

Отчет по лабораторной работе 6

Дисциплина: Информационная безопасность

Савченков Дмитрий Андреевич, НПИБд-02-18

Содержание

1	Цель работы	5
2	Подготовка лабораторного стенда:	6
3	Выполнение лабораторной работы:	8
4	Выводы	16
	Список литературы	17

List of Figures

2.1	Параметр ServerName	6
2.2	Отключение фильтра	6
2.3	Отключение фильтра	7
3.1	Проверка режима и политики	8
3.2	Проверка через браузер	9
3.3	Проверка статуса	9
3.4	веб-сервер Apache	9
3.5	Просмотр переключателей SELinux для Apache	10
3.6	Статистика	10
3.7	Определение типов файлов и круг пользователей	11
3.8	Создание файла	11
3.9	Проверка	11
3.10	Получение доступа к файлу через браузер	11
3.11	Изменение контекста, проверка	12
3.12	Получение доступа к файлу через браузер	12
3.13	Анализ ситуации	12
3.14	Изменеие порта 80 на 81	13
3.15	Анализ и просмотр лог-файлов	13
3.16	Выполнение и проверка	13
3.17	Возвращение контекста	14
3.18	Получение доступа к файлу через браузер	14
3.19	Исправленный файл apache	14
3.20	Удаление привязки к 81 порту	14
3.21	Удаление файла /var/www/html/test.html	15

List of Tables

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 Подготовка лабораторного стенда:

1. В конфигурационном файле `/etc/httpd/httpd.conf` задал параметр `ServerName`. (рис. -fig. 2.1).

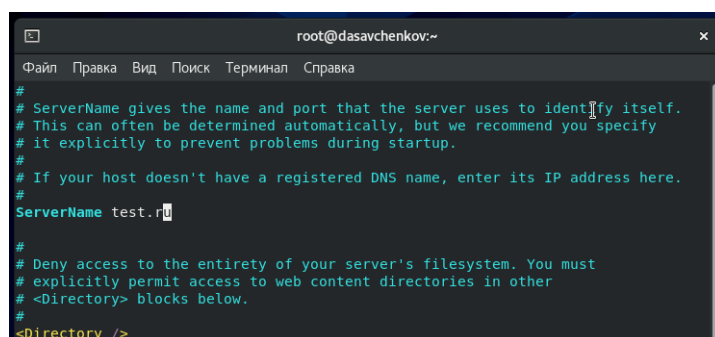
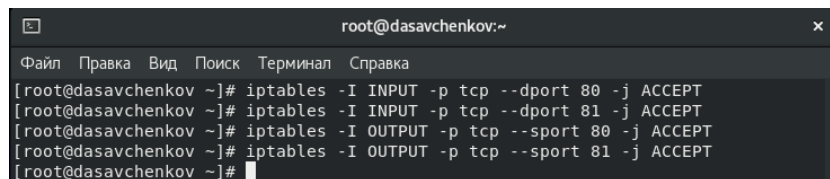


Figure 2.1: Параметр `ServerName`

2. Также проследил, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола `tcp`. Отключил фильтр командами: `iptables -F`, `iptables -P INPUT ACCEPT`, `iptables -P OUTPUT ACCEPT`. Так же добавил разрешающие правила. (рис. -fig. 2.2), (рис. -fig. 2.3).

```
[root@dasavchenkov ~]# iptables -F
[root@dasavchenkov ~]# iptables -P INPUT ACCEPT
[root@dasavchenkov ~]#
```

Figure 2.2: Отключение фильтра

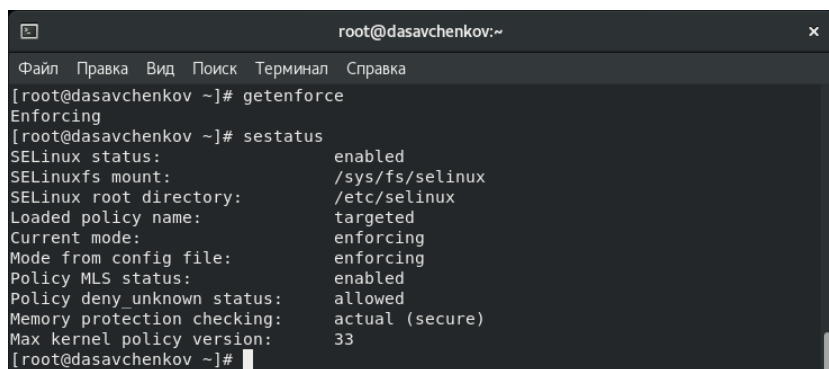


```
root@dasavchenkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@dasavchenkov ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT  
[root@dasavchenkov ~]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT  
[root@dasavchenkov ~]# iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT  
[root@dasavchenkov ~]# iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT  
[root@dasavchenkov ~]#
```

