitaproshech]# 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:            5100     Attributes:         258
Users:            8        Roles:              14
Booleans:         353     Cond. Expr.:       384
Allow:            65008    Neverallow:         0
Auditallow:       170     Dontaudit:          8572
Type_trans:       265344  Type_change:        87
Type_member:      35      Range_trans:        6164
Role allow:       38      Role_trans:         420
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:            660
Netifcon:         0      Nodecon:            0
```

Рис. 3: .

4. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, в директории `/var/www/html` (@pic:004).

```
[root@neproshech nikitaproshech]# ls -lz /var/www
ls: invalid option -- 'z'
Try 'ls --help' for more information.
[root@neproshech nikitaproshech]# 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 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23:21 html
[root@neproshech nikitaproshech]# ls -LZ /var/www/html
total 0
```

Рис. 4: .

5. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` (@pic:005) следующего содержания (@pic:006).



```
[root@neproskoshev nikitaiproskoshev]# touch /var/www/html/test.html
[root@neproskoshev nikitaiproskoshev]# gedit /var/www/html/test.html
```

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

6. Проверьте контекст созданного вами файла (@pic:007).

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

Рис. 5: .

7. 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 (@pic:008).

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

Рис. 6: .

8. 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.
9. 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`.
10. 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` (@pic:010).

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

Рис. 7: .

11. Верните контекст `httpd_sys_content__t` к файлу `/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». (@pic:011).

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

Рис. 8: .

12. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`. Удалите привязку `http_port_t` к 81 порту и проверьте, что порт 81 удалён. Удалите файл `/var/www/html/test.html` (@pic:011).

```
[root@neproshe nikitaproshe]# gedit /etc/httpd/conf/httpd.conf
(gedit:7671): dconf-WARNING **: 22:43:26.200: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
(gedit:7671): dconf-WARNING **: 22:43:26.200: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
(gedit:7671): dconf-WARNING **: 22:43:26.790: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
(gedit:7671): dconf-WARNING **: 22:43:26.790: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
(gedit:7671): dconf-WARNING **: 22:43:26.790: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
** (gedit:7671): WARNING **: 22:43:35.230: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:7671): WARNING **: 22:43:35.230: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:7671): WARNING **: 22:43:37.090: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:7671): dconf-WARNING **: 22:43:37.730: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
[root@neproshe nikitaproshe]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@neproshe nikitaproshe]# gedit /var/www/html/test.html
(gedit:7966): dconf-WARNING **: 22:45:14.190: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
(gedit:7966): dconf-WARNING **: 22:45:14.200: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
Error creating proxy: Error sending credentials: Error sending message: Broken pipe (g-io-error-quark, 44)
(gedit:7966): dconf-WARNING **: 22:45:14.600: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
(gedit:7966): dconf-WARNING **: 22:45:14.600: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
(gedit:7966): dconf-WARNING **: 22:45:14.600: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
** (gedit:7966): WARNING **: 22:45:20.010: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:7966): dconf-WARNING **: 22:45:20.040: failed to commit changes to dconf: Error sending credentials: Error sending message: Broken pipe
[root@neproshe nikitaproshe]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
```

Рис. 9: .

## Выводы

В ходе данной лабораторной работы удалось развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

## Список литературы