

Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Барсегян Вардан Левонович НПИбд-01-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	15
	Список литературы	16

Список иллюстраций

2.1	Запуск и проверка веб-сервера	6
2.2	Контекст безопасности веб-сервера	7
2.3	Состояние переключателей SELinux	7
2.4	Статистика по политике	7
2.5	Определение типа файлов и папок	8
2.6	test.html	8
2.7	Контекст файла	8
2.8	Проверка в браузере	9
2.9	Изучение map, проверка контекста	9
2.10	Изменение контекста	10
2.11	Системный лог-файл	10
2.12	Смена порта	11
2.13	Сбой веб-сервера	11
2.14	Проверка лог-файлов	12
2.15	Проверка лог-файлов	12
2.16	Проверка лог-файлов	12
2.17	Добавление порта 81 в список	13
2.18	Возвращение контекста и перезапуск веб-сервера	13
2.19	Смена порта на 80	14
2.20	Удаление привязки к 81 порту и удаление html-файла	14

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

1. Убеждаюсь, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus*. Запускаю веб-сервер командой *service httpd start* и проверяю его статус командой *service httpd status* (рис. 2.1)

```
[vlbarsegyan@vlbarsegyan ~]$ getenforce
Enforcing
[vlbarsegyan@vlbarsegyan ~]$ 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
[vlbarsegyan@vlbarsegyan ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
o 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)
[vlbarsegyan@vlbarsegyan ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[vlbarsegyan@vlbarsegyan ~]$ 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 Tue 2024-03-19 18:45:02 MSK; 2s ago
     Docs: man:httpd.service(8)
```

Рис. 2.1: Запуск и проверка веб-сервера

2. Определяю контекст безопасности веб-сервера с помощью команды *ps auxZ | grep httpd* (рис. 2.2)

```
vlbarsegyan@vlbarsegyan:~$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      2864  0.1  0.6 20340 11612 ?
Ss   18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2871  0.0  0.4 21676  7540 ?
S    18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2872  0.0  0.8 2521344 15220 ?
Sl   18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2873  0.0  0.8 2259136 15220 ?
Sl   18:45   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  2874  0.0  0.8 2259136 15224 ?
Sl   18:45   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 vlbarse+ 3128 0.0  0.1 22
1688 2480 pts/0 S+ 18:45   0:00 grep --color=auto httpd
[vlbarsegyan@vlbarsegyan ~]$
```

Рис. 2.2: Контекст безопасности веб-сервера

3. Просматриваю текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b | grep httpd` (рис. 2.3)

```
without options, show SELinux status.
[vlbarsegyan@vlbarsegyan ~]$ 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
```

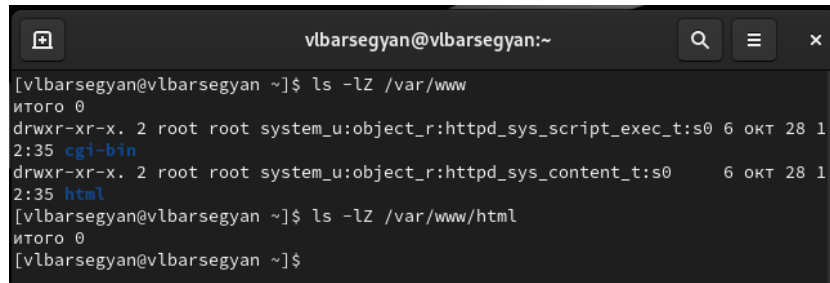
Рис. 2.3: Состояние переключателей SELinux

4. Смотрю статистику по политике с помощью команды `seinfo` (рис. 2.4)

```
vlbarsegyan@vlbarsegyan:~$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135
Sensitivities:           1
Types:                   5135
Users:                   8
Booleans:                357
Allow:                   65409
Auditallow:              172
Permissions:             457
Categories:              1024
Attributes:              259
Roles:                   15
Cond. Expr.:             390
Neverallow:              0
Dontaudit:               8647
```