Figure 2.3: Отключение фильтра

3 Выполнение лабораторной работы:

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. -fig. 3.1).



```
root@dasavchenkov:~  
Файл Правка Вид Поиск Терминал Справка  
[root@dasavchenkov ~]# getenforce  
Enforcing  
[root@dasavchenkov ~]# 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@dasavchenkov ~]#
```

Figure 3.1: Проверка режима и политики

2. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: `service httpd status` (рис. -fig. 3.2), (рис. -fig. 3.3).

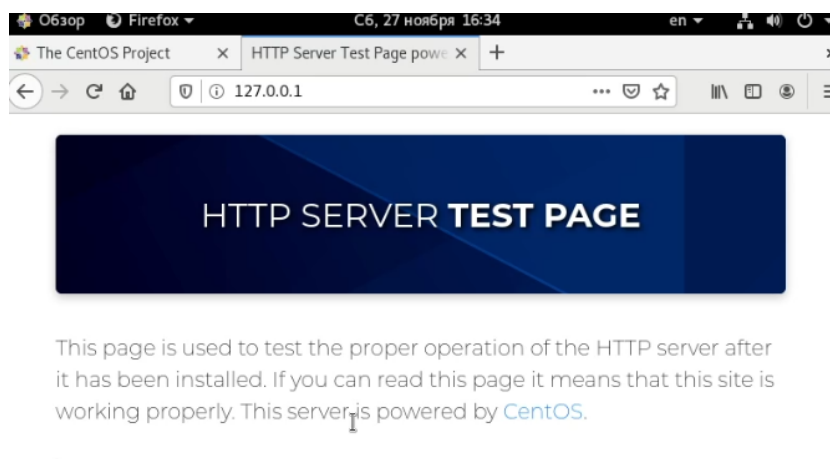


Figure 3.2: Проверка через браузер

```
[root@dasavchenkov ~]# ps auxZ | grep httpd
system u:system_r:httpd_t:s0 root 34728 0.0 0.3 273832 10964 ?
Ss 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34729 0.0 0.2 289836 8312 ?
S 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34730 0.0 0.3 1347644 9948 ?
Sl 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34731 0.0 0.3 1478772 9948 ?
Sl 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34732 0.0 0.3 1347644 9948 ?
Sl 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 35613 0.0 0.0 12136
1176 pts/0 R+ 16:35 0:00 grep --color=auto httpd
[root@dasavchenkov ~]#
```

Figure 3.3: Проверка статуса

3. Нашел веб-сервер Apache в списке процессов, определил его контекст без-опасности. (рис. -fig. 3.4).

```
[root@dasavchenkov ~]# ps auxZ | grep httpd
system u:system_r:httpd_t:s0 root 34728 0.0 0.3 273832 10964 ?
Ss 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34729 0.0 0.2 289836 8312 ?
S 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34730 0.0 0.3 1347644 9948 ?
Sl 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34731 0.0 0.3 1478772 9948 ?
Sl 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system_r:httpd_t:s0 apache 34732 0.0 0.3 1347644 9948 ?
Sl 16:33 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 35613 0.0 0.0 12136
1176 pts/0 R+ 16:35 0:00 grep --color=auto httpd
[root@dasavchenkov ~]#
```

Figure 3.4: веб-сервер Apache

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратил внимание, что многие из них находятся в положении «off». (рис. -fig. 3.5).

```
[root@dasavchenkov ~]# 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_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_avaahi off
```

