

Лабораторная работа 6

Мандатное разграничение прав в Linux

Лушин Артём Андреевич

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	15

Список иллюстраций

2.1	Проверка режима и политики	5
2.2	Проверка статуса	6
2.3	Определение контекста безопасности	6
2.4	Проверка переключателей	7
2.5	Статистика политики	8
2.6	Тип файлов html	8
2.7	Создание файла	9
2.8	Отображение на сайте	9
2.9	Смена контекста	10
2.10	Проверка нового контекста	10
2.11	Проверка лог-файла	10
2.12	Изменение порта на 81	11
2.13	Перезапуск сервера	11
2.14	Проверка файлов	11
2.15	Смена портов	12
2.16	Перезапуск веб-сервера с добавленным портом	12
2.17	Возвращение контекста	12
2.18	Проверка веб-сервера с новым портом	12
2.19	Возвращение старого порта	13
2.20	Удаление файлов	14

1 Цель работы

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

2 Выполнение лабораторной работы

- 1) Я проверил в каком режиме работает SELinux. Режим - Enforcing, а политика - targeted.

```
[guest@user aalusihn]$ getenforce
Enforcing
[guest@user aalusihn]$ sestatus
bash: sestatus: command not found...
[guest@user aalusihn]$ 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
[guest@user aalusihn]$
```

Рис. 2.1: Проверка режима и политики

- 2) Проверил статус браузера к веб-серверу, который запущен на компьютере. Статус - active.

```
guestuser aalusihm] service httpd status
The service command supports only basic LSB actions (start, stop, restart, try-restart, reload, reload-or-restart, try-reload-or-restart, force-reload, status, condrestart). For other actions, please try to use systemctl.
guestuser aalusihm] 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)
guestuser aalusihm] service httpd start
Redirecting to /bin/systemctl start httpd.service
guestuser aalusihm] 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: active (running) since Sat 2024-02-27 19:28:10 WOL; 5h ago
Docs: man:httpd.service(8)
Main PID: 16089 (httpd)
Status: "started, listening on port 80"
Tasks: 13 (limit: 8080)
Memory: 41.7M
CPU: 1.01s
CGroup: /system.slice/httpd.service
└─┬─ /usr/sbin/httpd -DFOREGROUND
   ├── /usr/sbin/httpd -DFOREGROUND
   ├── /usr/sbin/httpd -DFOREGROUND
   ├── /usr/sbin/httpd -DFOREGROUND
   └─ /usr/sbin/httpd -DFOREGROUND
guestuser aalusihm] █
```

Рис. 2.2: Проверка статуса

3) Я определил контекст безопасности веб-сервера Apache. Контекст - httpd_t.

```
guestuser aalusihm] ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 16039 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 16084 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 16085 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 16087 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 16088 ? 00:00:00 httpd
guestuser aalusihm] ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 16039 0.5 0.1 20340 11788 ? Ss 19:28 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16084 0.0 0.0 21676 7632 ? S 19:28 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16085 1.1 0.2 2521344 23520 ? Sl 19:28 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16087 1.0 0.1 2259136 15340 ? Sl 19:28 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 16088 0.8 0.1 2324672 15336 ? Sl 19:28 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 guest 35448 0.0 0.0 221664 2360 pts/0 R+ 19:29 0:00 grep --color=auto httpd
guestuser aalusihm] █
```

Рис. 2.3: Определение контекста безопасности

4) Посмотрел текущее состояние переключателей SELinux для Apache. Большая часть переключателей выключены.

```
[guest@user aalusihn]$ 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
cluster_use_execmem            off
cobbler_anon_write             off
cobbler_can_network_connect    off
cobbler_use_cifs               off
cobbler_use_nfs                off
collectd_tcp_network_connect   off
colord_use_nfs                 off
condor_tcp_network_connect     off
conman_can_network             off
conman_use_nfs                 off
container_connect_any          off
container_manage_cgroup        off
container_read_certs           off
container_use_cephfs           off
container_use_devices          off
```

Рис. 2.4: Проверка переключателей

- 5) Посмотрел статистику по политике. Пользователей - 8, ролей - 15, а типов - 5135.

```
[guest@user aalusihn]$ 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:        65380    Neverallow:      0
Auditallow:   172      Dontaudit:       8647
Type_trans:   267809   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
```

Рис. 2.5: Статистика политики

- 6) Определил тип файлов, которые находятся в директории “/var/www/html”. Все файлы созданы и относятся к пользователю root. Владелец так же является пользователь root.

```
[guest@user aalusihn]$ 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
[guest@user aalusihn]$
```

Рис. 2.6: Тип файлов html

- 7) От имени суперпользователя создал файл “test.html” в директории “/var/www/html”. Вписал туда необходимый текст, чтобы потом проверить его на сайте. А контекст для новых файлов - httpd_sys_content_t.


```

[root@user aalusihn]# echo "<html>" > /var/www/html/test.html
[root@user aalusihn]# n /var/www/html/test.html
bash: n: command not found...
[root@user aalusihn]# nano /var/www/html/test.html
[root@user aalusihn]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@user aalusihn]# touch /var/www/html/test1.html
[root@user aalusihn]# ls /var/www/html/test.html
/var/www/html/test.html
[root@user aalusihn]# ls /var/www/html
test.html
[root@user aalusihn]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@user aalusihn]# touch /var/www/html/test1.html
[root@user aalusihn]# ls /var/www/html
test1.html test.html
[root@user aalusihn]# cat /var/www/html/test1.html
[root@user aalusihn]# la -l /var/www/html
bash: la: command not found...
[root@user aalusihn]# ls -l /var/www/html
total 4
-rw-r--r--. 1 root root  0 Feb 17 19:37 test1.html
-rw-r--r--. 1 root root 33 Feb 17 19:36 test.html
[root@user aalusihn]#

```

Рис. 2.7: Создание файла

- 8) Я ввёл в браузере ссылку “http://127.0.0.1/test.html”. Файл успешно отобра-
зился и на сайте показали такой же текст, как и в файле.

