

# **Отчёт по лабораторной работе №6**

**Дисциплина: Основы информационной безопасности**

Дудырев Глеб Андреевич НПИбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>14</b>

# 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 . . . . .	8
2.5	Определение типа файлов и папок . . . . .	8
2.6	test.html . . . . .	8
2.7	Контекст файла . . . . .	9
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 . . . . .	10
2.13	Сбой веб-сервера . . . . .	11
2.14	Проверка лог-файлов . . . . .	11
2.15	Проверка лог-файлов . . . . .	11
2.16	Проверка лог-файлов . . . . .	12
2.17	Добавление порта 81 в список . . . . .	12
2.18	Возвращение контекста и перезапуск веб-сервера . . . . .	12
2.19	Смена порта на 80 . . . . .	13
2.20	Удаление привязки к 81 порту и удаление html-файла . . . . .	13

## 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)

```
[root@gadudihrev gadudihrev]# getenforce
Enforcing
[root@gadudihrev gadudihrev]# 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:      43
[root@gadudihrev gadudihrev]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@gadudihrev gadudihrev]# 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 Fri 2024-04-26 18:50:55 MSK; 7s ago
     Docs: man:httpd.service(8)
  Main PID: 10369 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 23037)
   Memory: 23.3M
      CPU: 44ms
   CGroup: /system.slice/httpd.service
           └─10369 /usr/sbin/httpd -DFOREGROUND
             └─10370 /usr/sbin/httpd -DFOREGROUND
               └─10374 /usr/sbin/httpd -DFOREGROUND
                 └─10375 /usr/sbin/httpd -DFOREGROUND
                   └─10376 /usr/sbin/httpd -DFOREGROUND

anp 26 18:50:55 gadudihrev systemd[1]: Starting The Apache HTTP Server...
anp 26 18:50:55 gadudihrev httpd[10369]: AH00558: httpd: Could not reliably det
anp 26 18:50:55 gadudihrev systemd[1]: Started The Apache HTTP Server.
anp 26 18:50:55 gadudihrev httpd[10369]: Server configured, listening on: port
lines 1-20/20 (END)
```

Рис. 2.1: Запуск и проверка веб-сервера

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

```
[root@gadudihrev gadudihrev]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      10369 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      10370 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      10374 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      10375 ?        00:00:00 httpd
system_u:system_r:httpd_t:s0      10376 ?        00:00:00 httpd
[root@gadudihrev gadudihrev]#
```

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)

```
[root@gadudihrev gadudihrev]# 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
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_avahi                off
httpd_dbus_sssd                 off
httpd_dontaudit_search_dirs     off
httpd_enable_cgi                on
httpd_enable_ftp_server         off
httpd_enable_homedirs           off
httpd_execmem                   off
httpd_graceful_shutdown         off
httpd_manage_ipa                off
httpd_mod_auth_ntlm_winbind     off
httpd_mod_auth_pam              off
httpd_read_user_content         off
httpd_run_ipa                   off
httpd_run_preupgrade            off
httpd_run_stickshift            off
httpd_serve_cobbler_files       off
httpd_setrlimit                 off
httpd_ssi_exec                  off
httpd_sys_script_anon_write     off
httpd_tmp_exec                  off
httpd_tty_comm                  off
httpd_unified                   off
httpd_use_cifs                  off
```

Рис. 2.3: Состояние переключателей SELinux

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

```
[root@gadudihrev gadudihrev]# 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:               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
[root@gadudihrev gadudihrev]#
```

Рис. 2.4: Статистика по политике

- 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)

```
[root@gadudihrev gadudihrev]# 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 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 12:35 html
[root@gadudihrev gadudihrev]# ls -lZ /var/www/html/
итого 0
[root@gadudihrev gadudihrev]#
```

Рис. 2.5: Определение типа файлов и папок

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

```
gadudihrev@gadudihrev:/home/gadudihrev — vim /var/www/html/test.html
<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@gadudihrev gadudihrev]# ps auxZ | grep html.test
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 10974 0.0 0.0 221824 2404 pts/0 S+ 19:02 0:00 grep --color=auto html.test
[root@gadudihrev gadudihrev]#
```