Рис. 2.4: Статистика по политике

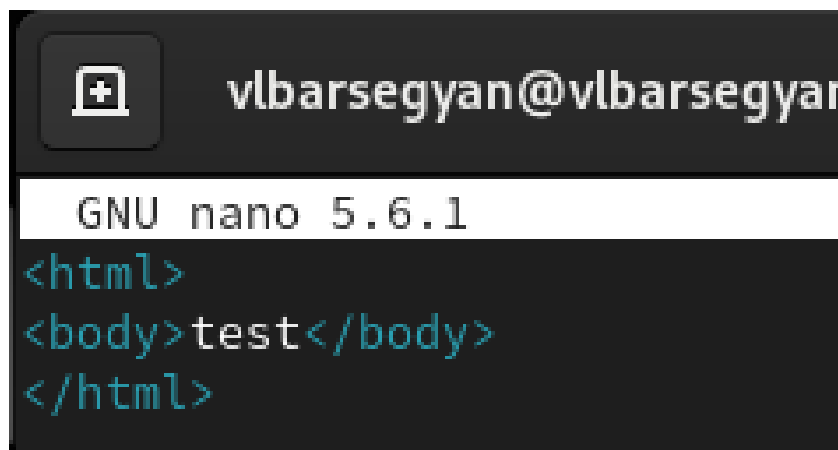
5. Определяю тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`. Аналогично для директории /var/www/html (рис. 2.5)



```
vlbarsegyan@vlbarsegyan:~$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 1
2:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 1
2:35 html
[vlbarsegyan@vlbarsegyan ~]$ ls -lZ /var/www/html
итого 0
[vlbarsegyan@vlbarsegyan ~]$
```

Рис. 2.5: Определение типа файлов и папок

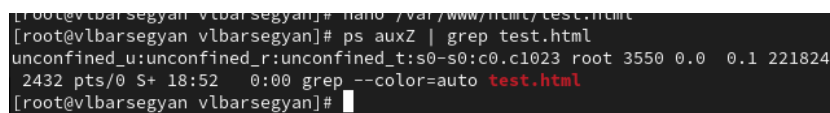
6. Создаю файл /var/www/html/test.html и записываю следующий html-код (рис. 2.6)



```
GNU nano 5.6.1
<html>
<body>test</body>
</html>
```

Рис. 2.6: test.html

7. Проверяю контекст созданного файла командой `ps auxZ | grep test.html` (рис. 2.7)



```
[root@vlbarsegyan vlbarsegyan]# nano /var/www/html/test.html
[root@vlbarsegyan vlbarsegyan]# ps auxZ | grep test.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3550 0.0 0.1 221824
2432 pts/0 S+ 18:52 0:00 grep --color=auto test.html
[root@vlbarsegyan vlbarsegyan]#
```

Рис. 2.7: Контекст файла

8. Проверяю в браузере, что файл успешно отображается (рис. 2.8)

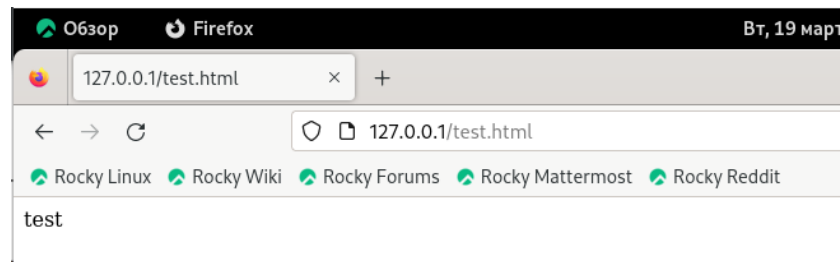


Рис. 2.8: Проверка в браузере

9. Изучаю справку man по командам `httpd` и `selinux`, также проверяю контекст файла командой `ls -Z /var/www/html/test.html` (рис. 2.9)

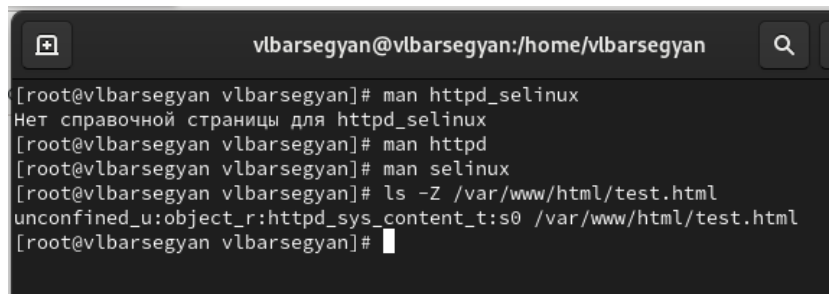


Рис. 2.9: Изучение man, проверка контекста

10. Изменяю контекст файла `test.html` командой `chcon -t samba_share_t /var/www/html/test.html`. После, проверяю его и открываю веб-страницу - нет доступа (рис. 2.10)