Figure 3.5: Просмотр переключателей SELinux для Apache

5. Посмотрел статистику по политике с помощью команды `seinfo`, также определил множество пользователей(8), ролей(14), типов(4959) (рис. -fig. 3.6).

```
Target Policy: selinux
Handle unknown classes: allow
Classes: 132
Sensitivities: 1
Types: 4959
Users: 8
Booleans: 340
Allow: 112885
Auditallow: 166
Type_trans: 253398
Type_member: 35
Role_allow: 38
Constraints: 72
MLS_Constrain: 72
Permissives: 0
Defaults: 7
Allowxperm: 0
Auditallowxperm: 0
Ibendportcon: 0
Initial_SIDs: 27
Genfscon: 106
Netifcon: 0
Permissions: 463
Categories: 1024
Attributes: 255
Roles: 14
Cond. Expr.: 389
Neverallow: 0
Dontaudit: 10362
Type_change: 87
Range_trans: 6015
Role_trans: 423
Validatetrans: 0
MLS_Val. Tran: 0
Polcap: 5
Typebounds: 0
Neverallowxperm: 0
Dontauditxperm: 0
Ibpkeycon: 0
Fs_use: 33
Portcon: 640
Nodecon: 0
```

Figure 3.6: Статистика

6. Определил тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды: `ls -lZ /var/www`.
7. Определил тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`.
8. Определил круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. (рис. -fig. 3.7).

```

[root@dasavchenkov ~]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07
:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07
:58 html
[root@dasavchenkov ~]# ls -lZ /var/www/html/
итого 0
[root@dasavchenkov ~]# ls -lZ /var/www/html
итого 0
[root@dasavchenkov ~]# ls -l /var/www/html
итого 0
[root@dasavchenkov ~]# ls -l /var/www
итого 0
drwxr-xr-x. 2 root root 6 ноя 12 07:58 cgi-bin
drwxr-xr-x. 2 root root 6 ноя 12 07:58 html
[root@dasavchenkov ~]#

```

Figure 3.7: Определение типов файлов и круг пользователей

9. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. -fig. 3.8).

```

<html>
  <body>test</body>
</html>

```

Figure 3.8: Создание файла

10. Проверил контекст созданного файла. httpd_sys_content_t (рис. -fig. 3.9).

```

[root@dasavchenkov html]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 35 ноя 27 1
6:43 test.html
[root@dasavchenkov html]#

```

Figure 3.9: Проверка

11. Обратился к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедился, что файл был успешно отображён. (рис. -fig. 3.10).

Figure 3.10: Получение доступа к файлу через браузер

12. Проверил контекст файла командой: `ls -Z /var/www/html/test.html` (рис. - fig. 3.11).
13. Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверил, что контекст поменялся. (рис. -fig. 3.11).

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

Figure 3.11: Изменение контекста, проверка

14. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получил сообщение об ошибке. (рис. -fig. 3.12).



Figure 3.12: Получение доступа к файлу через браузер

15. Проанализировал ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: `tail /var/log/messages` (рис. -fig. 3.13).

```
root@dasavchenkov:/var/www/html
Файл  Правка  Вид  Поиск  Терминал  Справка
Nov 27 16:48:27 dasavchenkov setroubleshoot[36884]: failed to retrieve rpm info
for /var/www/html/test.html
Nov 27 16:48:27 dasavchenkov setroubleshoot[36884]: SELinux is preventing /usr/s
bin/httpd from getattr access on the file /var/www/html/test.html. For complete
SELinux messages run: sealert -l e1c10ebb-c535-4c25-8991-5540730fac28
Nov 27 16:48:27 dasavchenkov setroubleshoot[36884]: SELinux is preventing /usr/s
bin/httpd from getattr access on the file /var/www/html/test.html.#012#012****
Plugin restorecon (92.2 confidence) suggests *****#012#012
If you want to fix the label. #012/var/www/html/test.html default label should b
e httpd_sys_content_t.#012Then you can run restorecon. The access attempt may ha
ve been stopped due to insufficient permissions to access a parent directory in
which case try to change the following command accordingly.#012Do#012# /sbin/res
torecon -v /var/www/html/test.html#012#012**** Plugin public_content (7.83 con
fidence) suggests *****#012#012If you want to treat test.html a
s public content#012Then you need to change the label on test.html to public con
tent t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content
t '/var/www/html/test.html' #012# restorecon -v '/var/www/html/test.html'#012#01
2**** Plugin catchall (1.41 confidence) suggests *****#
012#012If you believe that httpd should be allowed getattr access on the test.ht
ml file by default.#012Then you should report this as a bug.#012You can generate
a local policy module to allow this access.#012Do#012allow this access for now
by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semo
dule -X 300 -i my-httpd.pp#012
[root@dasavchenkov html]#
```

Figure 3.13: Анализ ситуации

16. Попробовал 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 нашел строчку Listen 80 и заменил её на Listen 81.(рис. -fig. 3.14).