Рис. 2.7: Контекст файла

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

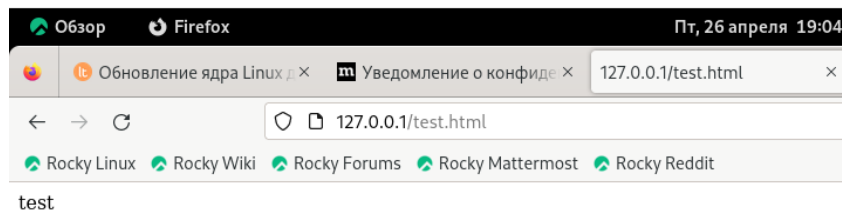


Рис. 2.8: Проверка в браузере

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

```
[root@gadudihrev gadudihrev]# man httpd
[root@gadudihrev gadudihrev]# man selinux
[root@gadudihrev gadudihrev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@gadudihrev gadudihrev]#
```

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)

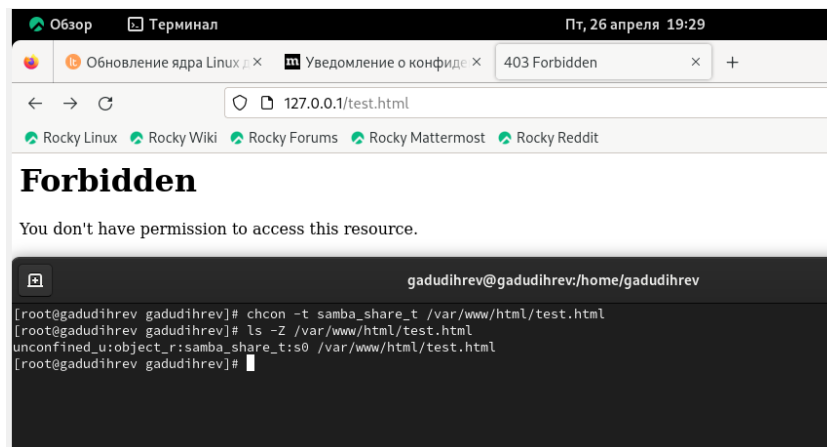


Рис. 2.10: Изменение контекста

## 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)

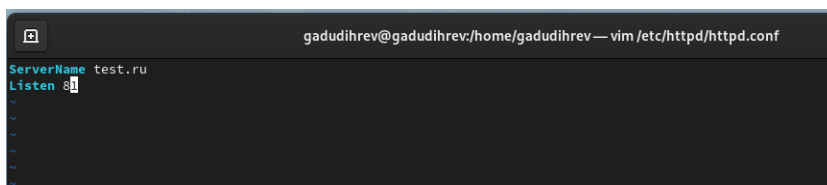


Рис. 2.12: Смена порта

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

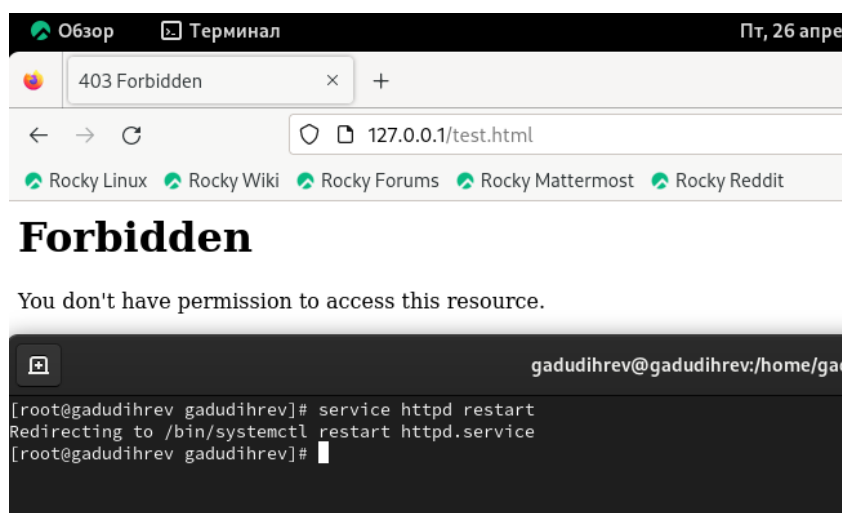


Рис. 2.13: Сбой веб-сервера

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

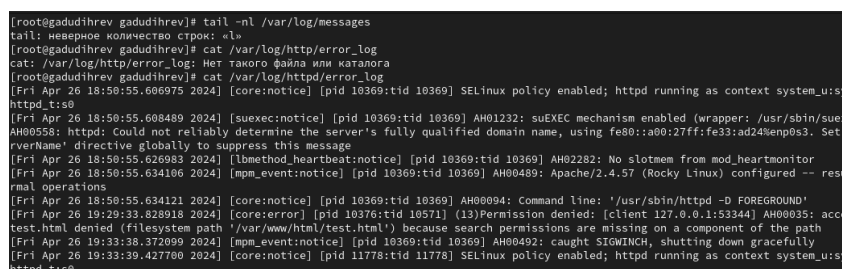


Рис. 2.14: Проверка лог-файлов

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



Рис. 2.15: Проверка лог-файлов

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

```
gadudihrev@gadudihrev:/home/gadudihrev
er(42 comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=USER_START msg=audit(1714145045.089:75): pid=1595 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 m
ss:op:PAKsession,open grantors:pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask acct="gdm" exe="/usr/libexec/gdm-session
on-worker" hostname=gadudihrev addr=? terminal=/dev/tty1 res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145046.608:76): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=kd
ump comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1714145049.092:77): prog-id=31 op=LOAD
type=BPF msg=audit(1714145049.092:78): prog-id=32 op=LOAD
type=BPF msg=audit(1714145049.092:79): prog-id=33 op=LOAD
type=SERVICE_START msg=audit(1714145049.337:80): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=systemd-
