

Лабораторная работа № 6

Мандатное разграничение прав в Linux

Хамдамова Айжана

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	16

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. SELinux имеет три основных режим работы:

Enforcing: режим по умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

Permissive: в случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Disabled: полное отключение системы принудительного контроля доступа.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены. Более подробно см. в [1].

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA). Для чего нужен Apache сервер:

чтобы открывать динамические PHP-страницы,
для распределения поступающей на сервер нагрузки,

для обеспечения отказоустойчивости сервера,

чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

3 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`.
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`.

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



```

[akhamdamova@akhamdamova ~]$ 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; preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
[akhamdamova@akhamdamova ~]$ sudo systemctl start httpd
[akhamdamova@akhamdamova ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[akhamdamova@akhamdamova ~]$ 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 Fri 2024-04-26 12:55:43 MSK; 16s ago
     Docs: man:httpd.service(8)
  Main PID: 41268 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 213 (limit: 10901)
   Memory: 23.5M
      CPU: 118ms
   CGroup: /system.slice/httpd.service
           └─41268 /usr/sbin/httpd -DFOREGROUND
             └─41269 /usr/sbin/httpd -DFOREGROUND
               └─41270 /usr/sbin/httpd -DFOREGROUND
                 └─41271 /usr/sbin/httpd -DFOREGROUND
                   └─41275 /usr/sbin/httpd -DFOREGROUND

Apr 26 12:55:42 akhamdamova.localdomain systemd[1]: Starting The Apache HTTP Server...
Apr 26 12:55:43 akhamdamova.localdomain systemd[1]: Started The Apache HTTP Server.
Apr 26 12:55:43 akhamdamova.localdomain httpd[41268]: Server configured, listening on: port 80
[akhamdamova@akhamdamova ~]$

```

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`

```

Apr 26 12:55:43 akhamdamova.localdomain systemd[1]: Started The Apache HTTP Server.
Apr 26 12:55:43 akhamdamova.localdomain httpd[41268]: Server configured, listening on: port 80
[akhamdamova@akhamdamova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      41268  0.0  0.6 20340 11672 ?        Ss   12:55   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41269  0.0  0.4 21676 7516 ?        S    12:55   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41270  0.0  0.7 1210624 13172 ?      Sl   12:55   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41271  0.0  0.6 1079488 11124 ?      Sl   12:55   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41275  0.0  0.6 1079488 11124 ?      Sl   12:55   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0:c1023 akhamda+ 41543 0.0  0.1 221664 2380 pts/0 S+   12:57   0:00 grep --color=auto httpd

```

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».

```

[akhamdamova@akhamdamova ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap    off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content           off
cluster_can_network_connect    off
cluster_manage_all_files       off

```

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.

```

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...
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

[akhamdamova@akhamdamova ~]$

```

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`

```

drwxr-xr-x. 2 akhamdamova akhamdamova 6 Feb 16 10:27 Videos
[akhamdamova@akhamdamova ~]$ 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
[akhamdamova@akhamdamova ~]$

```

7. Определите тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html`

```

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

```

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

```

[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html
total 0
[akhamdamova@akhamdamova ~]$ su -
Password:
[root@akhamdamova ~]# touch /var/www/html/test.html
[root@akhamdamova ~]# nano /var/www/html/test.html
[root@akhamdamova ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>

```

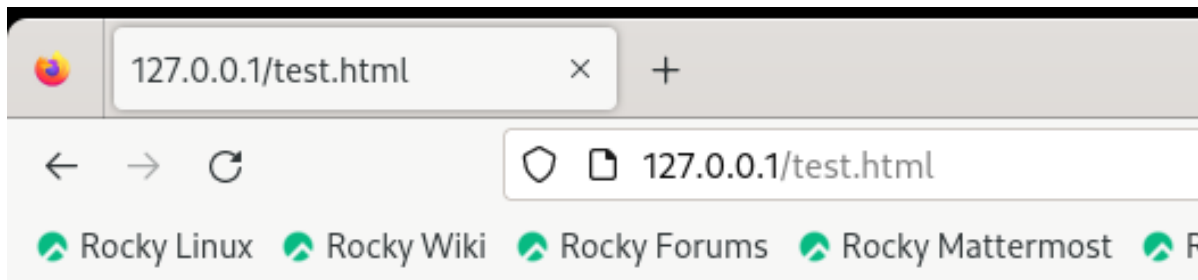
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

```

[akhamdamova@akhamdamova ~]$
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html
total 0
[akhamdamova@akhamdamova ~]$ su -
Password:
[root@akhamdamova ~]# touch /var/www/html/test.html
[root@akhamdamova ~]# nano /var/www/html/test.html
[root@akhamdamova ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@akhamdamova ~]# exit
logout
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Apr 26 13:05 test.html
[akhamdamova@akhamdamova ~]$

```

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.



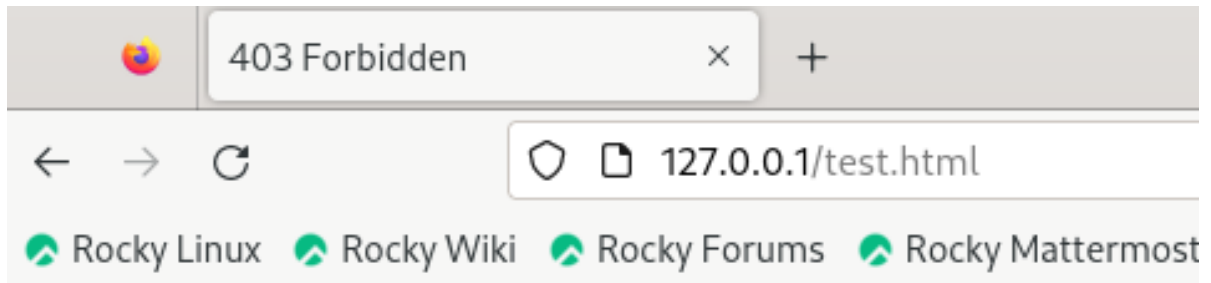
12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`

```
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Apr 26 13:05 test.html
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Apr 26 13:05 /var/www/html/test.html
[akhamdamova@akhamdamova ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted
[akhamdamova@akhamdamova ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] password for akhamdamova:
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Apr 26 13:05 /var/www/html/test.html
```

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`

```
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Apr 26 13:05 test.html
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Apr 26 13:05 /var/www/html/test.html
[akhamdamova@akhamdamova ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted
[akhamdamova@akhamdamova ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] password for akhamdamova:
[akhamdamova@akhamdamova ~]$ ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 Apr 26 13:05 /var/www/html/test.html
```

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.`



Forbidden

You don't have permission to access this resource.

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`

```

[akhamdamova@akhamdamova ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Apr 26 13:05 /var/www/html/test.html
[akhamdamova@akhamdamova ~]$ tail /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[akhamdamova@akhamdamova ~]$ sudo tail /var/log/messages
Apr 26 13:16:44 akhamdamova systemd[1]: Started dbus-1.1-0.org.fedoraproject.SetroubleshootPrivileged@1.service.
Apr 26 13:16:46 akhamdamova setroubleshoot[43004]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.
SELinux messages run: sealert -l 7d5efa19-445f-4dd0-b3f4-5abb3af2bc08
Apr 26 13:16:46 akhamdamova setroubleshoot[43004]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.
Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html de
n the test.html file by default.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access
y in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin
.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label
public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/va
tml'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed
access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr 26 13:16:46 akhamdamova setroubleshoot[43004]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.
SELinux messages run: sealert -l 7d5efa19-445f-4dd0-b3f4-5abb3af2bc08
Apr 26 13:16:46 akhamdamova setroubleshoot[43004]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.
Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html de
n the test.html file by default.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access
y in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin
.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label
public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/va
tml'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed
access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Apr 26 13:16:55 akhamdamova firefox.desktop[42643]: [ERROR viaduct::backend::ffi] Missing HTTP status
Apr 26 13:16:55 akhamdamova firefox.desktop[42643]: [ERROR viaduct::backend::ffi] Missing HTTP status
Apr 26 13:16:56 akhamdamova systemd[1]: dbus-1.1-0.org.fedoraproject.SetroubleshootPrivileged@1.service: Deactivated successfully.
Apr 26 13:16:56 akhamdamova systemd[1]: setroubleshootd.service: Deactivated successfully.
Apr 26 13:16:56 akhamdamova systemd[1791]: app-gnome-firefox-42643.scope: Consumed 12.029s CPU time.

```

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.

```

+ akhamdamova@akhamdamova:~ — nano /etc/httpd/conf/
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support

```

4 Выводы

Развита навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux¹. Проверила работу SELinux на практике совместно с веб-сервером Apache.