

# **Отчёт по лабораторной работе №6**

**Мандатное разграничение прав в Linux**

Федорина Эрнест Василевич

# Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	12
	Список литературы	13

## Список иллюстраций

3.1	начало работы с selinux . . . . .	7
3.2	статус enforce и работы веб-сервера . . . . .	8
3.3	активный веб-сервер . . . . .	8
3.4	контекст безопасности . . . . .	8
3.5	состояние переключателей SELinux . . . . .	9
3.6	статистика по политике . . . . .	9
3.7	работа с директорией html . . . . .	10
3.8	открытие test.html через веб-сервер . . . . .	10
3.9	просмотр и изменение контекста файла . . . . .	10
3.10	просмотр log-файлов . . . . .	11
3.11	просмотр новых log-файлов . . . . .	11
3.12	просмотр новых log-файлов . . . . .	11

## **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 Теоретическое введение

Apache HTTP-сервер (в иронической трактовке является искажённым сокращением от англ. а patchy server; среди русских пользователей общепринято переводное апáч) — свободный веб-сервер.

Apache является кроссплатформенным ПО, поддерживает операционные системы Linux, BSD, macOS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т.д.[1].

### 3 Выполнение лабораторной работы

Для начала организуем рабочий стренд, - установим арасче, проверим используемый режим и политику, а также отключим некоторые пакетные фильтры (рис. [3.1])

```
Установлен:
apr-1.7.0-12.el9.aarch64      apr-util-1.6.1-23.el9.aarch64
apr-util-bdb-1.6.1-23.el9.aarch64  apr-util-openssl-1.6.1-23.el9.aarch64
centos-logos-httpd-90.8-1.el9.noarch  httpd-2.4.62-1.el9.aarch64
httpd-core-2.4.62-1.el9.aarch64      httpd-filesystem-2.4.62-1.el9.noarch
httpd-tools-2.4.62-1.el9.aarch64     mod_http2-2.0.26-2.el9.aarch64
mod_lua-2.4.62-1.el9.aarch64

Выполнено!
[root@localhost evfedorina]# nano /etc/selinux/config
[root@localhost evfedorina]# iptables -F
[root@localhost evfedorina]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument 'iptables'
Try 'iptables -h' or 'iptables --help' for more information.
[root@localhost evfedorina]# iptables -P INPUT ACCEPT
[root@localhost evfedorina]# iptables -P OUTPUT ACCEPT
[root@localhost evfedorina]#
```

Рис. 3.1: начало работы с selinux

Увидели, что веб-сервер не работает (рис. [3.2]), включили его (рис. [3.3]) и посмотрели контекст безопасности (рис. [3.4])

```
[root@localhost evfedorina]# getenforce
Permissive
[root@localhost evfedorina]# sestatus
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: permissive
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@localhost evfedorina]# 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)
```

Рис. 3.2: статус enforce и работы веб-сервера

```
bash: start: команда не найдена...
[root@localhost evfedorina]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost evfedorina]# 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 2024-10-12 15:59:16 MSK; 10s ago
   Docs: man:httpd.service(8)
   Main PID: 96082 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
   Tasks: 177 (limit: 11746)
   Memory: 21.4M
   CPU: 112ms
   CGroup: /system.slice/httpd.service
           └─96082 /usr/sbin/httpd -DFOREGROUND
             └─96083 /usr/sbin/httpd -DFOREGROUND
               └─96084 /usr/sbin/httpd -DFOREGROUND
                 └─96085 /usr/sbin/httpd -DFOREGROUND
                   └─96089 /usr/sbin/httpd -DFOREGROUND

окт 12 15:59:16 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 12 15:59:16 localhost.localdomain httpd[96082]: AH00558: httpd: Could not reliably det
```

Рис. 3.3: активный веб-сервер

```
[root@localhost evfedorina]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 96082 0.0 0.5 29528 10104 ? Ss 15:5
9 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 96083 0.0 0.4 31572 8524 ? S 15:5
9 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 96084 0.0 0.5 1452924 11632 ? Sl 15:5
9 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 96085 0.0 0.7 1585020 14044 ? Sl 15:5
9 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 96089 0.0 0.6 1452924 11752 ? Sl 15:5
9 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 96267 0.0 0.4 237416 8320 pts/
0 T 15:59 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 96306 0.0 0.4 237416 8320 pts/
0 T 16:01 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 96324 0.0 0.1 221396 2048 pts/
0 S+ 16:03 0:00 grep --color=auto httpd
[root@localhost evfedorina]#
```

Рис. 3.4: контекст безопасности

Потом посмотрели состояние переключателей (рис. [3.5])



```
[root@localhost evfedorina]# 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
```

Рис. 3.5: состояние переключателей SELinux

Далее посмотрим статистику по политике (рис. [3.6])

```
[root@localhost evfedorina]# 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:                   5169     Attributes:              259
Users:                   8        Roles:                   15
Booleans:                358     Cond. Expr.:            390
Allow:                   65633    Neverallow:              0
Auditallow:              176     Dontaudit:              8703
Type_trans:              271851   Type_change:             94
Type_member:              37      Range_trans:            5931
Role allow:              40       Role_trans:              417
Constraints:             70       Validatetrans:           0
MLS Constrains:          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@localhost evfedorina]#
```

Рис. 3.6: статистика по политике

У нас 8 пользователей, 5169 типов и 15 ролей.

Определим тип файлов в директории /var/www/html, создадим там файл test.html и проверим его контекст (рис. [3.7])

```
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ash
[root@localhost evfedorina]# touch /var/www/html/test.html
[root@localhost evfedorina]# nano /var/www/html/test.html
[root@localhost evfedorina]# secon --file /var/www/html/test.html
user: unconfined_u
role: object_r
type: httpd_sys_content_t
sensitivity: s0
clearance: s0
mls-range: s0
[root@localhost evfedorina]#
```

Рис. 3.7: работа с директорией html

Обратимся к файлу через веб-сервер и увидим там текст, написанный нами ранее в файле test.html, доступ есть (рис. [3.8])

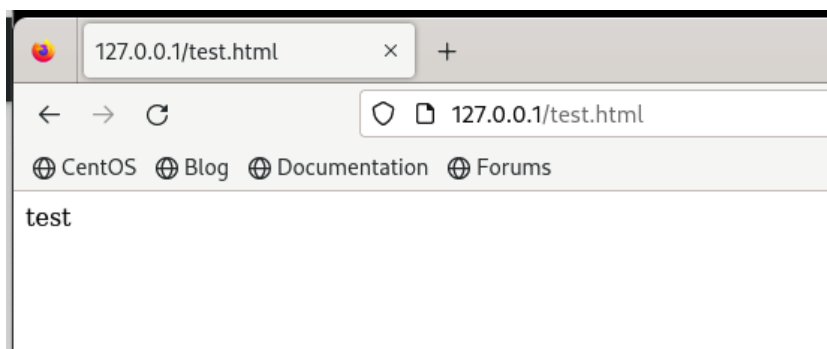


Рис. 3.8: открытие test.html через веб-сервер

Изучив справку httpd\_selinux мы выяснили нужные контексты, сопоставили их с контекстами нашего файла, рассмотрели полученный контекст детально, а потом изменили контекст файла, чтобы процесс httpd не имел доступа к файлу (рис. [3.9])

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

Рис. 3.9: просмотр и изменение контекста файла

Смотрим log-файлы веб-сервера и системные логи (рис. [3.10])

```
-rw-r--r--. 1 root root 33 окт 12 16:09 /var/www/html/test.html
[root@localhost evfedorina]# tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Нет такого файла или каталога
[root@localhost evfedorina]# tail /var/log/messages
Oct 12 16:16:36 localhost systemd[1]: dbus-1.1-1-org.fedoraproject.SetroubleshootPrivileged01.service: Deactivated successfully.
Oct 12 16:16:36 localhost systemd[1]: dbus-1.1-1-org.fedoraproject.SetroubleshootPrivileged01.service: Consumed 2.533s CPU time.
Oct 12 16:16:36 localhost systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 12 16:16:36 localhost systemd[1]: setroubleshootd.service: Consumed 3.431s CPU time.
Oct 12 16:16:42 localhost gnome-shell[1704]: libinput error: event1 - Parallels Virtual Mouse: client bug: event processing lagging behind by 19ms, your system is too slow
Oct 12 16:16:42 localhost gnome-shell[1704]: libinput error: event1 - Parallels Virtual Mouse: WARNING: log rate limit exceeded
Oct 12 16:17:13 localhost gnome-shell[1704]: Window manager warning: last_focus_time (12899017) is greater than comparison_time (12899017). This is a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 12 16:17:13 localhost gnome-shell[1704]: Window manager warning: last_user_time (12899017) is greater than comparison_time (12899017). This is a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 12 16:17:13 localhost gnome-shell[1704]: Window manager warning: W18 appears to be one of the offending windows with a bad focus time. This is a buggy client sending inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW. Trying to work around...
Oct 12 16:17:19 localhost pipewire[1765]: spa.audioconvert: 0xaaaf27ef300: (0 suppressed) out of buffers on port 0 1
[root@localhost evfedorina]#
```

Рис. 3.10: просмотр log-файлов

В httpd.conf изменили параметр listen с 80 на 81, потом перезапустили веб-сервер, произошёл сбой.

Далее мы опять посмотрели log-файлы (рис. [3.11])

```
[root@localhost evfedorina]# tail -l /var/log/messages
Oct 12 16:29:18 localhost gnome-shell[1704]: libinput error: event4 - Parallels Virtual Mouse: client bug: event processing lagging behind by 19ms, your system is too slow
Oct 12 16:29:18 localhost gnome-shell[1704]: libinput error: event3 - Parallels Virtual Mouse: client bug: event processing lagging behind by 18ms, your system is too slow
Oct 12 16:29:37 localhost systemd[1]: Stopping The Apache HTTP Server...
Oct 12 16:29:39 localhost systemd[1]: httpd.service: Deactivated successfully.
Oct 12 16:29:39 localhost systemd[1]: Stopped The Apache HTTP Server.
Oct 12 16:29:39 localhost systemd[1]: httpd.service: Consumed 3.107s CPU time.
Oct 12 16:29:39 localhost systemd[1]: Starting The Apache HTTP Server...
Oct 12 16:29:39 localhost httpd[99023]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
Oct 12 16:29:39 localhost systemd[1]: Started The Apache HTTP Server.
Oct 12 16:29:39 localhost httpd[99023]: Server configured, listening on: port 81
[root@localhost evfedorina]#
```

Рис. 3.11: просмотр новых log-файлов

Выполнили команду `semanage port`, проверили список портов и увидели там 81, а затем снова запустили веб-сервер Apache, успешно (рис. [3.12])

```
[root@localhost evfedorina]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@localhost evfedorina]# semanage port -l | grep http_port_t
http_port_t      tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
```

Рис. 3.12: просмотр новых log-файлов

В конце лабораторной работы убрали все изменения в файлах, удалили `test.html` и удалили привязку `httpd_port_t` к 81 порту

## 4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

## Список литературы

1. apache [Электронный ресурс]. Wikipedia, 2024. URL: <https://ru.wikipedia.org/wiki/Apache>.