localised comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145050.273:81): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=wp
a_supplicant comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145050.280:82): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=ge
oclue comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145051.035:83): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=pa
ckagekit comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1714145051.850:84): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=Net
workManager-dispatcher comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145055.370:85): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=co
lorc comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=BPF msg=audit(1714145055.484:86): prog-id=34 op=LOAD
type=SERVICE_START msg=audit(1714145055.790:87): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=fp
rintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145056.103:88): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=ire
alnd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SERVICE_START msg=audit(1714145057.347:89): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=pl
ymouth-quit-wait comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
type=SYSTEM_RUNNING msg=audit(1714145057.390:90): pid=1948 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=unit=ol
```

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)

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

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)

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

Рис. 2.18: Возвращение контекста и перезапуск веб-сервера

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

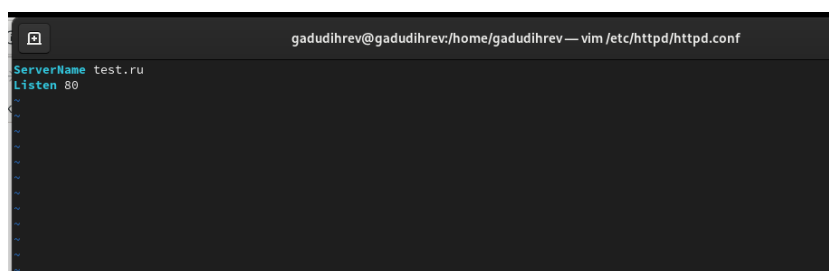


Рис. 2.19: Смена порта на 80

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)

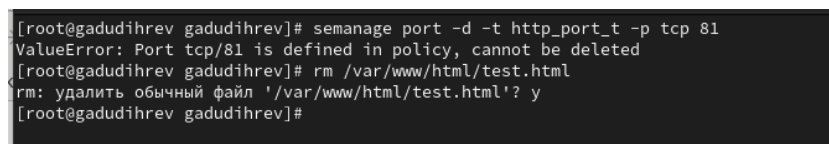


Рис. 2.20: Удаление привязки к 81 порту и удаление html-файла

## 3 Выводы

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