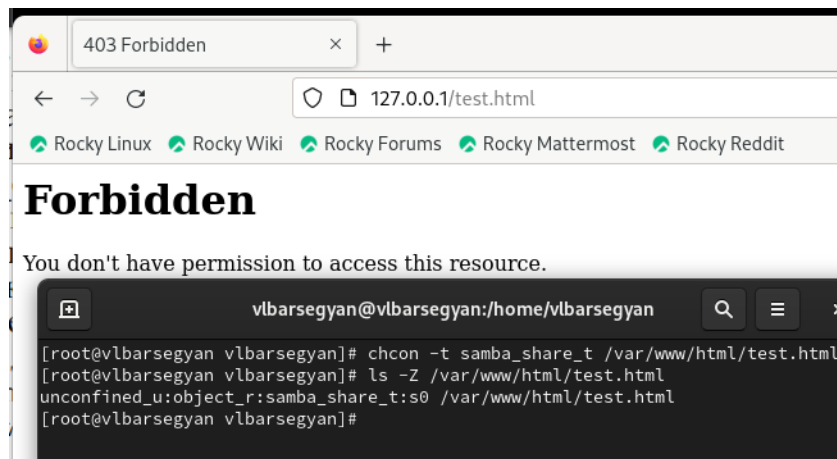


Рис. 2.10: Изменение контекста

11. Просматриваю системный лог-файл командой `tail /var/log/messages` (рис. 2.11)

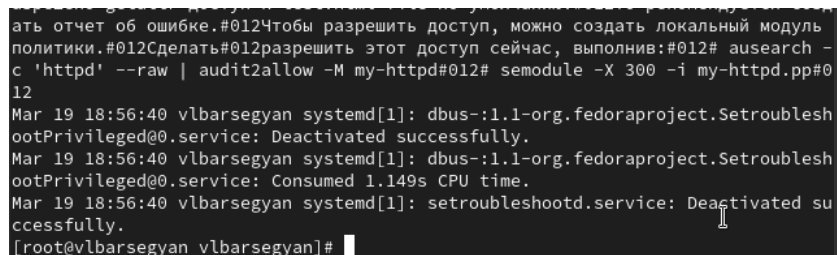


Рис. 2.11: Системный лог-файл

12. В файле `/etc/httpd/conf/httpd.conf` меняю порт на 81 (рис. 2.12)

```
#
# Change this to Listen on a specific IP address.
# httpd.service is enabled to run automatically
# available when the service starts.
# page for more information.
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) support
#
```

Рис. 2.12: Смена порта

13. Перезагружаю веб-сервер - получен сбой (рис. 2.13)

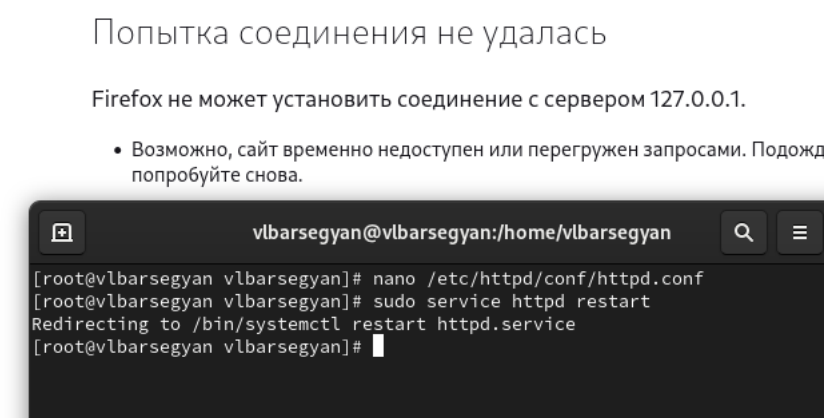


Рис. 2.13: Сбой веб-сервера

14. Анализирую лог-файлы командами `tail -nl /var/log/messages` и `cat /var/log/http/error_log` (рис. 2.14)

```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# tail -n1 /var/log/messages
Mar 19 19:03:08 vlbarsegyan systemd[2026]: Started Tracker metadata extractor.
[root@vlbarsegyan vlbarsegyan]# cat /var/log/httpd/error_log
[Tue Mar 19 18:45:02.155840 2024] [core:notice] [pid 2864:tid 2864] SELinux pol
icy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Tue Mar 19 18:45:02.159867 2024] [suexec:notice] [pid 2864:tid 2864] AH01232:
suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Tue Mar 19 18:45:02.195497 2024] [lbmethod:heartbeat:notice] [pid 2864:tid 286
4] AH02282: No slotmem from mod_heartbeat
[Tue Mar 19 18:45:02.201333 2024] [mpm_event:notice] [pid 2864:tid 2864] AH0048
9: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
```

Рис. 2.14: Проверка лог-файлов

15. Также проверяю лог-файл `/var/log/httpd/access_log` (рис. 2.15)

```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# cat /var/log/httpd/access_log
127.0.0.1 - - [19/Mar/2024:18:53:19 +0300] "GET /test.html HTTP/1.1" 200 33 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [19/Mar/2024:18:53:19 +0300] "GET /favicon.ico HTTP/1.1" 404 196
"http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2
0100101 Firefox/115.0"
127.0.0.1 - - [19/Mar/2024:18:56:26 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [19/Mar/2024:18:58:42 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [19/Mar/2024:18:58:43 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

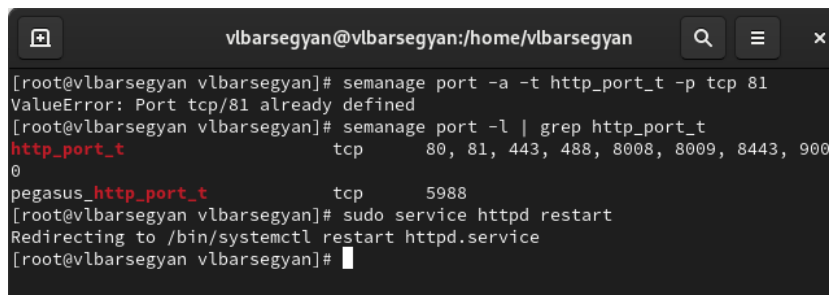
Рис. 2.15: Проверка лог-файлов

16. Также проверяю лог-файл `/var/log/audit/audit.log`. (рис. 2.16)

```
[root@vlbarsegyan vlbarsegyan]# cat /var/log/audit/audit.log
type=DAEMON_START msg=audit(1708186194.512:1034): op=start ver=3.0.7 format=enr
iched kernel=5.14.0-284.11.1.el9_2.x86_64 auid=4294967295 pid=722 uid=0 ses=429
4967295 subj=system_u:system_r:auditd_t:s0 res=successAUID="unset" UID="root"
type=SERVICE_START msg=audit(1708186194.521:5): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-journal-catalog-
update comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal
=? res=success'UID="root" AUID="unset"
```

Рис. 2.16: Проверка лог-файлов

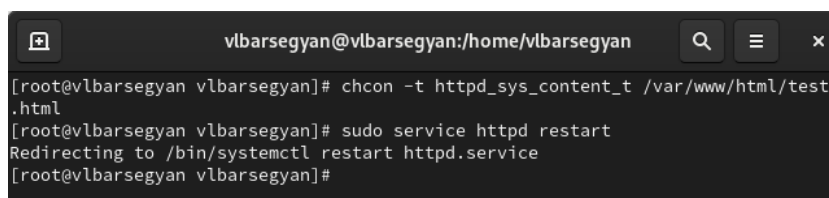
17. Выполняю команду `semanage port -a -t http_port_t -p tcp 81` и проверяю список портов командой `semanage port -l | grep http_port_t` - порт 81 появился в списке (рис. 2.17)



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@vlbarsegyan vlbarsegyan]# 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@vlbarsegyan vlbarsegyan]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@vlbarsegyan vlbarsegyan]#
```

Рис. 2.17: Добавление порта 81 в список

18. Возвращаю контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`, введя `chcon -t httpd_sys_content_t /var/www/html/test.html`. Перезапускаю веб-сервер командой `sudo service httpd restart` (рис. 2.18)



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@vlbarsegyan vlbarsegyan]# sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@vlbarsegyan vlbarsegyan]#
```

Рис. 2.18: Возвращение контекста и перезапуск веб-сервера

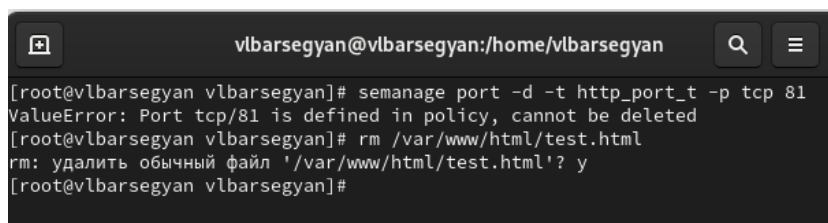
19. Возвращаю порт 80 в конфигурационном файле (рис. 2.19)

```
#
# Change this to Listen on a :
# httpd.service is enabled to
# available when the service s
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO)
```

Рис. 2.19: Смена порта на 80

20. Удаляю привязку `http_port_t` к 81 порту командой `semanage port -d -t http_port_t -p tcp 81` и удаляю файл `test.html` командой `rm /var/www/html/test.html` (рис. 2.20)



```
vlbarsegyan@vlbarsegyan:/home/vlbarsegyan
[root@vlbarsegyan vlbarsegyan]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@vlbarsegyan vlbarsegyan]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@vlbarsegyan vlbarsegyan]#
```

Рис. 2.20: Удаление привязки к 81 порту и удаление html-файла

3 Выводы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux, поработал с веб-сервером Apache

Список литературы