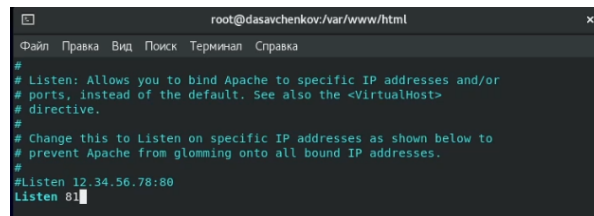


Figure 3.14: Изменеие порта 80 на 81

17. Проанализировал лог-файлы. Просмотрел файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log. (рис. -fig. 3.15).

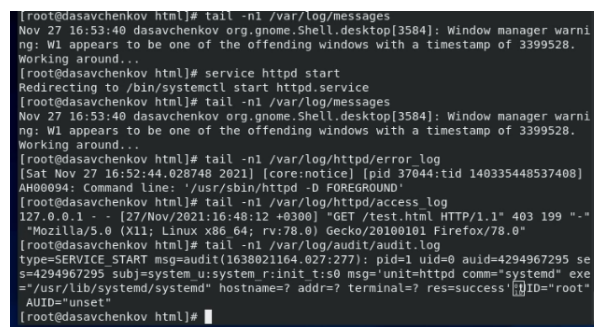


Figure 3.15: Анализ и просмотр лог-файлов

18. Выполнил команду: semanage port -a -t http_port_t -p tcp 81. После этого проверил список портов командой: semanage port -l | grep http_port_t. Убедился, что порт 81 появился в списке. (рис. -fig. 3.16).

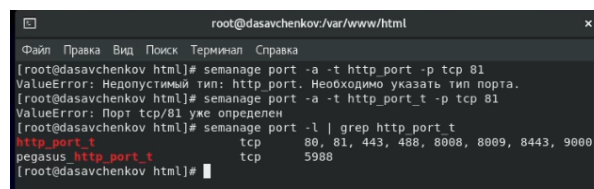
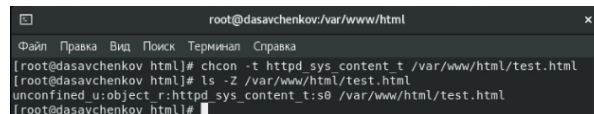


Figure 3.16: Выполнение и проверка

19. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`:
`chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test». (рис. -fig. 3.17), (рис. -fig. 3.18).



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

Figure 3.17: Возвращение контекста

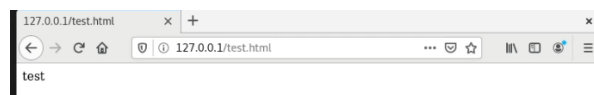
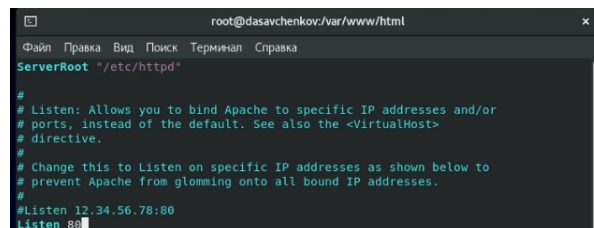


Figure 3.18: Получение доступа к файлу через браузер

20. Исправил обратно конфигурационный файл `apache`, вернув `Listen80`. (рис. -fig. 3.19).




```
root@dasavchenkov:/var/www/html
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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

Figure 3.19: Исправленный файл `apache`

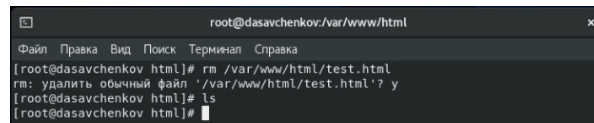
21. Удалил привязку `http_port_t` к 81 порту. (рис. -fig. 3.20).



```
[root@dasavchenkov html]# semanage port -d -t http_port_t -p tcp 81
```

Figure 3.20: Удаление привязки к 81 порту

22. Удалил файл `/var/www/html/test.html`. (рис. -fig. 3.21).

A terminal window titled 'root@dasavchenkov:/var/www/html' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the following commands and output:

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

Figure 3.21: Удаление файла /var/www/html/test.html

4 Выводы

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

Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов