

Лабораторная работа №6

Мандатное разграничение прав в Linux

Монастырская Кристина Владимировна НПИбд-02-19¹
2022, 19 March, Moscow, Russian Federation

¹RUDN University, Moscow, Russian Federation

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Убедилась, что SELinux работает в
режиме enforcing политики targeted

Убедилась, что SELinux работает в режиме enforcing политики targeted

```
[root@kvmonastyrskaya ~]# getenforce
bash: getenforce: command not found...
Similar command is: 'getenforce'
[root@kvmonastyrskaya ~]# getenforce
Enforcing
[root@kvmonastyrskaya ~]# 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
[root@kvmonastyrskaya ~]#
```

Рис. 1: Режим SELinux

Запустила веб-сервер

Запустила веб-сервер

```
[root@kvmonastyrskaya ~]# 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 pre
   Active: active (running) since Sun 2022-12-18 15:51:22 MSK; 53min ago
     Docs: man:httpd.service(8)
   Main PID: 3508 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes
     Tasks: 213 (limit: 10804)
   Memory: 35.2M
     CPU: 4.472s
   CGroup: /system.slice/httpd.service
           └─3508 /usr/sbin/httpd -DFOREGROUND
             └─3509 /usr/sbin/httpd -DFOREGROUND
               └─3510 /usr/sbin/httpd -DFOREGROUND
                 └─3511 /usr/sbin/httpd -DFOREGROUND
                   └─3512 /usr/sbin/httpd -DFOREGROUND

дек 18 15:51:22 kvmonastyrskaya systemd[1]: Starting The Apache HTTP Server...
дек 18 15:51:22 kvmonastyrskaya systemd[1]: Started The Apache HTTP Server.
дек 18 15:51:22 kvmonastyrskaya httpd[3508]: Server configured, listening on: p
lines 1-19/19 (FND)
```

Рис. 2: Проверка работы веб-сервера

Нашла веб-сервер Apache в списке
процессов

Нашла веб-сервер Apache в списке процессов

```
[root@kvmonastyrskaya ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3508 0.0 0.4 20132 8656 ?
Ss 15:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3509 0.0 0.2 21608 5132 ?
S 15:51 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3510 0.0 0.6 2062420 12112 ?
Sl 15:51 0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3511 0.0 0.7 2193556 14004 ?
Sl 15:51 0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3512 0.0 0.6 2062420 12532 ?
Sl 15:51 0:01 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 6405 0.0 0.1 221820
2360 pts/0 S+ 16:47 0:00 grep --color=auto httpd
[root@kvmonastyrskaya ~]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 3508 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3509 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3510 ? 00:00:01 httpd
system_u:system_r:httpd_t:s0 3511 ? 00:00:01 httpd
system_u:system_r:httpd_t:s0 3512 ? 00:00:01 httpd
[root@kvmonastyrskaya ~]#
```

Рис. 3: Список процессов

Текущее состояние переключателей SELinux для Apache

Текущее состояние переключателей SELinux для Apache

```
[root@kvmmonastyrskaya ~]# 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_avahi                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
httpd_read_user_content         off
httpd_run_ipa                   off
httpd_run_preupgrade            off
httpd_run_stickshift            off
httpd_serve_cobbler_files       off
httpd_setrlimit                 off
httpd_ssi_exec                  off
httpd_sys_script_anon_write     off
```

Рис. 4: Состояние переключателей SELinux

Статистика по политике

```
[root@kvmonastyrskaya ~]# 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:        5095     Attributes:       256
Users:        8        Roles:           14
Booleans:     351      Cond. Expr.:     383
Allow:        65187     Neverallow:       0
Auditallow:   165      Dontaudit:       8564
Type_trans:   257951   Type_change:      87
Type_member:  35        Range_trans:     6164
Role allow:   38        Role_trans:      419
Constraints:  70        Validatetrans:   0
MLS Constrai: 72        MLS Val. Tran:   0
Permissives:  0        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

[root@kvmonastyrskaya ~]#
```

Рис. 5: Статистика SELinux

Тип поддиректорий в директории
/var/www

Тип поддиректорий в директории /var/www

```
[root@kvmonastyrskaya ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 июл 22 14
:43 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 июл 22 14
:43 html
[root@kvmonastyrskaya ~]#
```

Рис. 6: Тип поддиректорий в директории /var/www

Круг пользователей с разрешением на
создание файлов в `/var/www/html`

Круг пользователей с разрешением на создание файлов в /var/www/html

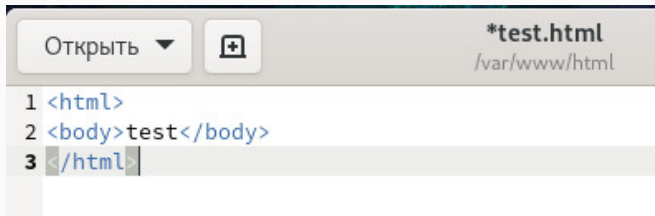
```
[root@kvmonastyrskaya ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 июл 22 14
:43 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 июл 22 14
:43 html
```

Рис. 7: Право на создание файлов

Создала html-файл

/var/www/html/test.html

Создала html-файл /var/www/html/test.html



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

Рис. 8: HTML-файл /var/www/html/test.html

Проверила контекст созданного файла

Контекст файла

Обратилась к файлу через веб-сервер

Обратилась к файлу через веб-сервер

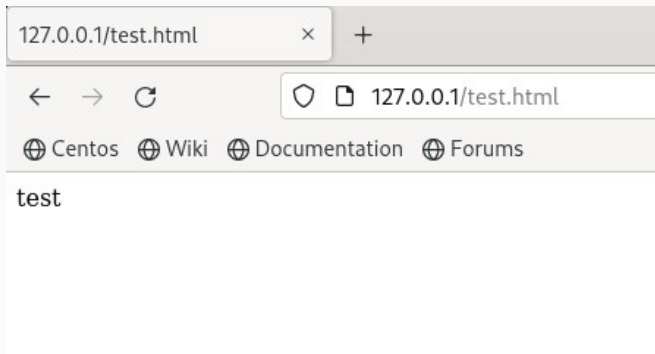


Рис. 9: Отображение файла test.html

Изменила контекст файла
`/var/www/html/test.html`

Изменила контекст файла /var/www/html/test.html

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

Рис. 10: Изменение контекста файла

Обратилась к файлу через веб-сервер

Обратилась к файлу через веб-сервер

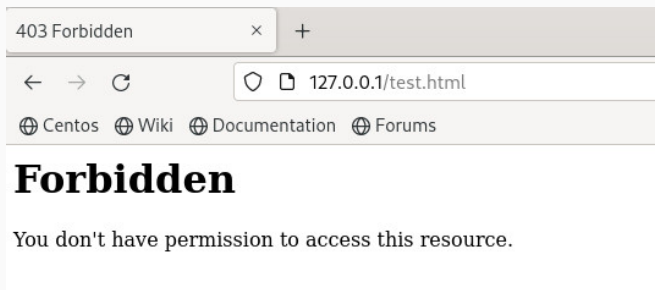


Рис. 11: Доступ через веб-сервер

Log-файлы веб-сервера Apache

Log-файлы веб-сервера Apache

```
[root@kvmnastyrskaya ~]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 дек 18 16:56 /var/www/html/test.html
[root@kvmnastyrskaya ~]# tail /var/log/messages
Dec 18 17:04:36 kvmnastyrskaya systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Dec 18 17:04:38 kvmnastyrskaya setroublshooot getattr(7503): SELinux запрещает /usr/sbin/httpd_dcsn getattr к файлу /var/www/html/
test.html. Для выполнения всех сообщений SELinux: sealer -l 0095e2e2-980e-4fce-a0f7-9db17343b02d
Dec 18 17:04:38 kvmnastyrskaya setroublshooot(7503): SELinux запрещает /usr/sbin/httpd_dcsn getattr к файлу /var/www/html/
test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить
метку.#012#012$PATH по умолчанию должен быть httpd_sys_content_t.#012#012Вы можете запустить restorecon. Возможно, но
пытка доступа была основана на из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайтс
я соответствующим образом изменить следующую команду.#012#012$semanage fcontext -t public_content_t '/var/www/html/test.html' #012#012****
Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html как обь
ект единственного контента.#012#012 необходимо изменить метку test.html c public_content_t на public_content_rw_t.#012#012$semana
ge fcontext -a -t public_content_t '/var/www/html/test.html' #012#012 restorecon -v '/var/www/html/test.html' #012#012****
Модуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разреше
но getattr доступ к test.html file по умолчанию.#012#012 рекомендуется создать отчет об ошибке.#012#012абы разрешить доступ, мож
но создать локальный модуль политики.#012#012$restorecon этот доступ сейчас, выполнив:#012#012 ausearch -c 'httpd' --raw |
auditallow -M my-httpd#012#012 semodule -X 300 -i my-httpd.pp#012
Dec 18 17:04:38 kvmnastyrskaya setroublshooot(7503): SELinux запрещает /usr/sbin/httpd_dcsn getattr к файлу /var/www/html/
test.html. Для выполнения всех сообщений SELinux: sealer -l 0095e2e2-980e-4fce-a0f7-9db17343b02d
Dec 18 17:04:38 kvmnastyrskaya setroublshooot(7503): SELinux запрещает /usr/sbin/httpd_dcsn getattr к файлу /var/www/html/
test.html.#012#012**** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправит
метку.#012#012$PATH по умолчанию должен быть httpd_sys_content_t.#012#012Вы можете запустить restorecon. Возможно, но
пытка доступа была основана на из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайтс
я соответствующим образом изменить следующую команду.#012#012$semanage fcontext -t public_content_t '/var/www/html/test.html' #012#012****
Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html как обь
ект единственного контента.#012#012 необходимо изменить метку test.html c public_content_t на public_content_rw_t.#012#012$semana
ge fcontext -a -t public_content_t '/var/www/html/test.html' #012#012 restorecon -v '/var/www/html/test.html' #012#012****
Модуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разреше
но getattr доступ к test.html file по умолчанию.#012#012 рекомендуется создать отчет об ошибке.#012#012абы разрешить доступ, мож
но создать локальный модуль политики.#012#012$restorecon этот доступ сейчас, выполнив:#012#012 ausearch -c 'httpd' --raw |
auditallow -M my-httpd#012#012 semodule -X 300 -i my-httpd.pp#012
Dec 18 17:04:48 kvmnastyrskaya system[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated succ
essfully.
Dec 18 17:04:48 kvmnastyrskaya systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.693s
CPU time.
Dec 18 17:04:48 kvmnastyrskaya systemd[1]: setroublshooot.service: Deactivated successfully.
Dec 18 17:04:48 kvmnastyrskaya systemd[1]: setroublshooot.service: Consumed 1.378s CPU time.
Dec 18 17:05:12 kvmnastyrskaya journal[531]: Source ID 15989 was not found when attempting to remove it
[root@kvmnastyrskaya ~]#
```