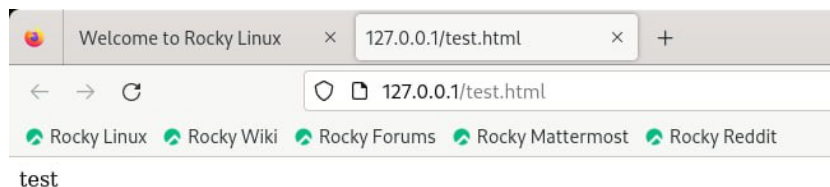


Рис. 2.8: Отображение на сайте

- 9) Я изучил справку “man httpd_selinux”. Для httpd определены следующие контексты: httpd_sys_conten_t, httpd_sys_script_exec_t, httpd_sys_script_ro_t, httpd_sys_script_rw_t, httpd_sys_script_ra_t, httpd_unconfined_script_exec_t. Я изменил контекст моего файла на “samba_share_t и провели, чтобы контекст установился.


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

Рис. 2.15: Смена портов

- 16) Я перезапустил веб-сервер и он запустился. Произошло это из-за того, что я добавил порт, которого до этого не было.

```
root@user aalusihn]# service httpd start
Redirecting to /bin/systemctl start httpd.service
root@user aalusihn]# 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: active (running) since Sat 2024-02-17 20:07:23 MSK; 2m ago
Docs: man:httpd.service(8)
Main PID: 6500 (httpd)
Status: "Total requests: 8; 126M/1000 workers 100/0/Requests/sec: 0; Bytes served/sec: 0 B/sec"
Tasks: 22 (1 limit: 65536)
Memory: 55.2M
CGroup: /system.slice/httpd.service
└─ httpd /usr/sbin/httpd -DFOREGROUND
   httpd /usr/sbin/httpd -DFOREGROUND
   httpd /usr/sbin/httpd -DFOREGROUND
   httpd /usr/sbin/httpd -DFOREGROUND
   httpd /usr/sbin/httpd -DFOREGROUND
Feb 17 20:07:23 user.linuxin systemd[1]: Starting The Apache HTTP Server...
Feb 17 20:07:23 user.linuxin httpd[6500]: Server configured, listening on: port 81
Feb 17 20:07:23 user.linuxin systemd[1]: Started The Apache HTTP Server.
root@user aalusihn]#
```

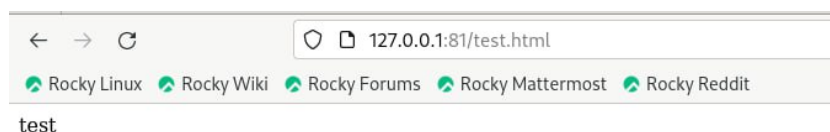
Рис. 2.16: Перезапуск веб-сервера с добавленным портом

- 17) Я вернул изначальный контекст файлу “text.html” и убедился в этом.

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

Рис. 2.17: Возвращение контекста

- 18) Попробовал зайти на веб-сервер, чтобы убедиться в том, что файл читается. Веб-сервер подключился и вывел текст “test”, как и в самом файле. Даже не смотря на то, что я поменял порт, веб-сервер запустился.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1:81/test.html". Below the address bar, there are several links: "Rocky Linux", "Rocky Wiki", "Rocky Forums", "Rocky Mattermost", and "Rocky Reddit". The main content area of the browser displays the word "test".

Рис. 2.18: Проверка веб-сервера с новым портом

- 19) Я исправил в конфигурационном файле 80 порт. Попытался вообще удалить привязку 81 порта, но этого нельзя сделать, так как не разрешает политика. Но тем не менее, теперь в конфигурационном файле стоит 80 порт и в списке портов он есть.

```
[root@user aalusihn]# nano /etc/httpd/conf/httpd.conf
[root@user aalusihn]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@user aalusihn]# 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@user aalusihn]# cat /etc/httpd/conf/httpd.conf
#
# This is the main Apache HTTP server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.4/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.4/mod/directives.html>
# for a discussion of each configuration directive.
#
# See the httpd.conf(5) man page for more information on this configuration,
# and httpd.service(8) on using and configuring the httpd service.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# server as '/www/log/access_log', where as '/log/access_log' will be
# interpreted as '/log/access_log'.
#
# 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 80
```

Рис. 2.19: Возвращение старого порта

- 20) Чтобы в дальнейшем мне не мешались тестовые файлы, я удалил все файлы, с которым работал в директории “var/www/html”.

```
[root@user aalusihn]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@user aalusihn]# rm /var/www/html/test1.html
rm: remove regular empty file '/var/www/html/test1.html'? y
[root@user aalusihn]# ls /var/www/html
[root@user aalusihn]#
```

Рис. 2.20: Удаление файлов

3 Выводы

Я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.