

Отчёт по лабораторной работе

Мандатное разграничение прав в Linux

Назарьева Алена Игоревна НФИбд-03-18

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	14

List of Figures

2.1	пункты 1-2	6
2.2	пункты 3-4	7
2.3	пункт 5	7
2.4	пункты 6-7	7
2.5	пункты 11	8
2.6	пункты 12-13	9
2.7	пункт 14	9
2.8	пункт 15	10
2.9	пункт 16	10
2.10	пункт 17	11
2.11	пункт 18-1	11
2.12	пункт 18-2	11
2.13	пункт 19-21-1	12
2.14	пункт 19-21-2	12
2.15	пункты 22-24	13

List of Tables

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 Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` (рис. -fig. 2.1)

```
[ainazarieva@ainazarieva ~]$ getenforce
Enforcing
[ainazarieva@ainazarieva ~]$ 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
Max kernel policy version:      31
[ainazarieva@ainazarieva ~]$ 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; vendor preset: disabled)
   Active: active (running) since Вт 2021-11-23 14:15:07 MSK; 10min ago
     Docs: man:httpd(8)
           man:apachectl(8)
```

Figure 2.1: пункты 1-2

3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. Как мы видим, этот процесс запущен на домене `httpd_t`. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`
4. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` (рис. -fig. 2.2)

```

[ainazarieva@ainazarieva ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      3403 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3494 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3495 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3496 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3497 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      3498 ?        00:00:00 httpd
[ainazarieva@ainazarieva ~]$ sestatus -bigrep httpd

```

Figure 2.2: пункты 3-4

5. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей:8, ролей:14, типов:4793. (рис. -fig. 2.3)

```

[root@ainazarieva ainazarieva]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:        272
Sensitivities:     1       Categories:         1024
Types:             4793    Attributes:         253
Users:             8       Roles:              14
Booleans:          316     Cond. Expr.:        362
Allow:             107834   Neverallow:         0
Auditallow:        158     Dontaudit:          10022
Type_trans:        18153   Type_change:        74
Type_member:        35     Role_allow:         37
Role_trans:        414     Range_trans:        5899
Constraints:        143    Validatetrans:      0
Initial SIDs:       27     Fs_use:             32
Genfscon:           103    Portcon:            614
Netifcon:           0      Nodecon:            0
Permissives:        0      Polcap:             5

```

Figure 2.3: пункт 5

6. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: `ls -lZ /var/www: httpd_sys_script_exec_t httpd_sys_content_t`
7. Определила тип файлов, находящихся в директории /var/www/html: `ls -lZ /var/www/html` (рис. -fig. 2.4)

```

[root@ainazarieva ainazarieva]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@ainazarieva ainazarieva]# ls -lZ /var/www/html

```

Figure 2.4: пункты 6-7

8. Определила круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. `rw-r-xr-x`
9. Создала 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
10. Проверила контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `unconfined_u:object_r:httpd_sys_content_t:s0` (рис. -fig. ??)

```
[ainazarieva@ainazarieva ~]$ ls -l /var/www
итого 0
drwxr-xr-x. 2 root root 6 ноя 10 17:27 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 10 17:27 html
[ainazarieva@ainazarieva ~]$ su
Пароль:
[root@ainazarieva ainazarieva]# touch /var/www/html/test.html
[root@ainazarieva ainazarieva]# echo "<html>
> <body>test</body>
> </html>">^C
[root@ainazarieva ainazarieva]# echo "<html>
> <body>test</body>
> </html>" > /var/www/html/test.html
[root@ainazarieva ainazarieva]# sudo ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@ainazarieva ainazarieva]# sudo ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.h
tml
[root@ainazarieva ainazarieva]#
```

11. Обратилась к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедилась, что файл был успешно отображён (рис. -fig. 2.5)

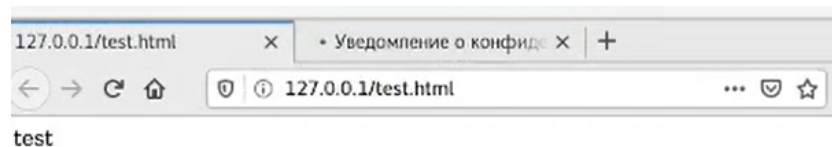


Figure 2.5: пункты 11

12. Изучила справку `man httpd_selinux` и выяснила, какие контексты файлов определены для `httpd:httpd_sys_content_t`; `httpd_sys_script_exec_t`; `httpd_sys_script_ro_t`; `httpd_sys_script_rw_t`. Они совпадают с типом

файла test.html. Проверила контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`

13. Изменила 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` После этого проверила, что контекст поменялся. (рис. -fig. 2.6)

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

Figure 2.6: пункты 12-13

14. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получила сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.` (рис. -fig. 2.7)

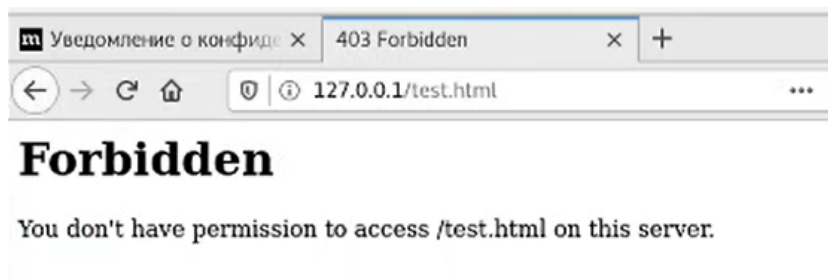


Figure 2.7: пункт 14

15. Проанализировала ситуацию. Доступ разрешен только между элементами с одинаковым типом, именно поэтому веб-сервер Apache может без проблем читать файл `/var/www/html/test.html`, который имеет тип `httpd_sys_content_t`. В то же самое время, так как Apache запущен на домене `httpd_t` и не имеет заполненных полей `userid:username`, он не может получить

доступ к файлу `home/username/test.html` с другим типом, хотя этот файл доступен для чтения процессам, для которых не определена целевая политика `ls -l /var/www/html/test.html` Просмотрела log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` В системе оказались запущенные процессы `setroubleshootd` и `audtd`, мы также смогли увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. (рис. -fig. 2.8)

```
[root@ainazarieva ainazarieva]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 23 14:50 /var/www/html/test.html
[root@ainazarieva ainazarieva]# tail /var/log/messages
Nov 23 15:01:01 ainazarieva systemd: Started Session 9 of user root.
Nov 23 15:02:03 ainazarieva systemd: Removed slice User Slice of root.
Nov 23 15:06:26 ainazarieva dbus[685]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Nov 23 15:06:36 ainazarieva dbus[685]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Nov 23 15:06:37 ainazarieva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Nov 23 15:06:38 ainazarieva setroubleshoot: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run:
sealert -l 514b9e88-f327-4df2-ad18-5e93fa3b98b2
Nov 23 15:06:38 ainazarieva python: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly. #012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public co
```

Figure 2.8: пункт 15

16. Попробовала 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` нашла строчку `Listen 80` и заменила её на `Listen 81`. (рис. -fig. 2.9)

```
[root@ainazarieva ainazarieva]# sed -i 's/Listen 80/Listen 81/g' /etc/httpd/conf/httpd.conf
[root@ainazarieva ainazarieva]#
```

Figure 2.9: пункт 16

17. Выполнила перезапуск веб-сервера Apache. Сбой не произошёл (рис. -fig. 2.10)

```
[root@ainazarieva ainazarieva]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@ainazarieva ainazarieva]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Figure 2.10: пункт 17

18. Проанализировала лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выяснила, что записи появились только в `/var/log/audit/audit.log` (рис. -fig. 2.11)

```
[root@ainazarieva ainazarieva]# tail /var/log/messages
Nov 23 15:24:29 ainazarieva systemd: Stopped The Apache HTTP Server.
Nov 23 15:24:33 ainazarieva systemd: Starting The Apache HTTP Server.
Nov 23 15:24:42 ainazarieva kernel: hrtimer: interrupt took 3582617 n
Nov 23 15:24:49 ainazarieva httpd: AH00558: httpd: Could not reliably
ver's fully qualified domain name, using ainazarieva.localdomain. Set
directive globally to suppress this message
Nov 23 15:24:49 ainazarieva systemd: Started The Apache HTTP Server.
Nov 23 15:26:03 ainazarieva systemd: Stopping The Apache HTTP Server.
Nov 23 15:26:04 ainazarieva systemd: Stopped The Apache HTTP Server.
Nov 23 15:26:04 ainazarieva systemd: Starting The Apache HTTP Server.
Nov 23 15:26:04 ainazarieva httpd: AH00558: httpd: Could not reliably
ver's fully qualified domain name, using ainazarieva.localdomain. Set
directive globally to suppress this message
Nov 23 15:26:04 ainazarieva systemd: Started The Apache HTTP Server.
[root@ainazarieva ainazarieva]# tail /var/log/http/error_log
tail: невозможно открыть «/var/log/http/error_log» для чтения: Нет та
алого
[root@ainazarieva ainazarieva]# tail /var/log/http/access_log
tail: невозможно открыть «/var/log/http/access_log» для чтения: Нет т
талого
```

Figure 2.11: пункт 18-1

(рис. -fig. 2.12)