Рис. 12: log-файл

Посмотрела системный лог-файл

Посмотрела системный лог-файл

```
[root@kvmnastyrskaya ~]# tail /var/log/audit/audit.log
type=AVC msg=audit(1671372275.164:399): avc: denied { getattr } for pid=3512 comm="httpd" path="/var/www/html/test.html"
dev="dm-0" ino=71300109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file pe
rmissive=0
type=SYSCALL msg=audit(1671372275.164:399): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f6f4c00caa8 a2=7f6
f68fe98b0 a3=0 items=0 ppid=3508 pid=3512 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tt
y=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=n
ewfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGI
D="apache"
type=PROCTITLE msg=audit(1671372275.164:399): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=AVC msg=audit(1671372275.165:400): avc: denied { getattr } for pid=3512 comm="httpd" path="/var/www/html/test.html"
dev="dm-0" ino=71300109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file pe
rmissive=0
type=SYSCALL msg=audit(1671372275.165:400): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f6f4c00cb88 a2=7f6
f68fe98b0 a3=100 items=0 ppid=3508 pid=3512 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48
tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=
newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FS
GID="apache"
type=PROCTITLE msg=audit(1671372275.165:400): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1671372276.228:401): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
type=SERVICE_START msg=audit(1671372276.785:402): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=dbus-1.1-0.org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=?
addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1671372288.820:403): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=dbus-1.1-0.org.fedoraproject.SetroubleshootPrivileged@0 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? a
ddr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1671372288.859:404): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s
0 msg='unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
[root@kvmnastyrskaya ~]#
```

Рис. 13: Системный лог-файл

Запустила веб-сервер Apache на
прослушивание TCP-порта

81

```
41 # Change this to Listen on a specific IP address, but note that if
42 # httpd.service is enabled to run at boot time, the address may not be
43 # available when the service starts. See the httpd.service(8) man
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
```

Рис. 14: Включение прослушивания 81 порта

Добавила порт 81 в список портов

Добавила порт 81 в список портов

```
[root@kvmonastyrskaya ~]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kvmonastyrskaya ~]# 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. 15: Список портов

Вернула контекст

`httpd_sys_content__t` и обратилась к
файлу через веб-сервер

Вернула контекст `httpd_sys_content__t` и обратилась к файлу через веб-сервер

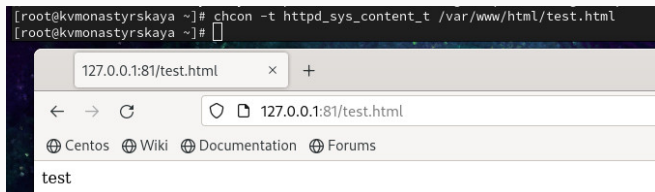


Рис. 16: Контекст файла и отображение страницы

Исправила конфигурационный файл
apache

```
44 # page for more information.  
45 #  
46 #Listen 12.34.56.78:80  
47 Listen 80  
48
```

Рис. 17: Конфигурационный файл Apache

Попробовала удалить привязку
http_port_t к 81 порту

Попробовала удалить привязку http_port_t к 81 порту

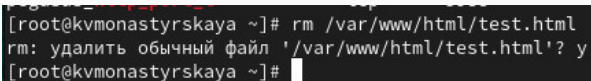
```
[root@kvmonastyrskaya ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@kvmonastyrskaya ~]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@kvmonastyrskaya ~]#
```

Рис. 18: Удаление порта из списка

Удалила файл

/var/www/html/test.html

Удалила файл /var/www/html/test.html

A terminal window with a dark background and light-colored text. The prompt is [root@kvmonastyrskaya ~]#. The command rm /var/www/html/test.html is entered. The output is rm: удалить обычный файл '/var/www/html/test.html'? y. The prompt is repeated at the end of the line.

```
[root@kvmonastyrskaya ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@kvmonastyrskaya ~]#
```

Рис. 19: Удаление файла

Вывод

Получили практическое знакомство с технологией SELinux1.
Проверили работу SELinx на практике совместно с
веб-сервером Apache.