```
[root@ainazarieva ainazarieva]# tail /var/log/audit/audit.log
type=LOGIN msg=audit(1637670001.584:501): pid=6134 uid=0 subj=system_
:s0-s0:c0.c1023 old-auid=4294967295 auid=0 tty=(none) old-ses=4294967
type=USER_START msg=audit(1637670001.767:502): pid=6134 uid=0 auid=0
_u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=
eyinit,pam_limits,pam_systemd acct="root" exe="/usr/sbin/crond" hostn
nal=cron res=success'
type=CRED_REFR msg=audit(1637670001.767:503): pid=6134 uid=0 auid=0 s
u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_er
="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=suc
type=CRED_DISP msg=audit(1637670001.928:504): pid=6134 uid=0 auid=0 s
u:system_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_er
="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=suc
```

Figure 2.12: пункт 18-2

19. Выполнила команду `semanage port -a -t http_port_t -p tcp 81` После этого проверила список портов командой `semanage port -l | grep http_port_t` Убедилась, что порт 81 появился в списке.
20. Попробовала запустить веб-сервер Apache ещё раз.
21. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`:
`chcon -t httpd_sys_content_t /var/www/html/test.html` (рис. -fig. 2.13)

```
[root@ainazarieva ainazarieva]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module,node,f
context,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: -p 81
[root@ainazarieva ainazarieva]# 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@ainazarieva ainazarieva]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@ainazarieva ainazarieva]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ainazarieva ainazarieva]#
```

Figure 2.13: пункт 19-21-1

После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидела содержимое файла — слово «test». (рис. -fig. 2.14)

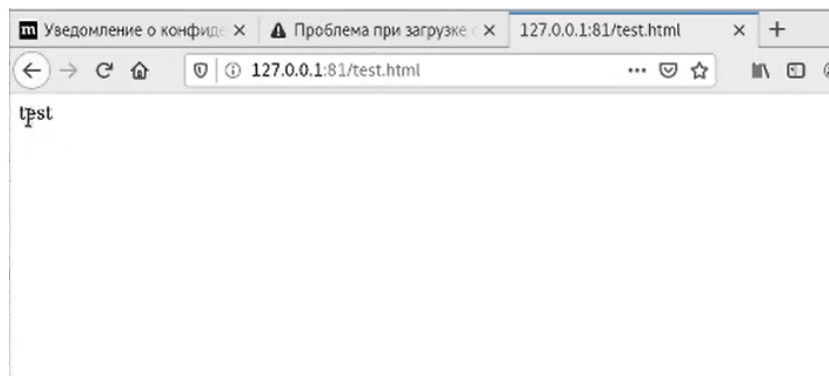


Figure 2.14: пункт 19-21-2

22. Исправила обратно конфигурационный файл apache, вернув `Listen 80`.

23. Попробовала удалить привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` порт 81 нельзя удалить, т.к. он определен на уровне политики
24. Удалила файл `/var/www/html/test.html`: `rm /var/www/html/test.html` (рис. - fig. 2.15)

```
[root@ainazarieva ainazarieva]# sed -i 's/Listen 81/Listen 80/g' /etc/httpd/conf/httpd.conf
[root@ainazarieva ainazarieva]# semanage port -d -t http_port_t -p tcp 81
^[[A^[[AValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ainazarieva ainazarieva]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@ainazarieva ainazarieva]# 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@ainazarieva ainazarieva]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»?
[root@ainazarieva ainazarieva]# ls /var/www/html
1.html test.html
[root@ainazarieva ainazarieva]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
```

Figure 2.15: пункты 22-24

3 Выводы

В результате выполнения работы я Развила навыки администрирования ОС Linux, Получила первое практическое знакомство с технологией SELinux1, Проверила работу SELinx на практике совместно с веб-сервером Apache.